IoT

MDPI

Review

Analyzing Threats and Attacks in Edge Data Analytics within IoT Environments

Poornima Mahadevappa [1,*], Redhwan Al-amri [2], Gamal Alkawsi [3,*], Ammar Ahmed Alkahtani [4], Mohammed Fahad Alghenaim [5] and Mohammed Alsamman [6]

1 School of Computer Science and Engineering, Taylor's University, Subang Jaya 47500, Malaysia
2 Department of Applied Computing, Wales Institute of Science and Art, University of Wales Trinity Saint David, Swansea SA1 8EW, UK; r.al-amri@uwtsd.ac.uk
3 Institute of Informatics and Computing in Energy, The Energy University, Kajang 43000, Malaysia
4 Renewable Energy Engineering Department, Fahad Bin Sultan University, Tabuk 71454, Saudi Arabia; aalkahtani@fbsu.edu.sa
5 Advanced Informatics Department, Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Kuala Lumpur 54100, Malaysia; aalghenaim@graduate.utm.my
6 School of Computing, Universiti Utara Malaysia, Sintok 06010, Malaysia; alsamman@uum.edu.my
* Correspondence: poornima.nkp@gmail.com (P.M.); gamal.abdulnaser@uniten.edu.my (G.A.)

Abstract: Edge data analytics refers to processing near data sources at the edge of the network to reduce delays in data transmission and, consequently, enable real-time interactions. However, data analytics at the edge introduces numerous security risks that can impact the data being processed. Thus, safeguarding sensitive data from being exposed to illegitimate users is crucial to avoiding uncertainties and maintaining the overall quality of the service offered. Most existing edge security models have considered attacks during data analysis as an afterthought. In this paper, an overview of edge data analytics in healthcare, traffic management, and smart city use cases is provided, including the possible attacks and their impacts on edge data analytics. Further, existing models are investigated to understand how these attacks are handled and research gaps are identified. Finally, research directions to enhance data analytics at the edge are presented.

Keywords: edge computing; edge data analytics; security threats; security models; edge applications

Citation: 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. https://doi.org/10.3390/iot5010007

Academic Editors: Arun Ravindran and Reshmi Mitra

Received: 30 January 2024
Revised: 22 February 2024
Accepted: 24 February 2024
Published: 5 March 2024

1. Introduction

Edge computing is a distributed systems paradigm that aims to offload selected services of applications from the cloud and bring them closer to the end-user. It is a generic term that captures associated paradigms, such as fog computing, mist computing, mobile edge computing, and cloudlet computing. Services are hosted at the edge of the network on nodes, such as routers, gateways, and micro-data centers. Data generated from end-users or sensors on Internet of Things (IoT) devices or sensors are analyzed and processed on the edge, which is nearer to the data source. Although edge nodes may be resource-limited when compared to the cloud, data analytics on the edge offers three benefits: (i) better responsiveness by reducing round-trip communication latency, (ii) a higher degree of data privacy, and (iii) minimizing the ingress bandwidth demand to the cloud [1].

Security is of paramount importance when using edge nodes for data processing since a large attack surface is exposed. User-generated or sensor data that are transferred to edge nodes must be protected for confidentiality and integrity, even if an edge node is attacked [2]. Data must be protected even when attacks, such as Man-In-The-Middle (MITM), Denial of Service (DoS), eavesdropping, and others (to be discussed later), are underway. Many attacks while performing data analytics have been previously understood in the context of the cloud and are inherited by the edge (for example, Man-In-The-Middle (MITM), Denial of Service (DoS), or eavesdropping). Recent security breaches or incidents in edge computing serve to highlight the severity of security risks in this domain. For example, in

2020, a vulnerability known as "Ripple20" was discovered, affecting millions of IoT devices across various industries, including edge computing devices. This vulnerability allowed attackers to remotely execute malicious code, potentially leading to data breaches or system compromise [3]. Another notable incident involved the exploitation of a vulnerability in the "Treck" TCP/IP stack, affecting numerous IoT and edge devices. This vulnerability, dubbed "AMNESIA:33," enabled attackers to execute remote code execution, DoS attacks, and other malicious activities [4]. These incidents underscore the importance of addressing security vulnerabilities in edge computing environments to mitigate the risk of data breaches, system compromise, and other cyber threats.

This article is concerned with security threats in the context of edge data analytics. There are two main reasons why security threats in edge data analytics need to be considered. Firstly, in edge computing, when ubiquitous devices outsource their data for processing to edge servers, vulnerabilities can be exploited for malicious activities on the data. This may be accentuated when there is a lack of data storage auditing services [5]. Therefore, data integrity and data authorization will be affected. Secondly, bandwidth and computation-intensive applications, such as augmented reality and video analytics (for example, cognitive wearable assistance [6]), will process sensitive data at the edge. These applications can emerge in the real world only if security threats arising from data analytics at the edge can be mitigated.

Numerous articles have examined security threats in the context of edge computing. They are summarized in Table 1. Twenty-six research articles are presented in the table, and whether they consider threats in edge data analytics, the impact of threats on edge nodes, and if they analyze edge threat models are highlighted. It is noted that most papers explore security in the general sense, but do not focus on edge data analytics. Security issues at the architectural, storage, and communication levels have been presented [7–9]. Fewer research articles examine security for data analytics at the edge. Examples include considering the computational complexities of existing security models and the security requirements for secure data analytics [10]. The threats related to data storage in a transient environment have been considered [11]. There is a partial consideration of threats during data analytics in the literature [12–17]. Similarly, the impact of the threats on edge nodes is partially considered [18,19]. This article more comprehensively examines the threats and the impact of threats and analyzes threat models relevant to edge data analytics.

The review method for preparing this article was based on an approach presented in the literature [20]. It included defining the objective of the review and the research questions.

The objectives of this review are to:

O1. Highlight the edge data analytics process for selected application use cases, including potential attacks and their impact on edge data analytics.

O2. Review the state-of-the-art security threat models to identify how attacks are handled on the edge during data analytics and identify research gaps.

O3. Identify the impact of threats on edge data analytics.

The research questions considered in this article are:

RQ1. How do various attacks affect data analytics in edge computing? This will be discussed in Section 4 by considering three use case applications.

RQ2. What are the different security models available to mitigate various data threats? This will be discussed in Section 5.

RQ3. What is the severity of the attacks on edge data analytics? This will be discussed in Section 5.1.

The remainder of this article is organized as follows. Section 2 presents the background to edge data analytics. Section 3 presents a classification of security threats relevant to edge data analytics. Section 4 discusses application use cases. Section 5 reviews the existing security threat models and identifies their impacts on the edge application use cases. Finally, Section 6 presents the challenges and potential future research directions for addressing security threats in edge data analytics.

Table 1. Summary of related work (✓—work considered, ×—not considered, and δ—partially considered).

Ref.	Description	Threat Considered	Impact of the Threat	Analysis of the Threat Model Considered	Remarks
[10]	Secure data analytics in edge computing	✓	×	✓	Propose key requirements for secure data analytics and identify pros and cons of existing works on data analytics.
[11]	Data security in edge computing	×	×	✓	Review different cryptography-based solutions to address data security issues in edge computing.
[21]	Security issues during authentication schemes for data integrity	×	×	✓	Evaluate existing methods to preserve data integrity in fog and cloud computing and identify their limitations.
[7]	Security issues in edge computing	×	×	✓	Review security issues in terms of access control, key management, privacy, attack mitigation, and anomaly detection.
[22]	Security-as-a-Service in multi-access edge computing	✓	×	✓	Evaluate IDS, secure communication, and access control mechanisms, and propose a secure service deployment framework.
[23]	Security issues that are caused by adopting virtualization in edge computing	✓	×	✓	Discuss the advantages of adopting virtualization, containers, Uni kernels, and real-time OS in edge computing. Security issues and attacks on these technologies with different use case scenarios are addressed.
[24]	Security and prevention mechanisms in fog computing	×	×	✓	Comparative analysis of different techniques to address common security issues in edge computing.
[25]	Security threats in mobile edge computing	✓	×	✓	Review the advantages of using machine learning techniques to improve network efficiency and handle malicious attacks.
[26]	Security aspects in fog computing	×	×	×	Discuss security issues in edge computing caused due to its operations in the physical environment and the need for interoperability between edge nodes and IoT devices with various solutions.
[27]	Security issues in edge, fog, and IoT applications	×	×	×	Identify security issues and evaluate authentication and encryption schemes to address these issues.
[28]	Review of fog-based applications' architecture and security issues at the architectural level	×	×	×	Discuss four edge-based applications and security concerns to prevent malicious access and data modification in these applications.
[29]	Security issues due to fog infrastructure in various applications	×	×	✓	The present data analytics taxonomy discusses the complexity during data processing with research challenges.
[17]	Discuss how to improve security issues and protocols in fog computing	×	×	✓	Present a comprehensive survey on overall issues in edge computing. Analyze security models that address location and data privacy, secure communication, and various intrusion systems.
[11]	Analyze fog computing architecture, security, and trust issues	×	✓	✓	Discuss security issues, various mechanisms, and different technologies to handle data security and privacy in edge computing.
[16]	A comprehensive review of edge computing security issues with a few proposed solutions	δ	δ	✓	Identify the challenges of the existing security models to handle threats in edge computing and suggest a few solutions that can be applied to a similar edge computing paradigm.

Table 1. *Cont.*

Ref.	Description	Threat Considered	Impact of the Threat	Analysis of the Threat Model Considered	Remarks
[8]	Security and privacy issues due to fog computing architecture	×	×	×	Identify the threats in the edge computing platform.
[30]	Challenges due to data security and privacy	δ	✓	×	Justify how cloud data security solutions cannot be applied to edge computing and highlight the importance of addressing this issue in edge computing.
[31]	Layer-wise security and threat issues	×	×	✓	Identify the threats in each layer and propose a risk-based trust model to secure the decision-making process and secure data in the edge layer.
[14]	Review of security and privacy issues to secure fog-based IoT application	δ	✓	×	Identify the threats and security issues related to data storage, computation, and data sharing in the fog layer.
[13]	Potential security issues in the fog-based application	✓	✓	×	Various edge computing solutions are analyzed, and security models related to privacy-preserving, insider attacks, resource management, encryption, and authentication schemes are discussed.
[32]	Address all the common security and privacy issues in fog computing and identify gaps in the existing security solutions	×	×	✓	Propose solution toward establishing trust, secure communication channels, and privacy-preserving schemes.
[33]	Concerning security and resilience edge and fog computing architectures are analyzed	×	×	×	Address issues related to virtualized infrastructure and software-driven communication.
[12]	Using fog computing, how to secure healthcare data is discussed	✓	×	×	Propose encryption algorithms to secure data on the edge layer.
[19]	MITM attacks are studied exclusively by CPU and memory consumption on fog devices	×	✓	×	Present authentication and authorization techniques to protect edge nodes from an MITM attack.
[34]	Security threats when adopting edge computing in IoT applications	×	×	×	Review existing security models that address MITM, intrusion detection, malicious nodes, and data protection models.
[18]	Security threats that affect the confidentiality, integrity, and availability of the architecture	×	✓	×	Discuss the advantages of adopting edge computing in IoT applications. Recommend a few solutions to address the vulnerabilities and threats due to adoption.
Current study	Security issues on edge nodes that affect decision-making and analytics of the applications	✓	✓	✓	Review potential threats that affect edge nodes and disturb the normal functioning of applications. Identify research gaps in existing security models.

2. Edge Data Analytics

Edge data analytics allows preprocessing data for obtaining real-time decisions. The data flow is similar to that on the cloud, with the difference that edge resources process data. The data analytics process will need to consider the following five aspects: (a) data source, (b) content format, (c) data storage, (d) data staging, and (e) data processing [35]. Data processing on edge nodes enables real-time interactions. The flow of data in an edge computing layer sandwiched between the cloud and end-user devices layer (referred to as the Internet of Things (IoT)) is shown in Figure 1. In edge-based IoT applications, sensing, collecting, and analyzing the data depend on the types of services they provide.

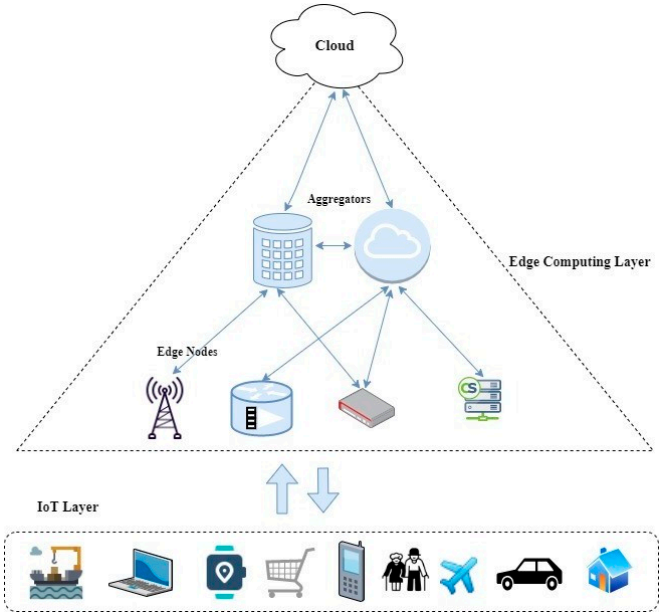

Figure 1. Flow of data in the edge computing layer.

A data processing model has been proposed for edge computing systems [36]. Heterogeneous data are collected from ubiquitous devices and pushed forward through communication channels to preprocess. Real-time analysis and decision-making occur to support quick responses to the applications on IoT devices. The services offering real-time analysis may be transferred to the cloud. Data processing depends on the information gathered from the hierarchical edge layer, how quickly the data are collected, and how they trigger the specific services for decision-making. The components that support this process are shown in Figure 2.

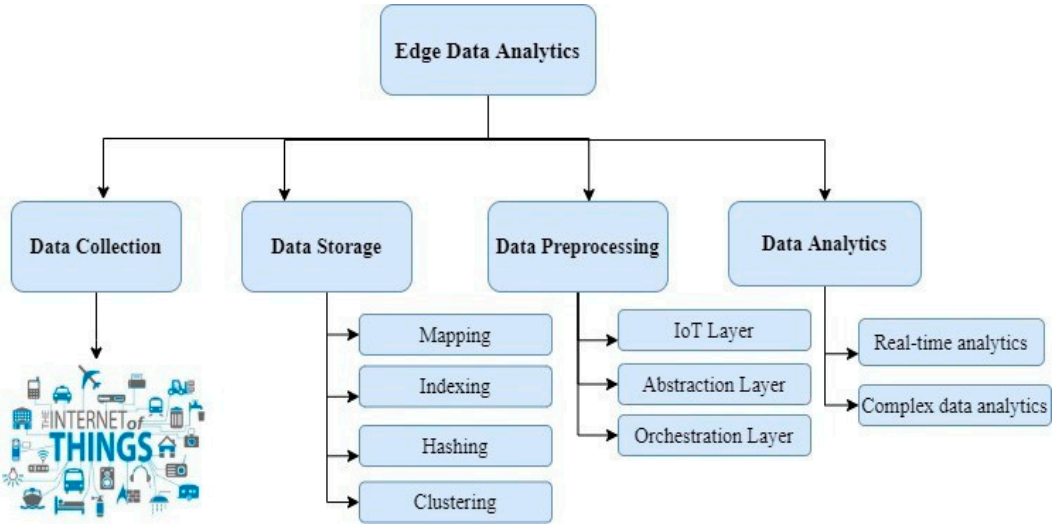

Figure 2. Components of edge data analytics.

Data Collection—All devices are the primary source to generate data. The devices may be electrical appliances, homes, or embedded systems connected with the unique Internet Protocol (IP) to establish connection and communication among them. Edge nodes closer to devices collect data and support computation for the IoT devices' applications by offloading tasks across the cloud and edge nodes. Various deployment models deploy the task as middleware between the cloud and IoT devices with efficient resource utilization [37].

Data Storage—Data collected from devices can be stored in either the device or on edge nodes in virtual machines or containers [38]. Typical efficient storage relies on techniques such as mapping, hashing, clustering, replication, indexing, and so on. Data are collected in clusters and sent to the storage devices [39]. In indexing, indexes are created based on the extraction, recognition, and labeling of real-time data, such as video streams or social media data [40]. In replication, the data are duplicated to support the data-intense applications by encapsulating the coherent data logically [41].

Data Processing—IoT verticals, abstraction layers, and orchestration layers are the three components responsible for data processing in edge computing architectures. IoT verticals include the application that is in use. They provide multitenancy to host the application on edge data servers and provide flexibility and interoperability to the edge nodes. The abstraction layer provides a uniform virtualized platform through a generic API to monitor, provision, and control physical resources. The orchestration layer includes data API and orchestration layer API, which are responsible for node placement or node selection, run-time monitoring, control during execution, and optimizing data-driven decisions [42,43].

Data Analytics—Data collected from IoT devices are preprocessed on the edge nodes through intensive real-time task analysis. This establishes real-time interactions between the edge nodes and the users. For example, generating a diagnosis report for a doctor to treat the patient remotely [44] or traffic signal detection for unmanned autonomous vehicles [41]. The volume of data that may be challenging for the edge nodes to analyze is pushed to the cloud for more complex data analysis [45,46]. Machine learning (ML) algorithms are usually employed to provide long-term predictive decisions [47].

Decision-Making in Edge Data Analytics

Data analytics and decision management are two critical components of decision-making. The report generated from data analytics is used by the decision management component to identify what decisions should be made. For example, in traffic management applications, information about traffic density, vehicle-specific data, and movement of other vehicles and pedestrians are collected to perform quick data analytics and generate decisions on traffic flow. Hence, agility in decision-making triggers the business process, resource utilization, and customer satisfaction. Based on agility, decision-making is divided into predictive and reactive models: (i) Predictive models rely on the cloud to collect large amounts of data and perform long-term data analysis to identify the best decisions. They evaluate decisions based on various policies in the applications and improve the predictive analysis over time. (ii) Reactive models respond to an event with reactive decisions within a short time interval. These models achieve real-time support without focusing on what the system might look like in the future. The key characteristics of real-time support are the most suitable for edge computing applications. To obtain a decision at an adequate response time, edge nodes have to be placed closer to IoT devices [48]. Whether services need to be placed on the cloud or edge is an optimization problem [49].

However, when edge nodes are scattered and placed closer to IoT devices, monitoring these nodes will be challenging. Geographical factors, such as network infrastructure and regulatory environments, significantly influence the design and deployment of edge security solutions [50]. In regions with limited network infrastructure, edge security solutions must adapt to unreliable or slow connectivity, potentially requiring decentralized architectures to ensure data processing and threat detection can occur locally [51]. Regulatory environments, such as GDPR (General Data Protection Regulation) or HIPAA (Health Insurance Portability and Accountability Act of 1996), dictate strict requirements for data privacy and security, impacting how data are stored, processed, and transmitted in edge computing environments [52]. Compliance with these regulations may necessitate additional encryption measures, data residency requirements, or auditing protocols in the design of edge security solutions. Moreover, variations in network latency due to geographical distances can affect the responsiveness of security measures, prompting the

optimization of algorithms or deployment strategies to accommodate latency-sensitive applications. Additionally, geographical factors influence physical security considerations, as edge devices deployed in remote or inaccessible locations may require robust physical protection against tampering or unauthorized access [53]. Overall, accounting for geographical factors is essential in designing and deploying effective edge security solutions that address the unique challenges posed by different environments. Intruders can easily compromise and gain access to the edge layer, and thus they can mine or steal data that are exchanged among edge nodes [54]. In cloud computing, there are regulations and obligations for data protection, as per the European Commission [38]. However, no such standards exist in edge computing, which makes them vulnerable to security attacks. In the next section, the security models that affect decision-making and the normal functioning of an application are reviewed.

3. Security Threats during Edge Data Analytics

Security threats during edge data analytics can render edge infrastructure vulnerable to attacks or create breaches that could be exploited later. Compared to traditional data processing environments, such as data centers or cloud platforms, security measures in edge data analytics primarily focus on centralized servers and network infrastructure [55]. However, in edge data analytics, where processing occurs closer to the data source on distributed devices, unique security challenges arise, including physical security threats, such as theft or tampering of edge devices, network security threats, such as Man-In-The-Middle attacks on data transmitted between edge devices and central servers, and device compromise risks due to limited resources and security features on edge devices [56]. Additionally, edge data analytics introduces specific concerns related to data privacy and integrity, as sensitive data are processed locally at the edge, emphasizing the importance of securing data at the source.

Security breaches in edge data analytics can have severe consequences for data privacy and system integrity, potentially violating regulations such as GDPR or HIPAA [57]. Unauthorized access or exposure of sensitive data can result in legal penalties, loss of trust, and reputational damage [58]. Integrity breaches can lead to inaccurate insights, posing risks to safety in critical systems [59]. Data manipulation can deceive users or automated systems, impacting decision-making [60]. Service disruptions may occur, impacting business continuity and customer satisfaction, while financial losses can stem from remediation costs, regulatory fines, and revenue loss. Intellectual property theft can undermine competitiveness and innovation [61].

Appropriate threat models are used to safeguard applications against attacks, representing the system it is running on, the users, and potential attackers. The growing number of research articles on security, privacy, and threats underscores the importance of addressing these issues in evolving edge computing applications. Table 2 summarize the related studies by following the Open Fog reference architecture presented by the Industrial Internet Consortium that categorizes threats based on attack venues: insider attack, software attack, hardware attack, and network-based attack, all of which violate confidentiality, integrity, authentication, availability, and data privacy.

Insider attack: An insider attack is caused by authorized users intentionally misusing the system and network to exploit. The majority of threats occur due to insider attacks [62]. Once the user gains access to the organization, it is effortless to implement an insider attack. There are very few opportunities to detect and prevent attacks. Host-based and network-based detection techniques are used in cloud computing to identify insider attacks [63].

Hardware attack: In a hardware attack, the attacker gains physical access to the system to obtain the information or modify its behavior. In many cases, covert or overt are the two types of hardware attacks [36]. Covert attacks are when the victim is unaware of the attack, and overt attacks are when the victim is aware of the attack on the system. A side-channel attack is a typical covert attack.

A hardware attack's main intention is to disrupt the normal working of the hardware or deny services, leading to system security failures [64].

Software attack: Software attacks are considered an indirect attack in many cases, as the attack is against software modules that run on a system. The attackers usually know the inner workings to launch an attack [65]. The attacker extracts information by introducing rogue applications or trojan horses in the system [66].

Network attack: A network attack is the most common attack that bypasses the security mechanisms of the victim. The attackers identify loopholes, bugs, and misconfigurations in the services and disturb normal network activities. Usually, the attacker launches this attack in four steps: gather network vulnerability information, compromise any nodes in the network, attack using a compromised node, and finally, clear the attack history in the activity log [67].

Table 2. Classification of threats.

Types	Ref.	Threats	Definition	Impact on the Edge Nodes and Networks
Insider or Malicious Attack	[68]	Data Breach	Illegal data access and data leak	Disclosure of confidential and sensitive data to an unauthorized person
	[69]	Hacking	Illegitimate users modifying or altering the edge and user data	Loss of data integrity, manipulation of decision-making, and disturb the normal functioning of the application
	[70]	Identity and Password Leak	Illegally hacked username and password to gain access to the application	Gain unrestricted access to the application and misuse of sensitive information
	[63]	Malicious Insider	Illegally access the network and control all the nodes	Behave legitimately and take advantage of the services
Hardware Attack	[71]	Forgery	Forge the identities and profiles	Generate fake information and mislead other users. Consumemore bandwidth, storage, and energy
	[72]	Jamming	Blocking communication channel	Loss of data or increased data transmission rate
	[73]	Side-Channel Attack	Deliberately block communication channel	Falsification of data and increased computation time
	[74]	Resource Depletion	Flood traffic and saturated storage or network resources	Affects data processing and delays decision-making due to a lack of resources
	[75]	Equipment Sabotage	Deliberately create resource deficiency	Damage resources and disturb real-time services
Software Attack	[76]	DoS attack	Disruption of edge nodes, hardware devices, or software applications	Consume more node resources, disrupt network operations, and generate false messages
	[77]	SQL Injection	Inject code to access sensitive data	Modify sender data or fabricate new malicious data to affect data confidentiality
	[78]	Impersonation	Claim to be an alternative user by using a forged character	Acquire illegitimate benefits and access confidential data with malicious intentions
	[14]	Tampering	Unauthorized entities intentionally modifying data	Causes privacy leakage, hijacks services, or creates other attacks
	[79]	Eavesdropping	Illegally gain access to the network and listen to the network communication	Hack users' data and intercept communication channels to degrade efficiency
	[80]	Message Replay	Illegitimate user sending authorized messages in the network	Compromises other nodes and exposes sensitive data
Network Attack	[81]	Spoofing	Fake users repetitively requesting services	Divert communication channel toward attackers' destination. Consumes more bandwidth and increases processing times
	[14]	Man-In-The-Middle	An illegitimate insider in the network with malicious intention	Steal users' credentials, attack communication channels, or alter data
	[82]	Flooding	Generate enormous illegitimate messages and increase network traffic	Disrupt the network and prevent legitimate users from accessing the network
	[77]	Pattern Analyses	Intercepting and examining the data flow and network pattern in the communication channels	Gain unauthorized access to the network and steal data
	[83]	Spamming	Send spontaneous messages to all the nodes requesting services	Collect user credentials and gain access to the network
	[84]	Sybil	Create a fake identity and gain access to the network	Acquire privileged access to the services
	[85]	Sinkhole attack	The malicious node sends a fake message and establishes a connection with a legitimate node	Creates maximum traffic flow and makes adjoining nodes collide. Increases bandwidth, leading to resource contention and message destruction

4. Motivating Use Case Applications

Various industries, including healthcare, transportation, and smart cities, leverage edge data analytics to derive real-time insights and enhance operational efficiency [86]. In healthcare, edge computing facilitates remote patient monitoring, medical imaging analysis, and wearable health devices, while facing security challenges related to patient data confidentiality, regulatory compliance, and medical device security [87]. In transportation, edge data analytics enables real-time traffic monitoring, predictive maintenance, and autonomous vehicle operations, posing security challenges such as protecting connected vehicles from cyberattacks and ensuring the integrity of navigation data [88]. In smart cities, edge computing supports smart energy management, public safety monitoring, and urban infrastructure optimization, with security challenges including safeguarding citizen data privacy and protecting critical infrastructure against cyber threats [89]. Addressing these unique security challenges requires industry-specific security measures, robust encryption, access controls, and ongoing security assessments to ensure the integrity and security of edge data analytics deployments across various industries.

The integration of edge computing for smart applications can improve the user experience by enhancing the computing efficiency. This has resulted in adopting edge computing for various use cases, including healthcare, traffic management, and smart city applications. In this section, the use cases are reviewed and tabulated in Table 3. The use cases are studied in the following section to understand the edge aspect of the applications, the working model, and how they contribute toward decision-making. Any attacks on these applications will adversely affect the decision-making process by falsifying information, hacking confidentiality, and privacy, and all these are studied further.

4.1. Healthcare Applications

The use of healthcare applications is rapidly increasing since they offer mobility, regular monitoring, periodic updates, and real-time interactions during an emergency. In many healthcare applications, typical end-users are elderly patients who require special attention and supervision. They use devices, such as smartwatches or smart glasses, with various sensors, accelerometers, gyroscopes, and GPS. These devices are interconnected and process patients' information, which requires high levels of privacy and integrity.

In the present context, COVID-19 is a fast-spreading chronic illness that requires monitoring of infected patients to control the rapid spread. Artificial intelligence (AI)-integrated edge computing is proposed to provide real-time processing of a patient's health data to predict whether the patient is infected or not [90]. The edge node contains AI units and a medical database capable of collecting, storing, processing, and generating alert messages. The AI unit uses ensemble-based techniques to perform clinical diagnoses and generate alert messages. The decision is based on the risk score estimated using an AI model. This triggers an alert message to the doctors and assists them in taking immediate action to quarantine the infected patients. Although AI supports the overwhelming decision-making process, it is proven that AI increases the computation load on the devices. In case of any attack on AI models, they become vulnerable to threats and lose their reliability [91]. This may result in delaying the alert message to the doctors and degrading the efficiency of the application. Similar applications were proposed for the Chikungunya virus diagnosis. This application uses Social Network Analysis (SNA) to predict the virus outbreak. SNA graphs generate relative scores for each region and identify the critical region. Based on this, appropriate alert messages are generated [92]. Cancer prediction and monitoring applications use data gathered in the healthcare system for decision-making based on neuromorphic multi-criteria [93]. These decisions help the specialist to determine the level of symptoms and provide quality services. There are several instances where cancer patients' data were hacked through cyber-attacks [94].

There are few fall detection applications available for patients suffering from stroke [95,96]. In these applications, sensors, edge gateways, and access points are interconnected in the Low-Power Wide-Area Network (LPWAN). They monitor electroencephalography (EEG),

electrocardiography (ECG), electromyography (EMG), blood pressure, and contextual data, such as temperature, humidity, and air quality. The combination of health data and contextual data assists in improving the accuracy of prediction. Low Bluetooth energy in LPWAN reduces latency during data transmission. When the fall is detected, a notification via smartphone is sent to the caregivers. However, if the body blocks the electromagnetic signal transmissions in some postures, it may either reduce the quality of the link or make communications within body devices impossible [97].

eWall is an advanced home sensing environment with e-health and e-solution for elderly patients to live independently. Elderly patients may suffer from declining memory functions, cardio-pulmonary conditions, neuro-muscular control movements, and so on. This application provides an effective solution to address all these societal challenges. It includes: (i) eWall devices, such as sensors and actuators, (ii) home sensing middleware to connect devices, collect, query, report, and store data, (iii) a local context manager to analyze human and non-audio/video perception processing, and (iv) a cloud to monitor complete infrastructure communication. The services provided by this application are daily activity monitoring (such as jogging, cycling, and gardening), daily functions' monitoring (such as shopping, walking in the park, cooking, sleeping, eating/drinking, socializing, mood status, self-care, and chores), healthcare support through teleconference with a medical professional, and caregiver notifications. Ubiquitous devices, such as sensors, accelerometers, gyroscopes, GPS, utility sensors (such as gas, electricity, and bed), passive infrared (PIR), and audio/video sensors are interconnected with Bluetooth or Zigbee technology to provide these services. The data transmission rate in this technology is very low [98]. The health Fog framework is another application where hospitals, clinics, and smart homes are equipped with sensors, actuators, smartphones, and other smart devices. Medical professionals monitor patient's sedentary lifestyle, which affects their health, and advise physical routines, diets, and other plans to pursue a healthy lifestyle. This is a patient-centric application to improve human health and well-being with suitably engaging technologies [99].

In the healthcare system, implementing security measures entails several ethical considerations. These include safeguarding patient data privacy and confidentiality, obtaining consent for data usage, ensuring patient data ownership and control, addressing biases in algorithms, promoting transparency and accountability, and prioritizing patient safety [100]. However, in healthcare applications, since devices are connected in WPAN (Wireless Personal Area Network) or BAN (Body Area Network), this makes the network vulnerable to potential attackers who can anonymously sneak into the devices, listen to all traffic, hack personal data, and exploit the system [101]. Common threats identified in healthcare applications include insider attacks, software attacks, and hardware attacks. Among these, insider attacks cause severe damage because the attacker pretends to be legitimate and can take control of the communication channel or devices [102].

Observation #1: The quality of medical services is improving tremendously due to the integration of AI and edge computing. The health applications are serving as a powerful tool for the medical field to monitor and control the spread of fatal diseases. Despite these advantages, as the data volume increases, AI computation tasks increase. This can drain the computation, network, and storage capacities of the edge infrastructure and affect its performance or reliability.

Observation #2: The sensors and the devices in the healthcare applications are connected in WPAN, Bluetooth, ZigBee, or WBAN. Even though these networks are energy efficient, they have a lower network range than Wi-Fi and cellular connections. This may decrease the necessary bitrate for biomedical signals, such as ECG or EEG. If the patient wears several body sensors, the transmission of electromagnetic signals may become blocked due to some body postures affecting data transmission.

4.2. Traffic Management Applications

VANET (Vehicular ad hoc Network) and VSDN (Vehicular Software-Defined Networking) are the standard networks used in most edge-based traffic management applications. The importance of these networks is to improve driving efficiency, navigation, and information exchange in a decentralized network structure. A Vehicular Fog Computing (VFC) network enables traffic schemes for traffic management and road safety in a decentralized network structure. Events such as traffic jams, car accidents, and road surfaces are uploaded to edge nodes, which are closer to the roadside units. Some data generated at this level can be used for vehicle-level decision-making, while other data are processed by the servers in the edge layer and pushed to the cloud. The traffic management server on the cloud is responsible for broadcasting feedback messages to vehicles through the edge nodes at roadside units [103]. When the data are transmitted to different nodes, a lack of authentication can lead to malicious activities, such as hacking users' personal data or affecting the consistency of data [104].

A vehicular network collaboration using VSDN is used to assist various services, such as autonomous driving, collision avoidance, accident detection, fast rescue, emergency traffic prioritization, emergency message dissemination, remote video analysis, and so on. This technique enables handling most of the software attack efficiently, but tracking location and a few network attacks, such as sinkhole, sniffing, and spoofing, are challenging [105,106]. The vehicles behave as a content provider or consumer simultaneously, so tracking them for process discovery or process request is very easy. Once these vehicles are tracked, they can be easily made unreachable and isolated from the network [107]. The virtualization in VANET is still evolving and there are no standards to integrate wireless communication mechanisms, as in IPv6. Therefore, they are more prone to attacks such as DDoS and network pattern analysis [108].

The 5G-based intelligent transport system was developed to track traffic violation reports using vehicles' speed sensors. It was based on security protocol to verify location-based information with a digital signature [109]. The edge nodes aggregate multiple speed violation reports, verify, and broadcast anonymous notifications to other entities in the vicinity. Considering these reports, the transportation authority generates the decisions on vehicles' traffic violations. The digital signature mitigates the risk of jamming, privacy violation, and false injection threats. Hence, the privacy of information and location, mutual authentication, traceability, data confidentiality, and integrity are achieved. However, hardware attacks, such as physical damage to sensor nodes or blocking communication channels, are not considered. These attacks can cause the edge nodes to wait indefinitely for the data [110].

Observation #3: In VANET, data are traversed from different nodes and regions. There is high mobility and uneven distribution of vehicles in the network. This makes selecting appropriate relay nodes challenging and results in consistency liability of data. Therefore, there is a need for an efficient correlation mechanism to address data inconsistency.

Observation #4: The 5G, SDN, and virtualization technologies are broadly adopted in VANET applications. They support traffic programmability, agility of services, and create policy-driven network supervision. However, it will be challenging to achieve reliability, abstraction, performance, scalability, and security by virtualizing the network infrastructure for edge computing.

4.3. Smart City Applications

Smart city applications have enhanced the living standards of the users [111]. IoT devices play a vital role in these applications to collect and sense real-time data. They collect users' data pertaining to city supervision and utilities (gas, lighting, etc.). In a video summarizing framework, the edge nodes collect the captured videos and create an embedded vision. Further, it is pushed to the centralized servers in the edge layer connected through internet gateways. The servers operate as master nodes, and these master nodes control the edge nodes. The servers offload the embedded vision to the cloud

through the MQTT communication protocol. The embedded vision reduces bandwidth consumption to the cloud significantly [112]. The MQTT protocol is prone to many threats, such as DoS, flooding, spoofing, tampering, and denying access control [113]. These threats result in maliciously dropped or delayed information, capture of transmitted data, send infinite false details, contribute to degrading decision-making efficiency, and block the resource for processing nodes [113].

A smart meter application is used to collect data on energy consumption. The collected data are aggregated by the edge nodes and transferred to the cloud. The edge computing layer includes smart meters to sense data, distribution transformers in the respective geographic region, and a meter data management system at the substation level. The data management system performs distributed data aggregation to summarize data before sending it to the cloud. The routing protocols are used to transfer the data with multiple hops to the destination [114]. The routing protocols can be prone to attacks, such as eavesdropping, network pattern analysis, jamming, spoofing, data alteration, message replay, and DoS [115]. In a smart lighting application, the controller node monitors the streetlight switches when vehicles are approaching [116]. The smart lighting is further enhanced by interconnecting to a smart city system for public safety. It includes various sensors, such as a video camera or gun-shot detection sensor, and datasets such as weather or traffic data. This application helps users to navigate the safest route based on pedestrian count and road traffic. Google map API is used to assist navigation for the users. In case of an emergency, such as accidents or theft, the users can press the emergency call button and streetlights begin to pulse immediately. The responder can locate the emergency by identifying pulsing streetlights nearby. The brightness of the streetlights and pulse are between 10% to 100%, making it visible to pedestrians and emergency responders. This application also includes secure communication protocols to mitigate cybersecurity threats, such as DoS, eavesdropping, session hijacking, and MITM [117]. Similarly, in the smart pipeline application, the controller node detects a fire or gas leak and closes the gas pipeline. Fiber optic sensors and sequential learning algorithms on edge nodes are used to detect events threatening pipeline safety [118]. The common threats anticipated are equipment sabotage, jamming, eavesdropping, tampering, and sinkhole attacks. These attacks can alter decisions, block the edge nodes from processing, or even isolate the edge nodes.

Observation #5: There are many sensors, IoT devices, and edge nodes connected in the smart city applications. They collect and process data in the long term to obtain deep sequential resolution. This advancement greatly reduces the power consumption of the devices while maintaining the same performance. Therefore, there is a need to preserve the longevity of devices and edge nodes.

Observation #6: Smart city applications continuously collect users' sensitive data for a long time and store them in the edge layer for processing before transferring them to the cloud. Any threats to the data stored can lead to catastrophic events, such as information theft or identity fraud. Lack of security measures can compromise the stored data and lead to a loss of public faith and affect the reputation of the applications.

Table 3. Analysis of edge use case applications and effects of threats on the applications.

Use Case	Ref.	Working Model	Decision Making Node	Evaluation	Insider Attack	Software Attack	Hardware Attack	Network Attack	Effect of Threats on the Model
Health Care Applications	[90]	Emergency alert message for COVID-19 infection	Artificial intelligence-based fog node	Generate medical report and alert message to caregivers and doctors	Data breach	-	Equipment malfunction	-	Hack data or may degrade alert message efficiency
	[96]	FAST—Fall detection system for stroke patients	Back-end module server on the cloud	Detects if the stroke patient is about to fall and triggers message to the emergency phone number	Forgery, MITM	Tampering	-	-	Causes false predictions, degrades efficiency, and maliciously drops or delays information
	[95]	Fall detection or electrocardiography monitoring	Edge gateway—Fall detection system	Notification and alert message to caregivers	Forgery, MITM	Tampering	-	-	May degrade notification efficiency
	[98]	eWall—Home management for senior citizens	eCloud or ePSOS	Track daily activities of an elderly patient. Alert message from eWall cloud to relatives or hospital	MITM, malicious insider	-	Resource depletion	-	Affect confidentiality, breach privacy, tamper with hardware devices, and disturb normal data flow
	[99]	Activity monitoring	Cloud Access Security Broker	Activity detection and calories burnt are sent to hospitals and nutritionists	MITM, insider, hacking	Impersonation	-	-	Affect confidentiality, privacy, and reliability of the decision
	[119]	Healthcare and Assisted Living (AAL) in Smart ambient	Fog Accelerator Nodes	Aggregate data from IoT sensors and monitor patients' fall or cardiovascular issues. In case of emergency, informs caretakers	-	SQL Injection	Equipment sabotage	-	Affect confidentiality, leak sensitive information, and destroy hardware devices
	[120]	Smart e-Healt hcare system	Gateway nodes	Gather medical information of patients from sensors, aggregate in edge layer, and generate EWS in case of emergency for doctors or caretakers	Malicious insider	Impersonation, jamming	-	-	Malicious insider can watch the activities, illegitimately communicate with other users, falsify data, or send a false alarm
	[92]	Chikungunya virus diagnosis solutions	Alert generation component in fog layer	Alert message is sent to government and healthcare to control outbreak of virus	-	-	Equipment sabotage	-	May not create an alert message or causes a delay in generating the alert message
	[93]	Detect cancer and monitor patients	Smart gateway nodes in fog layer	Send e-report to patients, send ambulance in case of emergency, and monitor patients until they recover	Data breach	-	-	Eavesdropping	Intruder may hack patients' personal data or may be a silent spectator

Table 3. *Cont.*

Use Case	Ref.	Working Model	Decision Making Node	Evaluation	Insider Attack	Software Attack	Hardware Attack	Network Attack	Effect of Threats on the Model
Traffic Management Application	[103]	Traffic Management Scheme	Cloudlets	Minimize response delay for traffic management by load balancing	Data breach, malicious insider	-	-	-	Breach data privacy
	[105]	Vehicular Network collaboration	Fog Controller Node	Accident notification and avoid road congestion Traffic prioritization in case of emergency and directs fast rescue route	Location privacy	-	Fault tolerance	Sinkhole, sniffing, spoofing	Track users' location or deprive them from the network
	[106]	Smart Traffic Control	Traffic Control Node	Identifies road congestion and avoids traffic jams	Location privacy	-	Fault tolerance	Sinkhole, sniffing, spoofing	Track users' location or deprive them from the network
	[109]	5G-based Intelligent Transport System	Transportation authority at the edge layer	Sends traffic violation report (TVR) based on the vehicle's speed sensors	-	-	Equipment sabotage, side channel attack		Physical damage to sensor nodes, blocks communication channels, and increases waiting time.
	[121]	Smart Car Parking system	Microcontroller device generates parking status	Identifies traffic jam and shows parking spots	Location privacy	-	Jamming		Track users and vehicle information, cause traffic congestion
Smart City Applications	[122]	Surveillance videos for smart cities	Fog Aggregate Nodes	Send compressed video data to the cloud	Side channel attack	Tampering	Equipment sabotage	Eavesdropping, Sybil, DDoS, pattern analysis	Maliciously drop or delay information, block the resource or request from the users, hack user privacy
	[123]	Smart things to machine interaction	Fog Controller Node	Intelligent lighting—sensor identifies when to turn the switch on/off	-	Tampering	-	-	Device tampering
	[118]	Smart pipeline monitoring system	Fog Controller Node	Closes gas pipeline in case of gas leakage or fire detection	-	Tampering	-	-	Device tampering
	[114]	Powerline communication for smart meters	Fog Computing Nodes	Summary of electric power consumption data is sent to the cloud	Data alteration	-	-	Eavesdropping, pattern analysis, jamming, DoS	Device tampering
	[124]	Forest Fire management systems	Prediction system	Identifies and generates an alert message to forest authorities	-	Tampering	-	-	Alters the decision with malicious intentions

5. Analyses of Existing Security Threat Models

As discussed in the previous section, edge computing has a potential number of applications in healthcare, traffic, and smart cities. Edge computing applications reduce the data flow to the cloud, provide uninterrupted connection, and improve the performance of the application. They also offload some part of the analytics from the cloud data center to the edge of the network, which leads to security and privacy issues. When the computation gets closer to the edge of the network, end-user devices and edge data centers become vulnerable to security threats. Therefore, it is necessary to build an expansive network with minimal vulnerabilities. This section summarizes the existing security models that have addressed the threats and built a secure edge computing layer. The findings with limitations are tabulated in Table 4. There are various mechanisms in the edge computing paradigm to handle the threats. Based on this mechanism, the available models are categorized and studied in this section.

Table 4. Review of existing threat models.

Ref	Solution Approach	Performance	Findings
[125]	Artificial neural network-based IDS	Detects malicious edge nodes based on the node's profile features. Identifies DoS, flooding, and replay attacks	High accuracy and low false alarm rate. Efficient to maintain the edge network's resilience by discarding the intruders
[126]	Identifies insider attacks using random Gossip Consensus algorithm	Detects insider attacks using edge node's state information without any supervision	Extensive resource consumption
[127]	Hierarchical Identity-Based Encryption Scheme to achieve data security	Four hierarchical layered security keys are used to secure data from the attack	Escrow key problem
[128]	Data privacy-preserving scheme based on data load forecasting	Smart meters are used to calculate the workload using the Oblivious Multivariate Polynomial valuation (OMPE) protocol and protect data from unauthorized access	Reduces computational overheads and data load to the cloud
[129]	Password-based secure communication protocol for data transmission between cloud and edge devices	Establishes secure communication based on pivotal agreement between user and edge devices. Eavesdropping, data alteration, MITM, impersonation, and malicious insider attacks are restricted	Most of the threats are addressed, and communication channels are secured. However, phishing can be used to easily hack the password
[130]	Gaussian Naive Bayesian theorem is used to analyze the packets and identify an intruder	Analyze the network using the Markov model and lure attackers using the Virtual Honeypot method	Attacker can act legitimately and gain access to the Honeypot method
[78]	Q-Learning-based reinforcement learning technique to identify impersonation attacks	Detects attack accurately in edge layer. False alarm rate, misdetection rate, and the average error rate are identified using channel state information	Channel state information can be considered to study further attacks, such as DoS, spoofing, jamming, authentication, etc. However, it is not considered in this approach

Table 4. *Cont.*

Ref	Solution Approach	Performance	Findings
[122]	Intrusion detection and intrusion prevention system	Identifies MITM attack. Interrogates communication channel using Advanced Symmetric Encryption, and exchanges keys using the Diffie–Hellman method	Not suitable for multi-hop attacks
[131]	Automated validation of Internet Security Protocols to secure Intelligent Edge-based Transport System	Generates a 64-bit symmetric key or 512-bit asymmetric key to secure communication. It is very complicated for attackers to break this key	It is impractical to assume that all vehicles are legitimate
[132]	Fault diagnosis of the hardware components	Case-based reasoning model to classify the fault type for a hydropower plant using storm-based architecture	System-specific application
[133]	Anonymous and Secure authentication scheme	Secure cryptographic algorithms are used to establish confidentially, privacy, and mutual authentication among edge nodes	Cryptographic algorithms may increase computational time
[134]	Cybersecurity framework to identify a malicious node	Identifies malicious node through Markov model and shifts that node to a Virtual Honeypot device	Efficiently traps the malicious node, but the attacker can act legitimately and gain access to the Honeypot method
[135]	Container-based map reduction protocol to secure computation	Hardware-assisted remote attestation mechanism is used to establish trusted containers	Linux containers encapsulate the application and establish trust during execution
[136]	The DDoS attack traffic system	Identifies spoofing or infinite false requests and mitigates to avoid power wastage	Challenging to implement during peak traffic
[12]	Privacy-preserving model in healthcare applications	Hybrid user profiling is used to identify the attacker and direct toward a decoy message to trap the attacker	The focus is only on multimedia data. It cannot be applied to other data
[137]	User profiling to handle data theft	Prototype-based web patterns validate the effectiveness of decoy messages in the edge layer	Decoy data generation is time-consuming
[138]	Snort-based Field Programmable Array Intrusion model	Signature-based detection through network traffic monitoring and generates an alert message	Edge networks accelerate at the generic level
[139]	A hybrid approach using machine learning	Two-stage detection: (a) identify intrusion using binary detection, and (b) detect and confirm attacks	High precision and recovery rate. Cannot classify the attack precisely
[140]	Fully automated IDS using multi-layered recurrent neural network	Detect attacks using traffic analyses engine and multi-layered recurrent neural network	Accurately identifies DoS attacks and works efficiently in real time

Table 4. *Cont.*

Ref	Solution Approach	Performance	Findings
[106]	Multi-attack IDS	Identifies abnormality using the backpropagation neural network and detects using the radial basis function	Mobile edge nodes assist to achieve high accuracy. Identifies combinations of mixed attacks
[81]	Spoofing detection using multichannel attribute	Creates clusters at edge servers using a local heuristics algorithm and identifies spoofing attacks	Clusters are created at close optimal solutions
[141]	Live data analytics with collaborative edge and cloud processing	Integrates edge computing and cloud computing to leverage their respective advantages and address the challenges of processing massive amounts of data generated by IoT devices	Resource optimization and efficient data analytics to address the challenges of handling large volumes of data and enhance network performance
[142]	Secure IoT service with an efficient balance dynamic based on cloud and edge computing	Creates new parsing templates, prioritize services with stringent demands, and ensures the reliability of IoT data transfer	Enhances trust evaluation mechanisms and collaborative strategies

5.1. Intrusion Detection System

In many security threat models, intrusion detection is the most widely adopted mechanism to identify an attack. The intrusion detection system (IDS) monitors network traffic to detect attacks and sends an alert message to the network administrator. There are two main types of IDS: anomaly-based IDS and signature-based IDS [143]. Anomaly-based IDS is based on identifying the normal system's anomalous behavior. It involves collecting data over a specific period, performing analyses, and determining whether the system's behavior is legitimate or not. The standard techniques used in anomaly-based IDS are data mining, statistical modeling, and the hidden Markov model. This approach is mainly employed when attack types are unknown and to reduce the false alarm rate [144]. Adaptive IDS is used to identify the anomalies, such as misuses, cyber-attacks, or system glitches, on the edge nodes. These anomalies can prevent data transmission on edge nodes or perform accurate automated actions. Adaptive IDS detects when the edge nodes are compromised and takes the required actions to ensure communication availability. Memory, CPU usage, and buffer utilization are the metrics used to measure against replay, flooding, and DoS attacks [125].

Signature-based IDS is based on a predefined attack pattern of an intruder stored in the system. The attack pattern is widely based on network traffic analysis. In case of any changes in the pattern, the network administrator can detect with high-level accuracy. However, this cannot be used for unknown or undefined attacks in IDS [144]. The combination of an anomaly and signature-based IDS is used to identify the patterns of attack signatures. Field Programmable Gate Arrays (FPGA) are used as edge gateway nodes, and IDS is incorporated on these nodes. FPGA are computationally intensive nodes capable of identifying when the edge network traffic changes. The Wu-Manber algorithm used in snort is used in FPGA as a signature-based IDS, while the adaptive threshold and change point detection algorithm are the two anomaly-based IDSs used. Snort is a regular expression-based engine used to identify the patterns of attack signatures [138]. Although this system efficiently identifies many attacks (DoS, SYN flooding, and port scanning), it executes at a generic level. To implement in a real-time scenario, the system's level of acceleration must be increased.

5.2. Combination of an Intrusion Detection and Intrusion Prevention System

The IDS and intrusion prevention system (IPS) methods are used together to identify an MITM attack and its variants, such as eavesdropping, packet modification, and wormhole attacks, on the edge computing layer. This system includes two types of nodes: the edge node and IDS node. When an IDS node identifies a compromised edge node or an intruder, it informs the neighboring edge nodes and disconnects the infected node. Later, to prevent the attack, IDS nodes acquire a key from the cloud and distribute it to the edge nodes to prevent intrusion. The proposed system uses the Advanced Encryption System (AES) symmetric encryption technique, and an encryption key is exchanged using the Diffie–Hellman key exchange. It is a lightweight encryption technique to periodically interrogate edge nodes that are one hop away. Even if the attacker identifies the IDS, it is challenging to predict the nature of the IPS [122]. In any wireless sensor network or ad hoc network of the edge computing layer, malicious nodes may unduly assign higher priority to source packets and lower priority to transit packets and launch a traffic remapping attack through multi-hop. These attacks are easy to launch, impossible to prevent, hard to detect, and harmful to genuine edge nodes. Thereby, the security threats posed by malicious nodes are aggravated by multi-hop [145].

5.3. Automated Intrusion Detcetion System

The automated IDS is used to identify cyber security attacks on the edge computing layer. The traffic analysis engine and recurrent neural network classification engine are deployed on the edge nodes. The traffic analysis engine preprocesses the traffic connection record leading to traffic data and classifies them as normal or attack data. Later, the recurrent neural network classification engine generates a security alarm using the backpropagation algorithm to inform the other edge nodes [140].

5.4. Machine Learning-Based Intrusion Detection System

The machine learning (ML)-based IDS is broadly adopted in a security system [146]. ML-based intelligence systems can easily detect different types of attacks according to normal and attack behaviors. Simulated annealing algorithms are incorporated on mobile edge nodes to detect anomalies and secure data transmission in edge assisted IoT applications. This ML algorithm uses backpropagation of the neural network to identify abnormal data that do not follow the characteristics of normal data. Later, the radial basis function of the neural network is used to detect multiple attacks in the periodicity of data generation [147]. Multi-channel attribute-based IDS is another approach, which uses the received signal strength, direction of arrival signal, and channel impulse response to identify spoofing on the edge network. The improved local heuristic-based cluster algorithm is used, and it reduces the edge node computational complexity compared to the single attribute detection technique [81]. Overall, it is observed that the ML-based IDS provides high detection accuracy and computational efficiency for data-based intrusion detection.

5.5. Cryptography-Based Systems

The cryptography technique is a mechanism of converting plain text into cipher text using encryption/decryption techniques and a private or public key. It protects confidential data from unauthorized access in a wireless communication network [80]. Identity-based hierarchical architecture for edge computing is proposed to provide data security in the edge layer. This architecture uses an identity-based asymmetric cryptography method that includes four phases: setup phase, extraction phase, encryption phase, and decryption phase. The unique secret key is generated to every edge node and reserves each node's security separately. The key's complexity is enhanced by using a private key to decrypt, and this key is known only to the root key generation center [127]. Combining bilinear pairing cryptography with the decoy technique is used to secure private medical data in edge-based healthcare applications. Two copies of medical data are created—original and default. The original data are secured in the cloud, while the default data are shared on the

edge layer. The default data are used in the honeypot as a decoy for the attackers. When the user requests their medical data, default data are shared. Later, user profiling, key exchange, and authentication algorithms are used to verify the authenticity of the user. After confirmation, access to the original data in the cloud will be granted [12].

A multi-encryption technique is used to establish mutual authentication between edge users and edge servers. This includes three phases: initialize, register, and authentication. Pseudonym-based encryption is used to initialize and register the user. The authentication phase uses session keys to secure communication between edge users and servers. The session keys and series of patterns are generated using elliptical curve cryptography, bilinear pairing, pseudonym-based identity-based encryption (IBE), and pseudo-random number generator (PRNG). It is challenging for the attackers to predict the pattern and break into the system [133]. The Q-learning algorithm-based security framework is another cryptography model used to identify impersonation attacks in the edge layer. The attributes of the communication channel between edge nodes and users, such as the signal strength, channel frequency response, and channel state information, are used to perceive the attack [78]. Cryptography techniques secure data transmission and prevent data theft, unauthorized data access, and system hacking in the edge layer. It will be challenging for any adversary to decrypt the private key and gain access to the system.

In identity-based cryptosystems, a private key generator (PKG) is a trusted third-party entity. It maintains the private key for all users and establishes trust in the system. This process of storing the keys is called key escrow. However, if any key is lost or compromised, then it can be used to decrypt data and permit restoring original data in an unencrypted state. This is a key escrow problem that can occur in PKG [148]. Simple cryptography techniques are based on computational infeasibility and incur too many resources to compute. Addition of cryptographic techniques in edge computing may cause processing delays in the edge computing layer [80].

5.6. Authentication Scheme in the Edge Computing Layer

The authentication scheme in the edge computing layer is the process of validating edge users, nodes, and servers who request access to the system. This prevents access of confidential information by unauthorized users and secures data from threats such as data leak, data breach, and data alteration [77]. A password-based secure communication protocol is used to establish mutual authentication among user, edge devices, and the cloud server. This protocol uses session key agreement to transmit sensitive data in the network [129]. However, password-based authentication systems are susceptible to protocol weaknesses that can be exploited by keystroke logging, Google hacking, wiretapping, and side-channel attacks. Even potentially strong passwords are prone to brute force dictionary attacks [149].

5.7. Hybrid Models

Hybrid models are used when the available models are not accurate enough to reduce instability. The state-of-the-art hybrid models present sufficiently high accuracy and attack detection rates. The hybrid binary classification method using the k-Nearest Neighbor (kNN) algorithm is used to identify DoS and its variants on the edge nodes. Each edge node performs intrusion detection locally without any interaction with the cloud and reports only the summary of detection, thus avoiding latency. Each edge node monitors network data traffic to identify malicious nodes and initiate the countermeasures [139]. This method can be adopted in any edge computing application, and based on the requirements, the IDS can be implanted on the edge nodes. The naive Bayesian classifier approach-based hybrid model is used to detect DDoS attacks in edge networks. This method combines the Markov model and Virtual Honeypot Device (VHD) to reduce the false alarm rate. The two-stage Markov model analyzes each edge device to identify attacks, and the hidden Markov model determines the future states of the devices. Based on the prediction of the future state, the edge devices are sent to the VHD [90]. The VHD is a simulated virtual

computer at the network level. It closely monitors the network and distracts the adversaries in the network by providing an early warning. The honeypots gather information through frequent interaction and notify the defender in case of attacks. However, the frequent interaction can compromise the network and make it vulnerable [150].

A similar approach is used to identify malicious edge devices in the edge computing layer [134]. The advantage of hybrid models is early detection of malicious nodes, the reduction of false alarms, and adaptability to any application framework. Similar to the VHD, decoy is another method used to provide the attacker with fake information or evidence and trap the attacker. The combination of an offensive decoy and user behavior profiling is used to identify data theft by insider attack in the edge computing layer. User access behavior profiling maintains a log of each user and validates them. When the system identifies any unauthorized access, the offensive decoy method asks challenging questions to verify authorization. It identifies the attacker based on the reply. However, generating and shuffling decoy questions may increase the run time [137].

5.8. Application-Specific Security Models

An edge computing-based fault diagnosis system is used to monitor hardware defects in hydro-power plants. This is an extension of the cloud-based system, where edge computing is used to provide parallel fault diagnosis with sufficient computational and bandwidth capacity. Edge nodes are used as a Strom-based computing unit. This creates a cluster of spout and bolt nodes, similar to the master–slave architecture. The performance of the hydro-power plant is extracted from different sensors connected to the bolt nodes. Spout nodes compare with standard fault cases stored in the database and report to the cloud in case of errors [132]. Similarly, an edge-based security framework is used for the Intelligent Traffic Light Control System. The edge nodes are used as a roadside unit to monitor specific regions and broadcast encrypted messages sent from the cloud server to vehicles [131].

5.9. Container and Consensus Protocols in Edge-Based Security Models

The container-based model is used to secure distributed computing in edge computing infrastructure. This model secures any IoT application deployed on edge computing infrastructure from hardware memory attacks and provides secure execution of application on the remote host. Linux containers are deployed on each edge node and container-based map to reduce prototypes for secure computing. It includes a remote attestation mechanism at the master node to validate the containers as a trusted node. Only trusted containers are integrated to the cluster, and un-trusted containers are discarded [151]. Hence, the protocol provides a secure and trusted execution with reasonable performance overhead. Containers in edge computing provide lightweight virtualization to support high interoperability and scalability among edge nodes with minimum performance overhead. Therefore, the containers are more suitable to enhance security in edge computing [152]. The consensus protocol is a primitive peer-to-peer message passing protocol that interacts randomly with other nodes and performs computation locally. A decentralized gossip consensus algorithm is used to identify insider attacks in neural network models. The consensus algorithm supports edge nodes to exchange information with neighboring nodes without any supervision. Considering this behavior, each node in the neural networks is trained to detect the attack online. The consensus algorithm has a significant advantage of monitoring the applications without a central controller and achieving scalability [126]. However, the consensus algorithm can increase the run time during implementation and deplete the edge nodes' resources [153].

5.10. Bridging Gap with Cloud Security

Security measures in edge and cloud computing aim to protect data integrity, confidentiality, and availability. Fundamental techniques, such as encryption, authentication, access control, and intrusion detection systems, are employed in both paradigms to mitigate

external threats and unauthorized access. However, the implementation of these measures varies between edge and cloud environments [154]. Edge computing operates in decentralized, resource-constrained settings, necessitating lightweight security solutions tailored to edge devices and networks. In contrast, cloud computing benefits from centralized management and ample computational resources, enabling the deployment of more sophisticated security measures, such as advanced threat detection algorithms [155]. While edge computing emphasizes real-time processing and proximity, cloud computing prioritizes scalability and standardization. Leveraging traditional cloud security features can enhance security within edge computing models by fortifying defenses against internal attacks, ensuring data integrity and confidentiality, and enabling dynamic resource allocation and efficient security-related tasks [156].

By leveraging both edge computing and cloud resources, the IoT service architecture dynamically balances service provision, resource allocation, and trust evaluation, leading to improved performance and adaptability [142]. In addition, integrating trust evaluation mechanisms and service templates across both cloud and edge layers further enhances security by deploying only authenticated and trusted services within the edge environment. This hybrid approach combines the robust security features of cloud computing with the agility and proximity of edge computing, addressing security challenges in IoT–cloud systems and bolstering overall security in edge computing deployments [141]. The overall security posture of edge computing infrastructure can be improved by applying security implementations from traditional cloud computing environments to edge data analytics [157].

Observation #7: The hybrid models and cryptography techniques discussed in this section include PKG to generate pseudonym keys to check authenticity and data integrity. However, the storage of these keys in edge nodes increases the transmission overhead. Further, if multiple keys are added to the edge nodes, it may cause network congestion in communication channels.

Observation #8: Adopting containers in edge computing has numerous benefits, such as lightweight, fast, more accessible to deploy, and better resource utilization. Along with this, the container also brings the complexities of optimizing edge computing infrastructure to containers, and they are vulnerable to kernel-based and container-based attacks.

5.11. Impact of Threats on Edge Data Analytics

In edge computing, highly granular data are used to perform real-time decisions and actions, referred to as edge data analytics. These actions are handled by edge nodes in the edge computing layer; in particular, edge nodes store and analyze the data gathered to perform data analysis [48]. Edge nodes are deployed in a place where there is a lack of strict protection and supervision. Thus, it becomes vulnerable to many threats and attacks that compromise the system [158]. This significantly impacts the data present in the edge layer and edge data analytics. This section summarizes the impact of the threats affecting the data analytics in the edge layer.

Data are transmitted between vehicles, vehicle to edge nodes, and edge nodes to the cloud in the traffic management applications. Deploying edge computing applications in roadside units facilitates accessibility, trust, and synchronization with sensors and edge devices. The absence of authentication on roadside units can cause malicious attacks, affecting data consistency. Inconsistent data can alter decisions during edge data analytics and disturb the normal functioning of the application [104]. In VANET, secure encryption techniques and digital signatures are used to secure systems from most software attacks. However, virtualization makes it prone to network attacks, such as spoofing, replay, DoS, flooding, and pattern analysis. These threats can expose the data stored in edge nodes, hack confidential data, and affect data integrity [159]. DoS or DDoS (Distributed DoS) are the most prevalent threats in VANET. These threats can bring down the network performance, consequently rendering the VANET unavailable. Security in edge computing requires adaptability and autonomy at the network's edge, whereas cloud computing focuses on

centralized control and scalability to safeguard vast amounts of data stored in centralized data centers [160].

In healthcare applications, security threats due to wireless sensor networks causing malicious attack are the major issues [161]. These threats affect data analysis thorough data breaches, hacking of personal data, and malicious insiders. They compromise access points and communication channels and may change the destination of packets or make routing inconsistent [13]. Similarly, when data are transmitted in WBAN, software attacks can cause threats such as eavesdropping, impersonation, data replay, or data modification. These threats can defraud adjacent edge nodes and cause system failure [101].

Finally, in smart city applications, the impacts of software, hardware, and insider attack are similar to those in healthcare and traffic applications. However, communication protocols, such as MQTT, or routing protocols can make the network more vulnerable to network attacks. For instance, in the MQTT protocol, a Denial of Service (DoS) attack can overwhelm the communication channel. This could enable attackers to compromise unsecured MQTT broker access, thereby gaining access to data stored in edge nodes or servers, escalating privileges to unauthorized users, or even tampering with edge devices. These threats can result in data modification and hijacking of communication channels, thereby affecting the data integrity [113]. Similarly, the routing protocol attacks can target MITM, sniffing, Sybil, and spoofing attacks, absorb network traffic, or inject themselves in the network, which controls the network traffic flow. They can monitor the data processing and decision-making performed by the edge nodes, thereby gaining complete control over the system [115].

6. Future Research Directions

Future research directions that could leverage the existing solutions to make further progress toward securing edge computing applications are listed below:

1. Adopting federated learning (FL) algorithms for edge data analytics—Following observation #1, the integration of AI in edge computing is widely adopted, especially in healthcare applications. It remarkably enhances the scope and computational efficiency of edge nodes [90]. However, the challenging aspects of AI models are their short battery life, power-hungry, delay-intolerant portable devices, vulnerable to security threats, and a loss of their reliability [91]. These limitations can be resolved by adopting the federated learning framework in AI models. Federated learning is an ML technique used to train data across decentralized edge devices without exchanging them with other devices. This reduces the amount of data in wireless uplinks, adapts well with heterogeneous cellular networks, and preserves privacy. Pace steering in FL is a flow control mechanism that controls data uplinks by regulating the device connection pattern [162]. FL deploys secure data aggregation mechanism, where data remains secure even in the memory to protect additional security in data centers [163]. Therefore, FL can be best applied for applications such as edge computing, where device data are more relevant, for better data transmission and to provide security.
2. Enhancing IEEE communication standards in edge-based healthcare applications—The sensors in healthcare applications are connected through BAN or WPAN. As noted in observation #2, the network may not offer necessary bitrates for biomedical signals' transmission. This will delay communication or reduce the quality of a link within body devices, especially when many body sensors are interconnected [97]. Currently, IEEE 802.15 technical standards are used in BAN or WPAN, which results in low-rate data transmission in edge data analytics, but this standard was designed for Zigbee or 6LoWPAN, whereas IEEE 802.15.6 is a standard for WBANs that helps healthcare service providers to monitor patients at any time and location. It provides human body communication with a data rate of more than 2 Mbps (Mega Bytes Per Second) and an operation band of 27 MHz (Mega Hertz). These operation bands are valid in the major European countries. Apart from that, it also provides secure communication with three different security levels through authentication and encryption. This provides

solutions for integrity, reply defense, confidentiality, privacy protection, and message authentication problems. Therefore, adopting IEEE 802.15.6 in healthcare applications can enhance the reliability, service quality, low power, data rate, and non-interference. This standard also deals with particular BAN requirements, such as security, energy consumption, range of communication, scale of the network, and data rate [164].

3. Developing a robust and efficient data dissemination technique in VANET for a node selection strategy—As noted in observation #3, in VANET it is challenging to maintain a specific topology for every vehicle due to the high mobility and uneven distribution of vehicles. Conventional routing protocols use a street-centric divide-and-conquer approach. This approach can be efficient if a succession of vehicles between the source and destination is determined in advance [165]. However, it may not be possible in a real-time scenario, as it results in unavoidable collision problems. Therefore, a robust and efficient data dissemination technique is required that considers selecting efficient relaying nodes to forward packets even when the source and destination of the vehicles are not known in advance [166]. The data dissemination technique should be aware of the vehicle topology within its coverage and monitor the changes in topology so that the data transmission between edge nodes and devices can be scheduled and secured with the assigned frame. This approach can greatly reduce the data transmission delay for edge analytics and secure the transmitted data.
4. Employing energy harvesting techniques to preserve longevity and processing capabilities of edge nodes in smart city applications—In an efficient smart city application, integrating energy harvesting techniques into edge computing for smart city applications offers a robust solution to safeguarding against data threats, ensuring the integrity, confidentiality, and authenticity of critical information. By harnessing renewable energy sources, edge devices can maintain continuous operation, facilitating real-time data analysis and threat detection. This uninterrupted surveillance capability is pivotal in detecting and mitigating potential security breaches. As noted in observation #5, high battery consumption is the most common problem in crowdsensing when actively collecting data, and this may affect the quality of data collected and the processing capabilities of edge nodes [167]. Moreover, with decentralized processing at the edge, sensitive data can be processed closer to its source, minimizing the risk of exposure during transit to centralized servers [168]. Additionally, energy harvesting supports the implementation of advanced encryption protocols and authentication mechanisms, further fortifying data security measures [102]. By combining energy harvesting with edge computing, smart city infrastructures can establish resilient defenses against evolving data threats, ensuring the trustworthiness and reliability of their systems in safeguarding citizen safety and critical infrastructure.
5. Enhancing network infrastructure in the edge layer—Different technologies, such as SD, NFV, 5G, or virtualization, can significantly bolster security measures against threats and attacks in edge data analytics. SDN and NFV enable centralized management and orchestration of network resources, allowing for dynamic and granular control over security policies and access permissions [169]. The 5G networks provide higher bandwidth, lower latency, and greater reliability, facilitating secure and real-time communication between edge devices and centralized servers [170]. Virtualization techniques enable the isolation of critical network functions and applications, limiting the potential impact of security breaches or attacks [171]. By leveraging these technologies collectively, organizations can establish resilient and adaptive network infrastructures capable of mitigating risks and ensuring the integrity, confidentiality, and availability of data in edge-based IoT environments.
6. Adopting fine-grained access control mechanisms in the edge layer—It can be noted from observation #6 that when data are stored in the edge layer for a long time before transferring them to the cloud, it can lead to any catastrophic events. This can result in data authentication and integrity issues, affecting the decision-making capabilities of the edge nodes. It is also observed that hybrid models and encryption techniques

are used to address these issues in the existing security model. However, as stated in observation #7, complex keys due to these techniques can result in network congestion in communication channels. Therefore, adopting access control mechanisms between data owners and the edge layer, which is a straightforward approach, can overcome these issues. This approach has proved to be efficient in cloud computing [172]. However, in edge computing, the access control mechanism has to be fine-grained, which supports secure collaboration, interoperability between heterogeneous devices, and enhances data tracking. At the same time, the design goals and resource constraints of edge nodes have to be considered so that it provides a lightweight and secure data analytics scheme.

7. Designing trust management models in an edge computing framework—The decentralized edge computing has a huge obstacle of collecting and managing information from various edge nodes to perform data analytics. These criteria can be distinct to various applications and services [32]. Further, edge nodes might frequently move from one area to another [10]. This movement causes challenges in establishing trust among edge nodes during data processing. Thus, designing a trust model that supports mobility and scalability is required in an edge computing framework. The trust models can be third-party models used to decrease the computation overload of the edge nodes and should manage interregional trust values through historical data to track the mobility of edge nodes.
8. Isolating the infected edge nodes in the edge computing layer—In the currently available edge threat models, malicious nodes are the common threats that affect the decision-making process. Malicious nodes can always compromise other nodes and create other attacks in the edge layer, such as DoS, repeated storage/processing requests, spoofing, or leakage of confidential data [158]. This induces security and trust risks, spreading among the edge nodes and to the whole edge layer. Therefore, a strategy needs to be developed to identify the malicious node and isolate it from the other nodes to reduce the risk of malicious nodes gaining control on the edge layer.
9. Enhancing security with emerging technologies, such as AI and blockchain—AI algorithms can play a crucial role in real-time threat detection and anomaly detection at the edge layer, continuously monitoring device behavior and network traffic to identify potential security threats. Additionally, AI-based techniques can leverage historical data to improve the accuracy and effectiveness of security measures in edge data analytics systems [173]. Furthermore, blockchain technology offers promising solutions for ensuring data integrity and enhancing trust in edge data analytics. By providing a decentralized and immutable ledger, blockchain can create tamper-proof records of data transactions, ensuring the authenticity and transparency of data collected and processed at the edge layer [174]. Moreover, blockchain facilitates secure and transparent data sharing among multiple parties in edge computing environments, preserving data privacy and confidentiality while enabling efficient collaboration [175]. Combining AI and blockchain technologies presents an exciting avenue for future research in enhancing security in edge data analytics. By integrating AI algorithms for threat detection with blockchain for secure data transactions, edge data analytics systems can achieve a higher level of security, trustworthiness, and resilience against security threats [176]. Exploring innovative approaches that leverage the synergies between AI and blockchain holds great potential for advancing the security capabilities of edge data analytics systems and addressing evolving security challenges in edge computing environments.

7. Discussion and Conclusions

Decision-making in edge computing is a critical aspect that provides data analysis at the end-user's proximity and uninterrupted real-time interactions. Real-time responsiveness has made edge computing widely adopted in many applications, such as healthcare, transportation, and smart cities. However, these services on the edge layer are prone

to security threats by compromising the edge nodes and affecting edge data analytics' efficiency. In this paper, we presented the basic concepts and features of edge data analytics and analyzed the working aspects with three use cases. The potential security threats and privacy issues that occur during data analytics were also analyzed to understand how they might degrade the efficiency. Further, we identified the limitations and challenges in existing security threat models.

The edge computing applications include a wide range of sensors and ubiquitous devices to collect and store data. They function uninterruptedly to provide deep progressive resolution, so it is required to preserve their endurance. When data are traversed from different nodes and regions in the edge layer, the crowdsensing mechanism should establish an efficient correlation to achieve data consistency and support reliable edge data analytics. New technologies, such as AI, SDN, NFV, and containers, are widely adopted in edge computing to provide agile services. However, they can burden edge nodes in computation and make them vulnerable to new security issues. Hence, cautionary measures should be considered before integrating edge computing with these technologies.

Advancing edge security presents several key challenges and opportunities. These include addressing the heterogeneity and scalability of edge environments, managing resource constraints on edge devices, and adapting to the dynamicity and mobility inherent in edge computing. Ensuring data privacy and trust while maintaining interoperability and regulatory compliance are also critical aspects. Interdisciplinary approaches involving computer science, cybersecurity, networking, and regulatory compliance are essential to develop scalable, adaptive, and privacy-preserving security mechanisms tailored to the unique characteristics of edge computing environments. Collaboration between researchers from diverse domains, integration of techniques from machine learning and cryptography, and engagement with policymakers are crucial for effectively addressing these challenges and seizing opportunities for innovation in edge security. Considering these key research challenges or limitations of the current research and research trends, it is critical to develop and design security models that secure data on the edge layer and, in turn, complement the edge computing characteristics.

Author Contributions: Conceptualization, P.M. and R.A.-a.; methodology, G.A.; validation, M.F.A.; formal analysis, G.A.; resources, M.A.; writing—original draft preparation, P.M. and R.A.-a.; writing—review and editing, P.M., R.A.-a., G.A., A.A.A., M.F.A. and M.A.; visualization, P.M.; supervision, A.A.A.; project administration, R.A.-a. and G.A.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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 conflict of interest.

References

1. Yahuza, M.; Bin Idris, M.Y.I.; Wahab, A.W.B.A.; Ho, A.T.S.; Khan, S.; Musa, S.N.B.; Taha, A.Z.B. Systematic review on security and privacy requirements in edge computing: State of the art and future research opportunities. *IEEE Access* **2020**, *8*, 76541–76567. [CrossRef]
2. Hu, P.; Dhelim, S.; Ning, H.; Qiu, T. Survey on fog computing: Architecture, key technologies, applications and open issues. *J. Netw. Comput. Appl.* **2017**, *98*, 27–42. [CrossRef]
3. Röckl, J.; Wagenhäuser, A.; Müller, T. Veto: Prohibit Outdated Edge System Software from Booting. In Proceedings of the International Conference on Information Systems Security and Privacy, Lisbon, Portugal, 22–24 February 2023; pp. 46–57. [CrossRef]
4. Rajkumar, V.S.; Stefanov, A.; Musunuri, S.; de Wit, J. Exploiting Ripple20 to Compromise Power Grid Cyber Security and Impact System Operations. *IET Conf. Proc.* **2021**, *2021*, 3092–3096. [CrossRef]
5. Yang, K.; Jia, X. Data storage auditing service in cloud computing: Challenges, methods and opportunities. *World Wide Web* **2012**, *15*, 409–428. [CrossRef]
6. Satyanarayanan, M. The emergence of edge computing. *Computer* **2017**, *50*, 30–39. [CrossRef]

7. Zeyu, H.; Geming, X.; Zhaohang, W.; Sen, Y. Survey on Edge Computing Security. In Proceedings of the 2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering, ICBAIE, Fuzhou, China, 12–14 June 2020; pp. 96–105. [CrossRef]
8. Aljumah, A.; Ahanger, T.A. Fog computing and security issues: A review. In Proceedings of the 2018 7th International Conference on Computers Communications and Control, ICCCC 2018, Oradea, Romania, 8–12 May 2018; pp. 237–239. [CrossRef]
9. Kumar, K.S.; Chythanya, K.R.; Jamalpur, B.; Kumar, K.S.; Harshavardhan, A. Contemporary Applications of Fog Computing along with Security Problems and Solutions. *J. Study Res.* **2019**, *XI*, 116–142.
10. 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]
11. Zhang, J.; Chen, B.; Zhao, Y.; Cheng, X.; Hu, F. Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues. *IEEE Access* **2018**, *6*, 18209–18237. [CrossRef]
12. Al Hamid, H.A.; Rahman, S.M.M.; Hossain, M.S.; Almogren, A.; Alamri, A. A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility with Pairing-Based Cryptography. *IEEE Access* **2017**, *5*, 22313–22328. [CrossRef]
13. Khan, S.; Parkinson, S.; Qin, Y. Fog computing security: A review of current applications and security solutions. *J. Cloud Comput.* **2017**, *6*, 19. [CrossRef]
14. Ni, J.; Zhang, K.; Lin, X.; Shen, X.S. Securing Fog Computing for Internet of Things Applications: Challenges and Solutions. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 601–628. [CrossRef]
15. Gupta, M.; Sandhu, R. Authorization Framework for Secure Cloud Assisted Connected Cars and Vehicular Internet of Things. In Proceedings of the 23rd ACM on Symposium on Access Control Models and Technologies, Indianapolis, IN, USA, 13–15 June 2018; ACM: New York, NY, USA; pp. 193–204. [CrossRef]
16. Roman, R.; Lopez, J.; Mambo, M. Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. *Future Gener. Comput. Syst.* **2018**, *78*, 680–698. [CrossRef]
17. Yousefpour, A.; Fung, C.; Nguyen, T.; Kadiyala, K.; Jalali, F.; Niakanlahiji, A.; Kong, J.; Jue, J.P. All one needs to know about fog computing and related edge computing paradigms: A complete survey. *J. Syst. Archit.* **2019**, *98*, 289–330. [CrossRef]
18. Shropshire, J. Extending the cloud with fog: Security challenges & opportunities. In Proceedings of the 20th Americas Conference on Information Systems, AMCIS 2014, Savannah, GA, USA, 7–9 August 2014; pp. 1–10.
19. Stojmenovic, I.; Wen, S.; Huang, X.; Luan, H. An overview of Fog computing and its security issues. *Concurr. Comput. Pract. Exp.* **2016**, *28*, 2991–3005. [CrossRef]
20. Varghese, B.; Wang, N.; Bermbach, D.; Hong, C.-H.; De Lara, E.; Shi, W.; Stewart, C. A Survey on Edge Performance Benchmarking. *ACM Comput. Surv.* **2021**, *54*, 1–33. [CrossRef]
21. Maheswari, K.; Bhanu, S.S.; Nickolas, S. A Survey on Data Integrity Checking and Enhancing Security for Cloud to Fog Computing. In Proceedings of the 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India, 5–7 March 2020; pp. 121–127. [CrossRef]
22. Tourani, R.; Bos, A.; Misra, S.; Esposito, F. Towards security-as-a-service in multi-access edge. In Proceedings of the 4th ACM/IEEE Symposium on Edge Computing, Arlington, VA, USA, 7–9 November 2019; ACM: New York, NY, USA, 2019; pp. 358–363. [CrossRef]
23. Caprolu, M.; Di Pietro, R.; Lombardi, F.; Raponi, S. Edge Computing Perspectives: Architectures, Technologies, and Open Security Issues. In Proceedings of the 2019 IEEE International Conference on Edge Computing, EDGE 2019—Part of the 2019 IEEE World Congress on Services, Milan, Italy, 8–13 July 2019; pp. 116–123. [CrossRef]
24. Ashraf, M.U.; Ilyas, I.; Younas, F. A Roadmap: Towards Security Challenges, Prevention Mechanisms for Fog Computing. In Proceedings of the 2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Swat, Pakistan, 24–25 July 2019; pp. 1–9. [CrossRef]
25. Subramaniam, P.; Kaur, M.J. Review of Security in Mobile Edge Computing with Deep Learning. In Proceedings of the 2019 Advances in Science and Engineering Technology International Conferences (ASET), Dubai, United Arab Emirates, 26 March–10 April 2019; pp. 1–5. [CrossRef]
26. Martin, B.A.; Michaud, F.; Banks, D.; Mosenia, A.; Zolfonoon, R.; Irwan, S.; Schrecker, S.; Zao, J.K. OpenFog security requirements and approaches. In Proceedings of the 2017 IEEE Fog World Congress (FWC), Santa Clara, CA, USA, 30 October–1 November 2017; pp. 1–6. [CrossRef]
27. Lioliou, P.; Lazaridis, G. Security and Privacy in Edge, Fog Computing and Internet of Things Applications: A Review. 2020. Available online: https://d1wqtxts1xzle7.cloudfront.net/63284174/Security_and_Privacy_in_Edge__Fog_Computing_and_Internet_of_Things_applications_A_review20200512-111442-timb6r-libre.pdf?1589288892=&response-content-disposition=inline;+filename=Security_and_Privacy_in_Edge_Fog_Computi.pdf&Expires=1709613571&Signature=Tl90PkqJ1ONhYgA5xciRwsYxK3MQDiLI67T3cpbnoPJIPLP4aTpU5edfpkKuV9GuGDFuceBdpHl8K4ZvZiPG1pIjFymEKTh6iU124Ziitf2zJjEip5o8jdcFavdJii2Zwu7WPrNsee74krrQZHQ3xHjxIVTmS2cMKU~EKSaBsIqB-TXkUkqwTiQ7211P-hWXF-lTQrW2cTopJGlrZhMpTLX-HH2T8meicAmqAhnVTI5dCcF3yuxSm4JCFX6tnhlSwe7Cko0yAyTG0-IBfWN9ww-yLWgA6FQbS4S5X~gMm-fO7GJ2~20Sv2GMlX5L9PQugDsAi5nFKq1qmH2G2Q3wfA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA (accessed on 23 February 2024).

28. Kunal, S.; Saha, A.; Amin, R. An overview of cloud-fog computing: Architectures, applications with security challenges. *Secur. Priv.* **2019**, *2*, e72. [CrossRef]
29. Kumari, A.; Tanwar, S.; Tyagi, S.; Kumar, N.; Parizi, R.M.; Choo, K.R. Fog data analytics: A taxonomy and process model. *J. Netw. Comput. Appl.* **2019**, *128*, 90–104. [CrossRef]
30. Guan, Y.; Shao, J.; Wei, G.; Xie, M. Data Security and Privacy in Fog Computing. *IEEE Netw.* **2018**, *32*, 106–111. [CrossRef]
31. Rauf, A.; Shaikh, R.A.; Shah, A. Security and privacy for IoT and fog computing paradigm. In Proceedings of the 2018 15th Learning and Technology Conference (L&T), Jeddah, Saudi Arabia, 25–26 February 2018; pp. 96–101. [CrossRef]
32. Mukherjee, M.; Matam, R.; Shu, L.; Maglaras, L.; Ferrag, M.A.; Choudhury, N.; Kumar, V. Security and Privacy in Fog Computing: Challenges. *IEEE Access* **2017**, *5*, 19293–19304. [CrossRef]
33. Shirazi, S.N.; Gouglidis, A.; Farshad, A.; Hutchison, D. The extended cloud: Review and analysis of mobile edge computing and fog from a security and resilience perspective. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 2586–2595. [CrossRef]
34. Lee, K.; Kim, D.; Ha, D.; Rajput, U.; Oh, H. On security and privacy issues of fog computing supported Internet of Things environment. In Proceedings of the 2015 6th International Conference on the Network of the Future (NOF), Montreal, QC, Canada, 30 September–2 October 2015; pp. 1–3. [CrossRef]
35. Hashem, I.A.T.; Yaqoob, I.; Anuar, N.B.; Mokhtar, S.; Gani, A.; Khan, S.U. The rise of "big data" on cloud computing: Review and open research issues. *Inf. Syst.* **2015**, *47*, 98–115. [CrossRef]
36. Dautov, R.; Distefano, S.; Bruneo, D.; Longo, F.; Merlino, G.; Puliafito, A. Data processing in cyber-physical-social systems through edge computing. *IEEE Access* **2018**, *6*, 29822–29835. [CrossRef]
37. Zhang, J.; Ma, M.; He, W.; Wang, P. On-demand deployment for IoT applications. *J. Syst. Archit.* **2020**, *111*, 101794. [CrossRef]
38. Tychalas, D.; Karatza, H. A Scheduling Algorithm for a Fog Computing System with Bag-of-Tasks Jobs: Simulation and Performance Evaluation. *Simul. Model. Pract. Theory* **2020**, *98*, 101982. [CrossRef]
39. Bonomi, F.; Milito, R.; Zhu, J.; Addepalli, S. Fog computing and its role in the internet of things. In *The First Edition of the MCC Workshop on MOBILE Cloud Computing—MCC'12*; ACM Press: New York, NY, USA, 2012; p. 13. [CrossRef]
40. Nikouei, S.Y.; Xu, R.; Nagothu, D.; Chen, Y.; Aved, A.; Blasch, E. Real-Time Index Authentication for Event-Oriented Surveillance Video Query using Blockchain. In Proceedings of the 2018 IEEE International Smart Cities Conference (ISC2), Kansas City, MO, USA, 16–19 September 2018.
41. Ouyang, Z.; Niu, J.; Ren, T.; Li, Y.; Cui, J.; Wu, J. MBBNet: An edge IoT computing-based traffic light detection solution for autonomous bus. *J. Syst. Archit.* **2020**, *109*, 101835. [CrossRef]
42. Wen, Z.; Yang, R.; Garraghan, P.; Lin, T.; Xu, J.; Rovatsos, M. Fog orchestration for IoT Services: Issues, Challenges and Directions. *IEEE Internet Comput.* **2017**, *21*, 16–24. [CrossRef]
43. Dsouza, C.; Ahn, G.-J.; Taguinod, M. Policy-driven security management for fog computing: Preliminary framework and a case study. In Proceedings of the 2014 IEEE 15th International Conference on Information Reuse and Integration (IEEE IRI 2014), Redwood City, CA, USA, 13–15 August 2014; pp. 16–23. [CrossRef]
44. Dou, C.; Zhang, S.; Wang, H.; Sun, L.; Huang, Y.; Yue, W. ADHD fMRI short-time analysis method for edge computing based on multi-instance learning. *J. Syst. Archit.* **2020**, *111*, 101834. [CrossRef]
45. Alkawsi, G.; Al-Amri, R.; Baashar, Y.; Ghorashi, S.; Alabdulkreem, E.; Tiong, S.K. Towards lowering computational power in IoT systems: Clustering algorithm for high-dimensional data stream using entropy window reduction. *Alex. Eng. J.* **2023**, *70*, 503–513. [CrossRef]
46. Al-Amri, R.; Murugesan, R.K.; Almutairi, M.; Munir, K.; Alkawsi, G.; Baashar, Y. A Clustering Algorithm for Evolving Data Streams Using Temporal Spatial Hyper Cube. *Appl. Sci.* **2022**, *12*, 6523. [CrossRef]
47. Varghese, B.; Gohil, B.N.; Ray, S.; Vega, S. Research challenges in query processing and data analytics on the edge. In Proceedings of the CASCON 2019 Proceedings—Conference of the Centre for Advanced Studies on Collaborative Research—Proceedings of the 29th Annual International Conference on Computer Science and Software Engineering, Toronto, ON, Canada, 4–6 November 2019; pp. 317–322. [CrossRef]
48. Bellavista, P.; Berrocal, J.; Corradi, A.; Das, S.K.; Foschini, L.; Zanni, A. A survey on fog computing for the Internet of Things. *Pervasive Mob. Comput.* **2018**, *52*, 71–99. [CrossRef]
49. Brogi, A.; Forti, S.; Guerrero, C.; Lera, I. How to place your apps in the fog: State of the art and open challenges. *Softw.—Pract. Exp.* **2020**, *50*, 719–740. [CrossRef]
50. Shruti; Rani, S.; Srivastava, G. Secure hierarchical fog computing-based architecture for industry 5.0 using an attribute-based encryption scheme. *Expert Syst. Appl.* **2024**, *235*, 121180. [CrossRef]
51. Mamatas, L.; Demiroglou, V.; Kalafatidis, S.; Skaperas, S.; Tsaoussidis, V. Protocol-Adaptive Strategies for Wireless Mesh Smart City Networks. *IEEE Netw.* **2023**, *37*, 136–143. [CrossRef]
52. Jumani, A.K.; Shi, J.; Laghari, A.A.; Hu, Z.; Nabi, A.U.; Qian, H. Fog computing security: A review. *Secur. Priv.* **2023**, *6*, e313. [CrossRef]
53. Ali, M.; Naeem, F.; Kaddoum, G.; Hossain, E. Metaverse Communications, Networking, Security, and Applications: Research Issues, State-of-the-Art, and Future Directions. In *IEEE Communications Surveys & Tutorials*; IEEE: Piscataway, NJ, USA, 2023; p. 1. [CrossRef]
54. Mukherjee, M.; Shu, L.; Wang, D. Survey of fog computing: Fundamental, network applications, and research challenges. In *IEEE Communications Surveys and Tutorials*; IEEE: Piscataway, NJ, USA, 2018; Volume 20, pp. 1826–1857. [CrossRef]

55. Katal, A.; Dahiya, S.; Choudhury, T. Energy efficiency in cloud computing data centers: A survey on software technologies. *Clust. Comput.* **2023**, *26*, 1845–1875. [CrossRef]
56. Bhushan, B.; Sahoo, G.; Rai, A.K. Man-in-the-middle attack in wireless and computer networking—A review. In Proceedings of the 2017 3rd International Conference on Advances in Computing, Communication \& Automation (ICACCA)(Fall), Dehradun, India, 15–16 September 2017; pp. 1–6.
57. de Kok, J.W.T.M.; de la Hoz, M.A.; de Jong, Y.; Brokke, V.; Elbers, P.W.G.; Thoral, P.; Castillejo, A.; Trenor, T.; Castellano, J.M.; Bronchalo, A.E.; et al. A guide to sharing open healthcare data under the General Data Protection Regulation. *Sci. Data* **2023**, *10*, 404. [CrossRef]
58. Kafi, A.; Akter, N. Securing Financial Information in the Digital Realm: Case Studies in Cybersecurity for Accounting Data Protection. *Am. J. Trade Policy* **2023**, *10*, 15–26. [CrossRef]
59. Ahmed, S.F.; Bin Alam, S.; Afrin, S.; Rafa, S.J.; Rafa, N.; Gandomi, A.H. Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions. *Inf. Fusion* **2024**, *102*, 102060. [CrossRef]
60. Papagiannidis, E.; Mikalef, P.; Conboy, K.; Van de Wetering, R. Uncovering the dark side of AI-based decision-making: A case study in a B2B context. *Ind. Mark. Manag.* **2023**, *115*, 253–265. [CrossRef]
61. Viswanathan, S.B.; Singh, G. Advancing Financial Operations: Leveraging Knowledge Graph for Innovation. *Int. J. Comput. Trends Technol.* **2023**, *71*, 51–60. [CrossRef]
62. Schultz, E. A framework for understanding and predicting insider attacks. *Comput. Secur.* **2002**, *21*, 526–531. [CrossRef]
63. Gunasekhar, T.; Rao, K.T.; Basu, M.T. Understanding insider attack problem and scope in cloud. In Proceedings of the 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015], Nagercoil, India, 19–20 March 2015; pp. 1–6. [CrossRef]
64. Phukan, J.; Li, K.F.; Gebali, F. Hardware covert attacks and countermeasures. In Proceedings of the 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), Crans-Montana, Switzerland, 23–25 March 2016; pp. 1051–1054. [CrossRef]
65. Gomez-Barrero, M.; Galbally, J.; Tome, P.; Fierrez, J. On the vulnerability of iris-based systems to a software attack based on a genetic algorithm. In Proceedings of the 17th Iberoamerican Congress, CIARP 2012, Buenos Aires, Argentina, 3–6 September 2012; pp. 114–121. [CrossRef]
66. Martinez-Diaz, M.; Fierrez, J.; Galbally, J.; Ortega-Garcia, J. An evaluation of indirect attacks and countermeasures in fingerprint verification systems. *Pattern Recognit. Lett.* **2011**, *32*, 1643–1651. [CrossRef]
67. Hoque, N.; Bhuyan, M.H.; Baishya, R.; Bhattacharyya, D.; Kalita, J. Network attacks: Taxonomy, tools and systems. *J. Netw. Comput. Appl.* **2014**, *40*, 307–324. [CrossRef]
68. Kronabeter, A.; Fenz, S. Cloud Security and Privacy in the Light of the 2012 EU Data Protection Regulation. In Proceedings of the Third International Conference, CloudComp 2012, Vienna, Austria, 24–26 September 2012; pp. 114–123. [CrossRef]
69. Jeun, I.; Lee, Y.; Won, D. A Practical Study on Advanced Persistent Threats. In Proceedings of the International Conferences, SecTech, CA, CES3 2012, Jeju Island, Republic of Korea, 28 November–2 December 2012; pp. 144–152. [CrossRef]
70. Claycomb, W.R.; Nicoll, A. Insider threats to cloud computing: Directions for new research challenges. In Proceedings of the International Computer Software and Applications Conference, Izmir, Turkey, 16–20 July 2012; pp. 387–394. [CrossRef]
71. Aslam, M.; Mohsin, B.; Nasir, A.; Raza, S. FoNAC—An automated Fog Node Audit and Certification scheme. *Comput. Secur.* **2020**, *93*, 101759. [CrossRef]
72. Guo, W.; Chen, Y. An Improved Dendritic Cell Algorithm Based Intrusion Detection System for Wireless Sensor Networks. *Int. J. Secur. Its Appl.* **2017**, *11*, 11–26. [CrossRef]
73. Yu, Z.; Au, M.H.; Xu, Q.; Yang, R.; Han, J. Towards leakage-resilient fine-grained access control in fog computing. *Future Gener. Comput. Syst.* **2018**, *78*, 763–777. [CrossRef]
74. Okafor, K.; Anulika, J.; Ononiwu, G. Vulnerability Bandwidth Depletion Attack on Distributed Cloud Computing Network: A QoS Perspective. *Int. J. Comput. Appl.* **2016**, *138*, 18–30. [CrossRef]
75. Hoyhtya, M.; Huusko, J.; Kiviranta, M.; Solberg, K.; Rokka, J. Connectivity for autonomous ships: Architecture, use cases, and research challenges. In Proceedings of the 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Republic of Korea, 18–20 October 2017; pp. 345–350. [CrossRef]
76. Jhaveri, R.H.; Patel, S.J.; Jinwala, D.C. DoS attacks in mobile ad hoc networks: A survey. In Proceedings of the 2012 2nd International Conference on Advanced Computing and Communication Technologies, ACCT 2012, Rohtak, India, 7–8 January 2012; pp. 535–541. [CrossRef]
77. Gupta, R.; Tanwar, S.; Tyagi, S.; Kumar, N. Machine Learning Models for Secure Data Analytics: A taxonomy and threat model. *Comput. Commun.* **2020**, *153*, 406–440. [CrossRef]
78. Tu, S.; Waqas, M.; Rehman, S.U.; Aamir, M.; Rehman, O.U.; Jianbiao, Z.; Chang, C.-C. Security in Fog Computing: A Novel Technique to Tackle an Impersonation Attack. *IEEE Access* **2018**, *6*, 74993–75001. [CrossRef]
79. Yuan, S.; Stewart, D. Protection of optical networks against interchannel eavesdropping and jamming attacks. In Proceedings of the 2014 International Conference on Computational Science and Computational Intelligence, CSCI 2014, Las Vegas, NV, USA, 10–13 March 2014; pp. 34–38. [CrossRef]
80. Kumar, V.; Sharma, A.; Mitali, V.K.; Sharma, A. A survey on various cryptography techniques. *Int. J. Emerg. Trends Technol. Comput. Sci. IJETTCS* **2014**, *3*, 307–312.

81. Xia, S.; Li, N.; Xiaofeng, T.; Fang, C. Multiple Attributes Based Spoofing Detection Using an Improved Clustering Algorithm in Mobile Edge Network. In Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, 15–17 August 2018; pp. 242–243. [CrossRef]
82. Mohammadi, P.; Ghaffari, A. Defending Against Flooding Attacks in Mobile Ad-Hoc Networks Based on Statistical Analysis. *Wirel. Pers. Commun.* **2019**, *106*, 365–376. [CrossRef]
83. Paharia, B.; Bhushan, K. A comprehensive review of distributed denial of service (DDoS) attacks in fog computing environment. In *Handbook of Computer Networks and Cyber Security*; Springer: Berlin/Heidelberg, Germany, 2019. [CrossRef]
84. Rajadurai, H.; Gandhi, U.D. Fuzzy Based Collaborative Verification System for Sybil Attack Detection in MANET. *Wirel. Pers. Commun.* **2020**, *110*, 2179–2193. [CrossRef]
85. Vasudeva, A.; Sood, M. Survey on sybil attack defense mechanisms in wireless ad hoc networks. *J. Netw. Comput. Appl.* **2018**, *120*, 78–118. [CrossRef]
86. Srirama, S.N. A decade of research in fog computing: Relevance, challenges, and future directions. *Softw.-Pract. Exp.* **2024**, *54*, 3–23. [CrossRef]
87. Hartmann, M.; Hashmi, U.S.; Imran, A. Edge computing in smart health care systems: Review, challenges, and research directions. *Trans. Emerg. Telecommun. Technol.* **2019**, *33*, e3710. [CrossRef]
88. Brochado, Â.F.; Rocha, E.M.; Costa, D. A Modular IoT-Based Architecture for Logistics Service Performance Assessment and Real-Time Scheduling towards a Synchromodal Transport System. *Sustainability* **2024**, *16*, 742. [CrossRef]
89. Ray, P.P.; Dash, D.; De, D. Edge computing for Internet of Things: A survey, e-healthcare case study and future direction. *J. Netw. Comput. Appl.* **2019**, *140*, 1–22. [CrossRef]
90. Singh, P.; Kaur, R. An integrated fog and Artificial Intelligence smart health framework to predict and prevent COVID-19. *Glob. Transit.* **2020**, *2*, 283–292. [CrossRef]
91. Hammoud, A.; Sami, H.; Mourad, A.; Otrok, H.; Mizouni, R.; Bentahar, J. AI, Blockchain, and Vehicular Edge Computing for Smart and Secure IoV: Challenges and Directions. *IEEE Internet Things Mag.* **2020**, *3*, 68–73. [CrossRef]
92. Sood, S.K.; Mahajan, I. Wearable IoT sensor-based healthcare system for identifying and controlling chikungunya virus. *Comput. Ind.* **2017**, *91*, 33–44. [CrossRef]
93. Abdel-Basset, M.; Mohamed, M. RETRACTED: A novel and powerful framework based on neutrosophic sets to aid patients with cancer. *Future Gener. Comput. Syst.* **2019**, *98*, 144–153. [CrossRef]
94. Bhosale, K.S.; Nenova, M.; Iliev, G. A study of cyber attacks: In the healthcare sector. In Proceedings of the 2021 Sixth Junior Conference on Lighting (Lighting), Gabrovo, Bulgaria, 23–25 September 2021; pp. 1–6. [CrossRef]
95. Queralta, J.P.; Gia, T.N.; Tenhunen, H.; Westerlund, T. Edge-AI in LoRa-based health monitoring: Fall detection system with fog computing and LSTM recurrent neural networks. In Proceedings of the 2019 42nd International Conference on Telecommunications and Signal Processing, TSP 2019, Budapest, Hungary, 1–3 July 2019; pp. 601–604. [CrossRef]
96. Cao, Y.; Chen, S.; Hou, P.; Brown, D. FAST: A fog computing assisted distributed analytics system to monitor fall for stroke mitigation. In Proceedings of the 2015 IEEE International Conference on Networking, Architecture and Storage, NAS 2015, Boston, MA, USA, 6–7 August 2015; pp. 2–11. [CrossRef]
97. Kraemer, F.A.; Braten, A.E.; Tamkittikhun, N.; Palma, D. Fog Computing in Healthcare–A Review and Discussion. *IEEE Access* **2017**, *5*, 9206–9222. [CrossRef]
98. Kyriazakos, S.; Mihaylov, M.; Anggorojati, B.; Mihovska, A.; Craciunescu, R.; Fratu, O.; Prasad, R. eWALL: An Intelligent Caring Home Environment Offering Personalized Context-Aware Applications Based on Advanced Sensing. *Wirel. Pers. Commun.* **2016**, *87*, 1093–1111. [CrossRef]
99. Ahmad, M.; Amin, M.B.; Hussain, S.; Kang, B.H.; Cheong, T.; Lee, S. Health Fog: A novel framework for health and wellness applications. *J. Supercomput.* **2016**, *72*, 3677–3695. [CrossRef]
100. Osama, M.; Ateya, A.A.; Sayed, M.S.; Hammad, M.; Pławiak, P.; Abd El-Latif, A.A.; Elsayed, R.A. Internet of Medical Things and Healthcare 4.0: Trends, Requirements, Challenges, and Research Directions. *Sensors* **2023**, *23*, 7435. [CrossRef] [PubMed]
101. Al Ameen, M.; Liu, J.; Kwak, K. Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. *J. Med. Syst.* **2012**, *36*, 93–101. [CrossRef] [PubMed]
102. Sethuraman, S.C.; Vijayakumar, V.; Walczak, S. Cyber Attacks on Healthcare Devices Using Unmanned Aerial Vehicles. *J. Med. Syst.* **2020**, *44*, 29. [CrossRef] [PubMed]
103. Ning, Z.; Huang, J.; Wang, X. Vehicular Fog Computing: Enabling Real-Time Traffic Management for Smart Cities. *IEEE Wirel. Commun.* **2019**, *26*, 87–93. [CrossRef]
104. Shafiq, H.; Rehman, R.A.; Kim, B.-S. Services and Security Threats in SDN Based VANETs: A Survey. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 8631851. [CrossRef]
105. Nobre, J.C.; de Souza, A.M.; Rosário, D.; Both, C.; Villas, L.A.; Cerqueira, E.; Braun, T.; Gerla, M. Vehicular software-defined networking and fog computing: Integration and design principles. *Ad Hoc Netw.* **2019**, *82*, 172–181. [CrossRef]
106. Wu, Q.; Shen, J.; Yong, B.; Wu, J.; Li, F.; Wang, J.; Zhou, Q. Smart fog-based workflow for traffic control networks. *Future Gener. Comput. Syst.* **2019**, *97*, 825–835. [CrossRef]
107. Bariah, L.; Shehada, D.; Salahat, E.; Yeun, C.Y. Recent advances in VANET security: A survey. In Proceedings of the 2015 IEEE 82nd Vehicular Technology Conference, VTC Fall 2015, Boston, MA, USA, 6–9 September 2015. [CrossRef]
108. Verma, K.; Hasbullah, H.; Kumar, A. Prevention of DoS Attacks in VANET. *Wirel. Pers. Commun.* **2013**, *73*, 95–126. [CrossRef]

109. Nkenyereye, L.; Liu, C.H.; Song, J. Towards secure and privacy preserving collision avoidance system in 5G fog-based Internet of Vehicles. *Future Gener. Comput. Syst.* **2019**, *95*, 488–499. [CrossRef]
110. Engoulou, R.G.; Bellaïche, M.; Pierre, S.; Quintero, A. VANET security surveys. *Comput. Commun.* **2014**, *44*, 1–13. [CrossRef]
111. Al-Amri, R.; Murugesan, R.K.; Alshari, E.M.; Alhadawi, H.S. Toward a Full Exploitation of IoT in Smart Cities: A Review of IoT Anomaly Detection Techniques. *Lect. Notes Netw. Syst.* **2022**, *322*, 193–214. [CrossRef]
112. Nasir, M.; Muhammad, K.; Lloret, J.; Sangaiah, A.K.; Sajjad, M. Fog computing enabled cost-effective distributed summarization of surveillance videos for smart cities. *J. Parallel Distrib. Comput.* **2019**, *126*, 161–170. [CrossRef]
113. Firdous, S.N.; Baig, Z.; Valli, C.; Ibrahim, A. Modelling and evaluation of malicious attacks against the IoT MQTT protocol. In Proceedings of the 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, iThings-GreenCom-CPSCom-SmartData 2017, Exeter, UK, 21–23 June 2017; pp. 748–755. [CrossRef]
114. Nazmudeen, M.S.H.; Wan, A.T.; Buhari, S.M. Improved throughput for Power Line Communication (PLC) for smart meters using fog computing based data aggregation approach. In Proceedings of the IEEE 2nd International Smart Cities Conference: Improving the Citizens Quality of Life, ISC2 2016, Trento, Italy, 12–15 September 2016; pp. 3–6. [CrossRef]
115. Ben-Shakhar, G. A survey of attacks and countermeasures in mobile ad hoc networks. In *Memory Detection: Theory and Application of the Concealed Information Test*; Cambridge University Press: Cambridge, UK, 2011; pp. 200–214. [CrossRef]
116. Mukta, M.Y.; Rahman, M.A.; Asyhari, A.T.; Bhuiyan, M.Z.A. IoT for energy efficient green highway lighting systems: Challenges and issues. *J. Netw. Comput. Appl.* **2020**, *158*, 102575. [CrossRef]
117. Jin, D.; Hannon, C.; Li, Z.; Cortes, P.; Ramaraju, S.; Burgess, P.; Buch, N.; Shahidehpour, M. Smart Street lighting system: A platform for innovative smart city applications and a new frontier for cyber-security. *Electr. J.* **2016**, *29*, 28–35. [CrossRef]
118. Tang, B.; Chen, Z.; Hefferman, G.; Pei, S.; Wei, T.; He, H.; Yang, Q. Incorporating Intelligence in Fog Computing for Big Data Analysis in Smart Cities. *IEEE Trans. Ind. Inform.* **2017**, *13*, 2140–2150. [CrossRef]
119. Cerina, L.; Notargiacomo, S.; Paccanit, M.G.; Santambrogio, M.D. A fog-computing architecture for preventive healthcare and assisted living in smart ambients. In Proceedings of the 2017 IEEE 3rd International Forum on Research and Technologies for Society and Industry (RTSI), Modena, Italy, 11–13 September 2017. [CrossRef]
120. Rahmani, A.M.; Gia, T.N.; Negash, B.; Anzanpour, A.; Azimi, I.; Jiang, M.; Liljeberg, P. Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. *Future Gener. Comput. Syst.* **2018**, *78*, 641–658. [CrossRef]
121. Alsafery, W.; Alturki, B.; Reiff-Marganiec, S.; Jambi, K. Smart Car Parking System Solution for the Internet of Things in Smart Cities. In Proceedings of the 1st International Conference on Computer Applications and Information Security, ICCAIS 2018, Riyadh, Saudi Arabia, 4–6 April 2018. [CrossRef]
122. Aliyu, F.; Sheltami, T.; Shakshuki, E.M. A Detection and Prevention Technique for Man in the Middle Attack in Fog Computing. *Procedia Comput. Sci.* **2018**, *141*, 24–31. [CrossRef]
123. Stojmenovic, I. Fog computing: A cloud to the ground support for smart things and machine-to-machine networks. In Proceedings of the 2014 Australasian Telecommunication Networks and Applications Conference (ATNAC), Southbank, Australia, 26–28 November 2014; pp. 117–122.
124. Srividhya, S.; Sankaranarayanan, S. IoT–Fog Enabled Framework for Forest Fire Management System. In Proceedings of the 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 27–28 July 2020; pp. 273–276. [CrossRef]
125. Pacheco, J.; Benitez, V.H.; Felix-Herran, L.C.; Satam, P. Artificial Neural Networks-Based Intrusion Detection System for Internet of Things Fog Nodes. *IEEE Access* **2020**, *8*, 73907–73918. [CrossRef]
126. Li, G.; Wu, S.X.; Zhang, S.; Li, Q. Neural Networks-Aided Insider Attack Detection for the Average Consensus Algorithm. *IEEE Access* **2020**, *8*, 51871–51883. [CrossRef]
127. Farjana, N.; Roy, S.; Mahi, M.J.N.; Whaiduzzaman, M. An Identity-Based Encryption Scheme for Data Security in Fog Computing. In *Studies in Computational Intelligence*; Uddin, M.S., Bansal, J.C., Eds.; Algorithms for Intelligent Systems; Springer: Singapore, 2020; Volume 669, pp. 215–226. [CrossRef]
128. Hou, S.; Li, H.; Yang, C.; Wang, L. A New Privacy-Preserving Framework based on Edge-Fog-Cloud Continuum for Load Forecasting. In Proceedings of the 2020 IEEE Wireless Communications and Networking Conference (WCNC), Seoul, Republic of Korea, 25–28 May 2020. [CrossRef]
129. Amin, R.; Kunal, S.; Saha, A.; Das, D.; Alamri, A. CFSec: Password based secure communication protocol in cloud-fog environment. *J. Parallel Distrib. Comput.* **2020**, *140*, 52–62. [CrossRef]
130. Singh, S.; Kumari, K.; Gupta, S.; Dua, A.; Kumar, N. Detecting different attack instances of ddos vulnerabilities on edge network of fog computing using gaussian naive bayesian classifier. In Proceedings of the 2020 IEEE International Conference on Communications Workshops, ICC Workshops, Dublin, Ireland, 7–11 June 2020. [CrossRef]
131. Khalid, T.; Khan, A.N.; Ali, M.; Adeel, A.; Khan, A.U.R.; Shuja, J. A fog-based security framework for intelligent traffic light control system. *Multimed. Tools Appl.* **2018**, *78*, 24595–24615. [CrossRef]
132. Xiao, J.; Kou, P. A hierarchical distributed fault diagnosis system for hydropower plant based on fog computing. In Proceedings of the 2017 IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference, ITNEC 2017, Chengdu, China, 15–17 December 2017; pp. 1138–1142. [CrossRef]

133. Ben Amor, A.; Abid, M.; Meddeb, A. A Privacy-Preserving Authentication Scheme in an Edge-Fog Environment. In Proceedings of the 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), Hammamet, Tunisia, 30 October–3 November 2017; pp. 1225–1231. [CrossRef]
134. Sohal, A.S.; Sandhu, R.; Sood, S.K.; Chang, V. A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. *Comput. Secur.* **2018**, *74*, 340–354. [CrossRef]
135. Bazm, M.-M.; Lacoste, M.; Sudholt, M.; Menaud, J.-M. Secure Distributed computing on untrusted fog infrastructures using trusted linux containers. In Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom, Nicosia, Cyprus, 10–13 December 2018; pp. 239–242. [CrossRef]
136. Deepali; Bhushan, K. DDoS attack mitigation and resource provisioning in cloud using fog computing. In Proceedings of the 2017 International Conference on Smart Technology for Smart Nation, SmartTechCon 2017, Bengaluru, India, 17–19 August 2017; pp. 308–313. [CrossRef]
137. Sharma, S. Data theft prevention using user behavior profiling and decoy documents. In Proceedings of the 2017 International Conference on Smart Technologies for Smart Nation (SmartTechCon), Bengaluru, India, 17–19 August 2017; pp. 957–961. [CrossRef]
138. Rebahi, Y.; Catal, F.; Tcholtchev, N.; Maedje, L.; Alkhateeb, O.; Elangovan, V.K.; Apostolakis, D. Towards Accelerating Intrusion Detection Operations at the Edge Network using FPGAs. In Proceedings of the 2020 5th International Conference on Fog and Mobile Edge Computing, FMEC 2020, Paris, France, 20–23 April 2020; pp. 104–111. [CrossRef]
139. de Souza, C.A.; Westphall, C.B.; Machado, R.B.; Sobral, J.B.M.; Vieira, G.d.S. Hybrid approach to intrusion detection in fog-based IoT environments. *Comput. Netw.* **2020**, *180*, 107417. [CrossRef]
140. Almiani, M.; AbuGhazleh, A.; Al-Rahayfeh, A.; Atiewi, S.; Razaque, A. Deep recurrent neural network for IoT intrusion detection system. *Simul. Model. Pract. Theory* **2020**, *101*, 102031. [CrossRef]
141. Sharma, S.K.; Wang, X. Live Data Analytics with Collaborative Edge and Cloud Processing in Wireless IoT Networks. *IEEE Access* **2017**, *5*, 4621–4635. [CrossRef]
142. Wang, T.; Zhang, G.; Liu, A.; Alam Bhuiyan, Z.; Jin, Q. A Secure IoT Service Architecture with an Efficient Balance Dynamics Based on Cloud and Edge Computing. *IEEE Internet Things J.* **2019**, *6*, 4831–4843. [CrossRef]
143. Lakshminarayana, D.H.; Philips, J.; Tabrizi, N. A survey of intrusion detection techniques. In Proceedings of the 18th IEEE International Conference on Machine Learning and Applications, ICMLA 2019, Boca Raton, FL, USA, 16–19 December 2019; pp. 1122–1129. [CrossRef]
144. Modi, C.; Patel, D.; Borisaniya, B.; Patel, H.; Patel, A.; Rajarajan, M. A survey of intrusion detection techniques in Cloud. *J. Netw. Comput. Appl.* **2013**, *36*, 42–57. [CrossRef]
145. Konorski, J.; Szott, S. Modeling a Traffic Remapping Attack Game in a Multi-Hop Ad Hoc Network. In Proceedings of the GLOBECOM 2017—2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017; pp. 1–7. [CrossRef]
146. Al-amri, R.; Murugesan, R.K.; Man, M.; Abdulateef, A.F.; Al-Sharafi, M.A.; Alkahtani, A.A. A Review of Machine Learning and Deep Learning Techniques for Anomaly Detection in IoT Data. *Appl. Sci.* **2021**, *11*, 5320. [CrossRef]
147. Wu, D.; Yan, J.; Wang, H.; Wang, R. Multiattack intrusion detection algorithm for edge-assisted internet of things. In Proceedings of the IEEE International Conference on Industrial Internet Cloud, ICII 2019, Orlando, FL, USA, 11–12 November 2019; pp. 210–218. [CrossRef]
148. Yuen, T.H.; Susilo, W.; Mu, Y. How to construct identity-based signatures without the key escrow problem. *Int. J. Inf. Secur.* **2010**, *9*, 297–311. [CrossRef]
149. Narayanan, A.; Shmatikov, V. Fast dictionary attacks on passwords using time-space tradeoff. In Proceedings of the ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 7–11 November 2005; pp. 364–372. [CrossRef]
150. Karthikeyan, R.; Geetha, T.; Vijayalakshmi, S. Honeypots for Network Security. *Int. J. Res. Dev. Technol.* **2017**, *7*, 62–66.
151. Bazm, M.-M.; Lacoste, M.; Sudholt, M.; Menaud, J.-M. Side-channels beyond the cloud edge: New isolation threats and solutions. In Proceedings of the 2017 1st Cyber Security in Networking Conference (CSNet), Rio de Janeiro, Brazil, 18–20 October 2017; pp. 1–8. [CrossRef]
152. Mahadevappa, P.; Murugesan, R.K. Study of Container-Based Virtualisation and Threats in Fog Computing. In Proceedings of the Second International Conference, ACeS 2020, Penang, Malaysia, 8–9 December 2020; Abdullah, A.N., Manickam, S., Eds.; Communications in Computer and Information Science. Springer: Singapore, 2021; Volume 1347, pp. 535–549. [CrossRef]
153. Rahbari-Asr, N.; Ojha, U.; Zhang, Z.; Chow, M.-Y. Incremental Welfare Consensus Algorithm for Cooperative Distributed Generation/Demand Response in Smart Grid. *IEEE Trans. Smart Grid* **2014**, *5*, 2836–2845. [CrossRef]
154. 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]
155. Ahmadi, S. Security Implications of Edge Computing in Cloud Networks. *J. Comput. Commun.* **2024**, *12*, 26–46. [CrossRef]
156. Makitalo, N.; Ometov, A.; Kannisto, J.; Andreev, S.; Koucheryavy, Y.; Mikkonen, T. Safe, Secure Executions at the Network Edge: Coordinating Cloud, Edge, and Fog Computing. *IEEE Softw.* **2017**, *35*, 30–37. [CrossRef]
157. Javadpour, A.; Wang, G.; Rezaei, S. Resource Management in a Peer-to-Peer Cloud Network for IoT. *Wirel. Pers. Commun.* **2020**, *115*, 2471–2488. [CrossRef]
158. Zhang, P.; Zhou, M.; Fortino, G. Security and trust issues in Fog computing: A survey. *Future Gener. Comput. Syst.* **2018**, *88*, 16–27. [CrossRef]

159. Mahadevappa, P.; Murugesan, R.K. Review of data integrity attacks and mitigation methods in edge computing. In Proceedings of the Advances in Cyber Security: Third International Conference, ACeS 2021, Penang, Malaysia, 24–25 August 2021; Revised Selected Papers 3, pp. 505–514.
160. Ren, J.; Zhang, D.; He, S.; Zhang, Y.; Li, T. A survey on end-edge-cloud orchestrated network computing paradigms: Transparent computing, mobile edge computing, fog computing, and cloudlet. *ACM Comput. Surv.* **2019**, *52*, 1–36. [CrossRef]
161. Chatterjee, J.; Das, M.K.; Ghosh, S.; Das, A.; Bag, R. A review on security and privacy concern in IOT health care. *Internet Things Healthc. Technol.* **2020**, 247–271.
162. Xia, Q.; Ye, W.; Tao, Z.; Wu, J.; Li, Q. A survey of federated learning for edge computing: Research problems and solutions. *High-Confid. Comput.* **2021**, *1*, 100008. [CrossRef]
163. Bonawitz, K.; Eichner, H.; Grieskamp, W.; Huba, D.; Ingerman, A.; Ivanov, V.; Kiddon, C.; Konečný, J.; Mazzocchi, S.; McMahan, H.B.; et al. Towards federated learning at scale: System design. *arXiv* **2019**, arXiv:1902.01046.
164. Salehi, S.A.; Razzaque, M.A.; Tomeo-Reyes, I.; Hussain, N. IEEE 802.15.6 standard in wireless body area networks from a healthcare point of view. In Proceedings of the Asia-Pacific Conference on Communications, APCC 2016, Yogyakarta, Indonesia, 25–27 August 2016; pp. 523–528. [CrossRef]
165. Zhang, X.; Cao, X.; Yan, L.; Sung, D.K. A Street-Centric Opportunistic Routing Protocol Based on Link Correlation for Urban VANETs. *IEEE Trans. Mob. Comput.* **2016**, *15*, 1586–1599. [CrossRef]
166. Shen, X.; Cheng, X.; Yang, L.; Zhang, R.; Jiao, B. Data dissemination in VANETs: A scheduling approach. *IEEE Trans. Intell. Transp. Syst.* **2014**, *15*, 2213–2223. [CrossRef]
167. Lau, B.P.L.; Marakkalage, S.H.; Zhou, Y.; Hassan, N.U.; Yuen, C.; Zhang, M.; Tan, U.-X. A survey of data fusion in smart city applications. *Inf. Fusion* **2019**, *52*, 357–374. [CrossRef]
168. Weddell, A.S.; Magno, M.; Merrett, G.V.; Brunelli, D.; Al-hashimi, B.M.; Benini, L. A Survey of Multi-Source Energy Harvesting Systems. In Proceedings of the 2013 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, 18–22 March 2013.
169. Baktir, A.C.; Ozgovde, A.; Ersoy, C. How Can Edge Computing Benefit from Software-Defined Networking: A Survey, Use Cases, and Future Directions. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2359–2391. [CrossRef]
170. Liu, D.; Li, Z.; Jia, D. Secure distributed data integrity auditing with high efficiency in 5G-enabled software-defined edge computing. *Cyber Secur. Appl.* **2023**, *1*, 100004. [CrossRef]
171. Bari, F.; Boutaba, R.; Esteves, R.; Granville, L.Z.; Podlesny, M.; Rabbani, G.; Zhang, Q.; Zhani, M.F. Data Center Network Virtualization: A Survey. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 909–928. [CrossRef]
172. Zhang, P.; Chen, Z.; Liu, J.K.; Liang, K.; Liu, H. An efficient access control scheme with outsourcing capability and attribute update for fog computing. *Future Gener. Comput. Syst.* **2018**, *78*, 753–762. [CrossRef]
173. Hernandez-Jaimes, M.L.; Martinez-Cruz, A.; Ramírez-Gutiérrez, K.A.; Feregrino-Uribe, C. Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures. *Internet Things* **2023**, *23*, 100887. [CrossRef]
174. Wang, X.; Ren, X.; Qiu, C.; Xiong, Z.; Yao, H.; Leung, V.C. Synergy of Edge Intelligence and Blockchain: A Comprehensive Survey. *TechRxiv* **2021**.
175. Zhou, Z.; Wan, Y.; Cui, Q.; Yu, K.; Mumtaz, S.; Yang, C.-N.; Guizani, M. Blockchain-Based Secure and Efficient Secret Image Sharing with Outsourcing Computation in Wireless Networks. *IEEE Trans. Wirel. Commun.* **2023**, *23*, 423–435. [CrossRef]
176. Li, J.; Herdem, M.S.; Nathwani, J.; Wen, J.Z. Methods and applications for Artificial Intelligence, Big Data, Internet of Things, and Blockchain in smart energy management. *Energy AI* **2023**, *11*, 100208. [CrossRef]