future internet

MDPI

Review

From Bottom of Sea to Space: Quo Vadis IoT? So What About Security?

Behrouz Zolfaghari *, Jacob Krzciok and Khodakhast Bibak

Department of Computer Science and Software Engineering, Miami University, Oxford, OH 45056, USA; krzciojj@miamioh.edu (J.K.); bibakk@miamioh.edu (K.B.)

* Correspondence: zolfagb@miamioh.edu

Abstract: In recent years, we have witnessed the era of IoT. Extensions of the IoT are found almost everywhere in the modern world: under the ground, on the ground, under the sea, in the sky, and in space. Such a rapid proliferation has given rise to a variety of requirements and challenges. As suggested by the recent literature, security is the most critical challenge in this area. A comprehensive survey in this area can pave the way for further research by highlighting current trends and shedding light on less-studied aspects of the area. This paper provides a comprehensive review of the current state of research on IoT extensions, with a focus on security. We start with reviewing existing relevant surveys, noting their shortcomings. We highlight the lack of inclusiveness in existing surveys. Moreover, we show that these surveys do not look closely at security challenges and fail to develop a taxonomy or a solid future roadmap. Then, we provide an overview of the security challenges and mechanisms of IoT extensions. We proceed to develop a taxonomy of these extensions with a focus on security. Lastly, we discuss what the future may hold for IoT extensions, given the role of artificial intelligence in IoT and the advancements of artificial intelligence on the horizon.

Keywords: IoT; IoT extensions; security challenges; security mechanisms

check for updates

Academic Editor: Paolo Bellavista

Received: 24 December 2024
Revised: 8 February 2025
Accepted: 12 February 2025
Published: 17 February 2025

Citation: Zolfaghari, B.; Krzciok, J.; Bibak, K. From Bottom of Sea to Space: Quo Vadis IoT? So What About Security? *Future Internet* **2025**, *17*, 91. https://doi.org/10.3390/fi17020091

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

In recent years, extensions of IoT have been of great interest to researchers [1]. An extension of the IoT is formed by a set of geographically distributed, special-purpose cyber–physical, or cyber-enabled things, which are connected using special-purpose protocols on top of the Internet to achieve a specific goal. To mention a few of these extensions, one may refer to Internet of Vehicles [2] and Vehicular Things [3], Internet of Medical [4] and Healthcare [5] Things, Internet of Bodies [6], Internet of Vessels [7], or Internet of Energy [8].

These extensions have been studied from different technological aspects [9,10]. Different objectives have been considered by IoT extension designers and researchers. Among these objectives, some may refer to performance [11], Quality of Service (QoS) [12], Quality of Experience (QoE) [13], timeliness [14], reliability [15], scalability [16], fault tolerance [17], or energy efficiency [18]. However, security is probably the most challenging design objective for IoT extensions [19].

Extensions of the IoT are spread from the bottom of the sea [20] to space [21]. This is shown in Figure 1. The application of IoT extensions under the ground, under the sea, on the ground, in the sky, and in space makes it pertinent to study these extensions from different perspectives. Related challenges, as well as current and future trends, need to be thoroughly investigated. A comprehensive survey in this area can serve to meet these

goals. Although there are some surveys that are somewhat relevant, their shortcomings (discussed in Section 2.6 of Section 2 motivate our work in this paper).

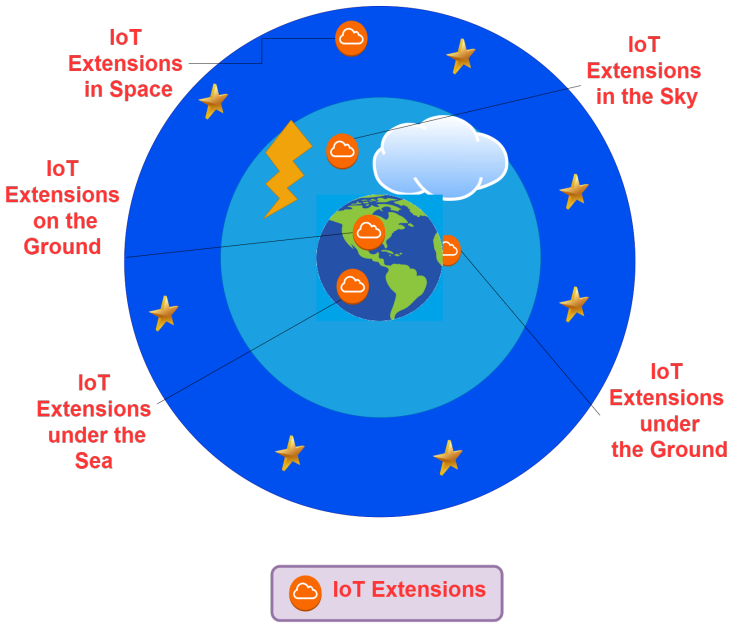


Figure 1. IoT extensions spread everywhere.

This paper provides a comprehensive review of the current state of research on IoT extensions, with a focus on security. We first classify extensions of the IoT based on the geographical locations where they are deployed, e.g., under the sea, under the ground, on the ground, in the sky, or in space. We study security challenges in the design of each extension. Moreover, we discuss security mechanisms used in each extension. Then, we present a taxonomy of existing IoT extensions. Lastly, we develop a future roadmap with a focus on the role of AI in the future of IoT extensions. This study is unique in its broad perspective in the sense that we cover all types of IoT extensions, all security challenges, and all security mechanisms.

1.1. Goals and Objectives

In this study, we attempt to provide detailed answers to the following questions:

1. What types of IoT extensions have been proposed, designed, and studied so far?
2. What security challenges are faced by designers and researchers?
3. What security mechanisms have been used to resolve each of the challenges?
4. What parameters should be considered for classifying IoT extensions?
5. What does the security-oriented taxonomy of IoT extensions look like?
6. What does the taxonomy reveal regarding the less-studied aspects of secure IoT extensions?
7. What will the future hold for secure IoT extensions, given the role of Artificial Intelligence (AI) in these extensions and the current trends in AI?

1.2. Achievements

The achievements of this study can be listed as below:

1. This paper is the first of its kind to cover all existing IoT extensions along with all related security challenges and all security mechanisms of each extension (Section 3).
2. This paper presents the first taxonomy, and especially, the first security-oriented taxonomy on all existing extensions of IoT (Section 4). The security-oriented taxonomy

facilitates the identification of related topics, which have not been adequately studied in the literature (Subsection 5.1).

3. This paper is the first to study the role of AI in the future of secure IoT extensions (Subsection 5.2).

The summary of our research goals and achievements can be seen in Figure 2.

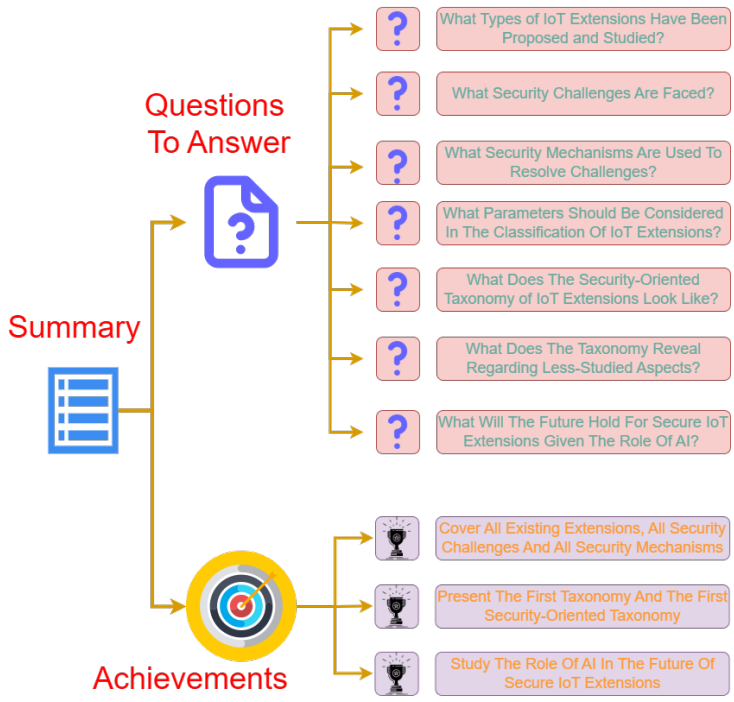


Figure 2. Research summary.

1.3. Organization

The rest of this paper is organized as follows. Section 2 reviews the existing surveys and highlights their shortcomings in order to clarify our motivations for this research. Section 3 studies the security challenges and mechanisms of IoT extensions. Section 4 develops the security-oriented taxonomy on IoT extensions. Section 5 presents some directions for future research. In this section, we first use the taxonomy of Section 4 to shed light on some less-studied aspects of secure IoT extensions. Then, we present a look-ahead to the future of secure IoT extensions, given the role of AI in current trends. Lastly, Section 6 concludes the paper and suggests future works.

2. Existing Surveys

In this section, we briefly study existing relevant surveys in order to highlight their shortcomings, which motivate the work of this review. We classify existing surveys into the following categories:

- Surveys that focus on a single type of IoT extension without discussing security challenges or mechanisms. These surveys are studied in Section 2.1.
- Surveys that cover a group of IoT extensions without focusing on security-related issues. These surveys are studied in Section 2.2.
- Surveys focusing on security-related issues in IoT extensions. Although this category contains some surveys covering different security-related aspects, none of them studies all existing types of IoT extensions. Section 2.3 discusses this category of IoT extensions.

- Surveys focusing on the role of AI in IoT extensions, without investigating security considerations. None of the existing surveys falling into this category covers all kinds of IoT extensions or studies the role of AI in the future of these extensions. These surveys are reviewed in Section 2.4.

In our reviews, we did not identify any survey related to the role of AI in the security of IoT extensions. None of the existing surveys covers all types of AI models or all types of IoT extensions. Moreover, none of them anticipates the role of AI in the future of secure IoT extensions.

2.1. Surveys Focusing on a Single IoT Extension

This subsection reviews surveys that study a specific type of IoT extension without a focus on security-related considerations. The extensions studied in these surveys can be classified as follows:

- **Extensions Deployed under the Ground:** Surveys on these extensions are reviewed in Section 2.1.1.
- **Extensions Deployed on the Ground:** Surveys related to this class are studied in Section 2.1.2.
- **Extensions Deployed in the Sea:** We discuss surveys focusing on these extensions in Section 2.1.3.
- **Extensions Deployed in Space:** Surveys on this class are reviewed in Section 2.1.4.

2.1.1. Extensions Deployed Under the Ground

The recent literature comes with some surveys focusing on the Internet of Underground Things. For example, state-of-the-art sensing and Cloud integration components used in this IoT extension were studied in [22] along with related challenges. The authors of [22] reviewed the applications of this extension as well. Moreover, in [23], the authors studied the role of the Internet of Underground Things in soil fertility monitoring. They first highlighted the impact of soil fertility monitoring on qualitative and quantitative improvement in food production as well as reduction in greenhouse gas emissions. In the next step, they presented a survey on underground sensing technologies as well as communication protocols used in this type of IoT extension.

2.1.2. Extensions Deployed on the Ground

Several surveys have focused on different types of IoT extensions deployed on the ground, including the Internet of Bodies, Internet of Audio Things, Internet of Vehicles, Internet of Autonomous Vehicles, Internet of Medical Things, Internet of Wearable Things, and Internet of Bio-Nano Things. These surveys are reviewed in the following.

Internet of Bodies

The Internet of Bodies can be used for a wide range of services and applications for a broad spectrum of sectors. These services include, but are not limited to, medicine, safety, security, health, and entertainment. Despite this critical importance, there are only a few surveys focusing on the Internet of Bodies. One such survey has been reported in [24]. In this research, the authors argued that given the recent crisis caused by COVID-19, the Internet of Bodies can revolutionize public health and safety infrastructures in today's world. They reviewed the communication and networking requirements of this IoT extension along with related standards and protocols. These researchers presented a survey on channel modeling issues for various link types in Human Body Communication (HBC) channels. These channels are of critical importance due to the heterogeneous and lossy dielectric properties of the human body.

Internet of Audio Things

In this kind of IoT extension, audio things, such as acoustic sensors, are connected over an infrastructure capable of allowing local or remote, multidirectional communications. The authors of [25] presented an overview on this IoT extension. They established an ecosystem for this extension consisting of interoperable devices and services related to human–human and human–machine interactions. These researchers investigated design and implementation challenges in this field and developed directions for future research in this area.

Internet of Multimedia Things

A survey related to this type of extension has been reported in [26]. The authors of [26] stated that the underlying protocol stacks in the Internet of Multimedia Things need to fulfill stringent requirements in terms of quality of Service (QoS), latency, reliability, bandwidth, and storage, which are raised by multimedia data. Moreover, they highlighted interoperability as a challenging task in the Internet of Multimedia Things due to the existence of heterogeneous multimedia sensors. They presented a survey on the challenges faced by seamless, interoperable communication in this type of IoT extension. The authors also studied Cloud as a promising paradigm for eliminating the storage requirements in these extensions.

Internet of Vehicles (IoV)

The Internet of Vehicles is one of the best-studied extensions of the IoT. There are several surveys on different aspects of the IoV. For example, a review of existing methods for recommending driving strategies, appropriate routes, and entertainment content in the IoV has been presented in [27]. As another example, one may refer to [28], where the authors present a survey on Business Models (BM) adapted for Fifth Generation (5G) network slicing with a focus on applications in the IoV. This technology is capable of creating virtually isolated and logically parallel networks, enabling a large range of complex services. Another survey on the applications of 5G standards and infrastructures in Vehicle-to-Everything Communications (V2X) and IoV has been reported in [29]. The evolution of traditional V2X technologies to IoV platforms has been studied in relevant research [30].

Moreover, the authors of [31] highlighted the shortcomings of existing cellular communication technologies such as Fifth Generation (5G) and short-range wireless communication standards such as Dedicated Short-Range Communication (DSRC) in supporting the high volume of data generated by IoV sensors. They presented a survey on advances in Millimeter-wave (mmWave) technology with a focus on applications in the IoV. In [32], the adoption of blockchain as a system platform for supporting the information exchange requirements of the IoV has been studied. They noted that the underlying information exchange platform of the IoV needs to be immutable, transparent, and secure in order to support the intended objectives of an Intelligent Transportation System (ITS). There are also other surveys briefly discussing different technological challenges of the IoT [33].

Internet of Autonomous Vehicles

A survey on the Internet of Autonomous (Driverless) Vehicles has been presented in [34]. This survey compares traditional client-server communication models with centralized models. The authors of this survey demonstrate how this IoT extension will move from network-centric communication models to user-centric ones in the future. They also discuss the role of Value-Added Services (VASs) in the Internet of Autonomous Vehicles.

Internet of Medical Things

The authors of [35] stated that frequent topology changes due to user mobility and posture alteration increase the complexity of routing and resource allocation in the Internet of Medical Things. They reviewed individual and group health monitoring architectures based on the Internet of Medical Things that allow users to freely move around. They discussed the enabling technologies for each of the studied architectures. Moreover, they investigated existing solutions for route breakage in this kind of IoT extension.

Internet of Wearable Things (IoWT)

Wearable things include smart clothes, smart jewelry, smartwatches, and similar personal mobile devices. The IoWT lies in the intersection of the IoT and the technologies related to these devices. The battery-powered nature of these devices raises energy efficiency as a critical requirement in the IoWT. A comparative, systematic literature review, along with a taxonomy of energy-efficient solutions proposed for IoWT-based scenarios, has been presented in [36]. This survey discusses related performance parameters as well as existing solutions for improving energy efficiency in IoWT.

Internet of Nano Things

The literature comes with surveys on different aspects of the Internet of Nano Things. For example, a survey presented in [37] studies this IoT extension with a focus on applications in healthcare environments. Another relevant research presents a survey on routing protocols in the Internet of Nano Things [38].

2.1.3. Extensions Deployed in the Sea

Some extensions of the IoT are deployed under the sea, e.g., the Internet of Underwater Things, or on the sea, e.g., the Internet of Ships (IoS). These extensions have been studied in a few surveys, which are discussed below.

Internet of Underwater Things

The Internet of Underwater Things has been studied from different perspectives. For example, the survey presented in [39] discusses current advances, challenges, and open issues in this IoT extension, with a focus on applications in smart oceans. Moreover, a five-layer system architecture for the Internet of Underwater Things has been proposed in this survey. The proposed architecture consists of a sensing layer, communication layer, networking layer, fusion layer, and application layer. Another relevant survey has studied the Internet of Underwater Things from a big data analytics perspective [40].

Internet of Ships

A survey on the IoS has been presented in [41], along with related architectures and elements. This survey also discusses emerging applications of the IoS. Moreover, some potential future opportunities, such as satellite communications, as well as some potential challenges, such as data collection, management, and analytics, have been studied in this survey.

2.1.4. Extensions Deployed in Space

Internet of Space Things, as well as the Internet of Drones, fall into this category. Surveys on these extensions are discussed in the following.

Internet of Space Things

There are only a few surveys in this area. Among these surveys, one may refer to the one presented in [42]. This survey reviews existing research on connectivity and computing

technologies in the IoT for non-terrestrial space environments. Moreover, it presents an overview of the area along with key challenges as well as a look-ahead to the future opportunities.

Internet of Drones (IoD)

There is a survey on applications, deployments, and integration of the IoD [43]. This survey discusses some enabling technologies that support the IoD in different scenarios. Optimization-based methods, Neural Networks (NNs), and blockchain are among these enabling technologies.

2.2. Surveys Focusing on a Group of IoT Extensions

To the best of our knowledge, the only survey covering a group of IoT extensions has been reported in [44]. In [44], the authors have tried to study the current trends and predict the future of IoT extensions. They have anticipated that a hyperspace will be formed consisting of physical space (traditional IoT), social-inspired space (Internet of People), and brain-abstracted space (Internet of Thinking). They refer to this hyperspace as Internet of X.

2.3. Surveys on the Security of IoT Extensions

Different security aspects of different IoT extensions have been investigated in some survey research works. Relevant surveys are discussed below.

2.3.1. Secure Internet of Vehicles

Different security aspects in different variants of the Internet of Vehicles have been studied in existing surveys. For example, the authors of [45] have studied the Social Internet of Vehicles from a location privacy perspective. A similar survey has been conducted on the 6G-Enabled Internet of Vehicles [46]. As another example, in [47], the authors have studied authentication protocols in the Internet of Vehicles along with related testbeds and challenges.

2.3.2. Secure Internet of Medical Things

There are some surveys related to secure Internet of Medical Things extensions. As an example, we can mention the one reported in [48], where the authors have highlighted the critical role of this extension as safety-critical platforms in the monitoring of patients suffering from chronic diseases. The authors of [48] presented a literature review on research works focusing on secure data collection, transmission, and storage in the Internet of Medical Things. Furthermore, they studied some related attacks and some mitigation techniques. There is another relevant survey where risk assessment methodologies capable of being used in the Internet of Medical Things have been studied and classified [49].

2.3.3. Secure Internet of Intelligent Things

The authors of [50] presented a tutorial on techniques for designing generalized blockchain-based schemes for authentication and key management in the Internet of Intelligent Things. They discussed some prevailing consensus algorithms used for this purpose. These researchers also highlighted some related challenges as directions for future research in this area.

2.3.4. Secure Internet of Drones

In [51], the authors presented a taxonomy on drones used in the Internet of Drones. They studied the severity of security and privacy threats associated with each type of drone. They tried to develop an architecture for a secure Internet of Drones. Moreover,

they established a taxonomy on attacks that hit this type of IoT extension. They reviewed existing attack mitigation techniques as well.

2.3.5. Secure Internet of Bio-Nano Things

The authors of [52] presented a review on bio-cyber interface technologies in the Internet of Bio-Nano Things (e.g., bio-electronic devices, implantable Radio Frequency Identification(RFID) chips, and electronic tattoos). They proceeded to study some security vulnerabilities of these technologies along with related mitigation strategies.

2.4. Surveys on the Role of AI in IoT Extensions

There are a few surveys somewhat related to the role of AI in the IoT extensions. In the following, we review surveys of this type.

2.4.1. AI-Assisted Internet of Medical Things

The authors of [53] noted that Cloud computing, Edge computing (EC), and AI can be impactful in assisting the Internet of Medical Things. They investigated how Cloud computing can facilitate the storage of data collected by medical sensors, how edge computing can support code caching in edge nodes, and how AI can assist big data analysis in this type of IoT extension.

2.4.2. AI-Assisted Internet of Vehicles

A survey has been presented in [54] that focuses on the role of AI in IoV environments supported by EC. In EC-enabled IoV, AI tools can help dynamic, real-time decision making in Road-Side Units (RSUs), which play the role of edge nodes. AI-based methods can improve learning capacity and assist dynamic resource allocation in edge nodes. The authors of [54] reviewed common IoV edge service frameworks in order to explore the applications of AI in service offloading and edge server placement.

2.5. Summary

Table 1 summarizes existing relevant surveys in order to make it easy to compare them with our work in this paper.

Table 1. Summary of existing surveys.

Survey	Year	All Ext.	All Sec.	Tax.	Roadmap	AI	Survey	Year	All Ext.	All Sec.	Tax.	Roadmap	AI
[22]	2020	No	No	No	No	No	[39]	2020	No	No	No	Yes	No
[23]	2022	No	No	Yes	No	No	[40]	2021	No	No	No	No	No
[24]	2022	No	No	No	Yes	No	[41]	2020	No	No	No	Yes	No
[25]	2020	No	No	No	Yes	No	[42]	2021	No	No	NO	Yes	No
[26]	2020	No	No	No	Yes	No	[43]	2021	No	No	No	Yes	No
[27]	2020	No	No	No	No	No	[44]	2021	Yes	No	No	Yes	No
[28]	2021	No	No	No	Yes	No	[45]	2020	No	No	No	Yes	No
[29]	2020	No	No	No	Yes	No	[46]	2022	No	No	No	No	No
[30]	2020	No	No	No	No	No	[47]	2020	No	No	No	Yes	No
[31]	2020	No	No	No	Yes	No	[48]	2021	No	No	No	No	No
[32]	2021	No	No	No	Yes	No	[49]	2021	No	No	No	No	No
[33]	2021	No	No	No	Yes	No	[50]	2020	No	No	No	Yes	No
[34]	2020	No	No	No	Yes	No	[51]	2021	No	Yes	No	Yes	No
[35]	2020	No	No	No	Yes	No	[52]	2021	No	Yes	No	No	No
[36]	2020	No	No	No	Yes	No	[53]	2020	No	No	No	Yes	No
[37]	2020	No	No	Yes	No	No	[54]	2022	No	No	No	Yes	No
[38]	2020	No	No	No	No	No							

Table 1 consists of two blocks. Each block can be described as follows. The first entry in each row cites one of the surveys studied above. The second column contains a "Yes" if the survey covers all kinds of IoT extensions. It contains a "No" otherwise. The third column indicates whether or not the survey studies all security challenges and mechanisms. The fourth column contains a "Yes" only for surveys that provide a taxonomy. In the fifth column, a "Yes" indicates a survey that presents a future roadmap. Lastly, the sixth column indicates whether or not the survey cited in the first column discusses the role of AI in the future of secure IoT extensions.

2.6. Motivations

As seen in Table 1, although the literature comes with some surveys somewhat relevant to this study, there is no survey with all of the following properties:

- Presenting a taxonomy on all existing kinds of IoT extensions.
- Studying all security challenges and mechanisms for all kinds of IoT extensions.
- Presenting a future roadmap for secure IoT extensions in consideration of AI's role.

This study is an attempt to address the above gap. The most relevant survey is the one reported in [44], where the authors have covered a group of IoT extensions and tried to anticipate what the future may hold for these technologies. However, this work is different from our work in the following ways:

- It does not provide any taxonomy on existing IoT extensions.
- It does not focus on security-related challenges and mechanisms.
- It does not discuss the role of AI in future developments of IoT extensions.

3. Security Challenges and Mechanisms

3.1. IoT Under the Ground

3.1.1. Internet of Underground Things

The Internet of Underground Things has been used in a variety of applications including, but not limited to, precision agriculture, pipeline monitoring, border control, oil and gas reservoir exploration, and monitoring of oil wells or soil fertility [23]. To the best of our knowledge, there is a lack of research focusing on the security of this extension. We believe this may be due to the absence of significant security incidents or threats reported in these platforms as their operation underground has yet to generate concerns in this regard.

3.1.2. Internet of Mine Things Things

Internet of Mine Things is used in applications such as mine water control. There is a close relationship between the Internet of Underground Things and the Internet of Mine Things in the way that they have been studied alongside each other in some recent works [55]. To the best of our knowledge, there is no research report focusing on the security of this IoT extension.

3.2. IoT on the Ground

3.2.1. Extensions with Applications in Medicine

Internet of Medical Things

The recent advancements in mini-hardware manufacturing, microcomputing, and Machine-to-Machine (M2M) communications have made it possible for IoT platforms to reshape many existing networking applications. Healthcare systems are among these applications. Their evolution under the impact of IoT has led to an IoT extension referred to as the Internet of Medical Things.

The application areas of the Internet of Medical Things (IoMT) vary from heart [56] and skin [57] disease detection, as well as C-reactive protein and serum Amyloid detection to healthcare monitoring [58], emotion recognition [59], tumor prediction [60], Colonoscopy [61], remote patient diagnosis [62] and surgery [63].

As suggested in recent research, the most important security challenges and mechanisms of this extension can be listed below:

- Security Challenges
  - Privacy

    The authors of the paper [64] suggest the use of a blockchain-based record to have decentralized electronic health records. They propose that the blockchain model be used in part with smart-contract-based service automation. Some of the major drawbacks of such a system include high latency, large storage costs, and single-point failure. The proposed solution is the use of a Distributed Data Storage System. Device authentication is handled by a decentralized selective ring-based access control. The anonymity of the patient information is protected through the use of different patient anonymity algorithms.

    Similarly, the paper [65] uses the blockchain-based model. The proposed system uses a triple subject purpose-based access control model. The model would work in part with a transactional blockchain network to also allow for a more decentralized approach. Access to the system will be limited to users with certain privileges following a Local Differential Privacy-based policy. This will prevent malicious users from having access to the entire system. The proposed blockchain-enabled method has been tested in a live setting with more than 100,000 patient records and has shown great improvements over current systems.

    To compare the decentralized blockchain methods proposed above, ref. [66] uses two non-colluding severs and a privacy-preserving cloud-aided diagnosis scheme to create a secure way to outsource diagnoses. This diagnosis scheme uses a combination of AES and homomorphic encryption to make user requests more efficient. The analysis in the paper illustrates that the proposed scheme is better than prior works when looking at the system in terms of security and usability. The paper [67] goes further and talks about how most new solutions focus on data encryption, increasing the cost of sending and computing information to patients and users. The scheme these authors propose focuses on three main points: a guarantee of privacy, efficient integrity verification to prevent incorrect query and computation, and lastly, lightweight operations of the patient and the user. This aims to take full advantage of cloud-aided systems while limiting resource costs.

    Another area that has gained a lot of attention is the future of 5G networks. Ref. [68] suggests a method of device-to-device communication for medical services that uses future 5G networks. The method is the use of an intelligent trust cloud management system. The authors propose an update to the current system to make it more adaptive and intelligent in a wireless medium. Tests performed by the authors demonstrate that the updates will address trust uncertainty and improve the detection accuracy of malicious devices.

    The following paper [69] was inspired by the current pandemic and proposes a new privacy-enhanced data fusion strategy. The design of the system is proven to successfully demonstrate an improvement in the protection of data fusion during the outbreak of COVID-19. The authors take into account task completion, classification accuracy, reliability, and a low rate of errors based on its use in IoMT. They are able to do this through the use of a validation method based on a deterministic policy gradient, which keeps the accuracy of the data intact.

The authors believe that most current systems lack the ability to accurately and efficiently validate the large amounts of data caused by the pandemic.

- Trust

  Trust is an important factor in successful communication, especially in the realm of IoMT. The authors of [70] discuss the reasons that trust struggles in current systems. The main attack focused on in this paper is the Sybil attack. The attack creates a fake node in an attempt to infiltrate the system. The proposed solution to the detection of malicious activity is the use of trust management. It allows a system to authenticate its neighboring nodes while neglecting the malicious nodes. The proposed version of trust management focuses on the use of fuzzy logic processing and the fuzzy filter.

  Most of the sensors in medical devices have a limited amount of resources to implement many proposed protocols to safely authenticate each other. The authors of [71] propose a group key agreement (GKA) protocol to allow for a reduction in computational cost and an increase in the possibility of more dynamic connections between groups of sensors. The GKA would be performed using a physical unclonable function (PUF) to create unique fingerprints. The method focuses on higher security and efficiency.

- Attack Resilience

  As more information and systems are developed in the IoT, there is a growing number of ways for systems to be attacked. A common goal of these attacks is intrusion into a system or attempts to breach data. The authors of [72] propose a method of intrusion detection through the use of a deep learning-based method called the Deep Belief Network algorithm. When tested, the system received a 95% success rating in most classes of attacks.

  Another common attack on these systems is man-in-the-middle-attacks (MITM). These attacks are especially dangerous because they often do not raise alarms. The authors of [73] propose a framework that is capable of sending a smaller digital signature by creating a key based on the strength of the received signal. When tested, the false alarm rate was low, while its ability to detect MITM attacks was high.

- Security Mechanisms

  - Authentication

    As the automation of remote healthcare continues to grow, the need for authentication continues to grow with it. The focus on a trustworthy, efficient, and resourceful system is important to the growth of the industry. The authors of [74] suggest an improvement in the use of a mutual authentication protocol for a Telecare Medical Information System (TMIS) proposed by Chiou et al. [75] in 2016. The authors discuss the shortcomings of the current system and suggest the use of smart service authentication. The method better protects patient anonymity and stolen smart device attacks through the use of three stages: initialization by a security authority center, registration by a medical censor, and authentication by a smart device. Smart device authentication makes use of a common key to allow for mutual authentication. When the researchers of [74] tested the method, it showed significant improvements to the Chiou et al. [75] method.

    As discussed previously, mutual key authentication can be a strong tool. One such method for performing this is mutual authentication and key agreement (MAAKA). This is a method of authentication that has been proposed frequently but tends to fall short in the case of being provably secure and lightweight (PSL) solutions. This tends to be a problem as most of the systems are complex and have

a wide variety of requirements. The authors of [76] propose a new solution to create a PSL-MAAKA protocol. The protocol is kept lightweight by using hashing algorithms and XOR operations for authentication. Security is ensured by using a random oracle model. Through security analysis testing, a long list of properties proposed by the authors of [76], the paper proves that the PSL-MAAKA protocol out performs other schemes including, Ali et al.'s [77], Fotouhi et al.'s [78], Chang et al.'s [79] and Kumari et al.'s [80].

The authors of [81] propose another method of mutual authentication that ensures that both the source and destination are checked for integrity to prevent packet loss. The main focus of the authors is to defend against the black hole attack, a commonly forgotten attack. It is an attack in which a router deletes all messages it was supposed to forward. The proposed scheme is the combined use of medium access control and enhanced on-demand vector-enabled routing. Mobile devices must start a session with a registered device in order to begin communication. The encryption method used is the well-known elliptical-curve Diffie–Hellman method. Through simulation testing, they were able to prove the effectiveness of the scheme against multiple attacks with a high rate of success.

Mutual key authentication allows users to ensure that the data they collect are the same as the information sent. There are other methods that allow for the same authentication through a form of digital signature. The authors of [82] propose a method composed of four main parts: checksum computation, the novel left data mapping (LDM), the pixel repetition method (PRM), and RC4 encryption. PRM is used to upscale an input image. RC4 is then used to encrypt the binary secret data that are then grouped together in 3-bit groups that are then converted to decimal. Using LDM, the decimal digits are encoded and inserted into a cover image. To protect against taper, a checksum digit is created and inserted into a main diagonal pixel. If the image is tampered with, the checksum digit will not match when calculated again. This is a form of digital signature to check the authenticity of the data received. The experimental results collected by the authors of [82] show that the proposed system outperforms some of the best systems when focusing on computational complexity, the ability to detect tapering, payload, and imperceptibility.

- Encryption

Encryption is very important in the secure transport of information from IoMT to another location. One such method proposed by the authors of [83] suggests the use of the Rivest Cipher to generate a key value followed by the use of the Elliptic Curve Digital Signature Algorithm (ECDSA) to encrypt the value. Lastly, the value is hashed using SHA256. The proposed scheme is tested by the authors and proven to be sufficient against attacks.

With IoMT a lot of authors have looked for easy ways to transmit data from IoMT to servers. This leads us to the use of smartphones in today's society. They allow for easy transportation of data between users and healthcare professionals. The issue comes with communicating that sensitive data in a way that does not allow attackers to take advantage of the system of communication. The authors of [84] have proposed a method using blockchain and key authentication agreements. The protocol would provide a secure place for keys to be managed on the blockchain. This would allow for the secure transfer of keys between implanted devices, personal servers, and cloud servers. The data would then be accessible to appropriate users via the blockchain. The Automated Validation of

Internet Security Protocols and Applications (AVISPA) tool was used to perform tests on the proposed system and proved to be resilient against attacks.

Since the beginning of COVID-19, many physicians have moved to remote care for their patients, also known as telemonitoring. When doing so, doctors must transmit an extensive amount of patients' personal data. To keep the information safe, the authors of [85] have proposed a lightweight method of mutual authentication and secret key establishment protocol. The secret key agreement uses PUFs to allow devices to check the authenticity of a sensor node as well as a doctor's legitimacy before relaying information. The scheme has been robustly tested with the use of AVISPA tools and has performed well, preventing attacks such as MITM and using fewer systems than similar schemes.

Also influenced by the pandemic, the authors of [86] propose a time-bound group key authentication using extended chaotic maps. These time-bound group keys allow for groups of devices to authenticate each other for a short period of time. This function is low-cost as the device does not need to retrieve a key every time it connects to the application layer, rather than encrypting and decrypting every time like other methods. The chaotic maps' unpredictable nature makes them useful in the authentication and key-agreement process of the scheme.

For IoMT, it is important to protect the integrity and confidentiality of the data. The authors of [87], inspired by the pandemic, propose an Attribute-Based Encryption (ABE) method for providing user privacy and confidentiality. This method is a partially policy-hidden and large universe ABE model that is publicly traceable. An area of focus for the authors is that the amount of data is independent of the publicly available information; this allows for any amount of electronic health records (EHR) to be stored. In addition, any person who is in possession of the encryption key is able to easily track the data linked to it. The final area of focus of the system is that it will have fewer bilinear pairings, allowing for smaller costs during decryption.

A big concern with most encryption is the cost of encryption and decryption. Using traditional encryption, there is a large cost of computation, making it an unfeasible way for patients' data to be transferred in real time. The authors of [88] propose a lightweight and efficient encryption algorithm that could be used efficiently in the transferring of image data. The method uses two permutation methods to secure the image. This new encryption method takes into account 256 bits to be encrypted and then breaks them into 16 different blocks of 16 bits. They have tested the algorithm on multiple test images and, when compared to the current standard, have proved to be much more efficient when considering execution time when compared to other similar forms of encryption.

- Signcryption

  Encryption and electronic signatures are significant parts of the transfer of data securely. Signcryption is a system design that achieves privacy and authenticity without increasing the cost of computation by combining the digital signature and encryption algorithm. Other higher-cost models separate encryption from signing, creating a less cost-effective option. The authors of [89] propose the use of signcryption in conjunction with a publicly verifiable cloud-centric healthcare system. This system collects data from IoMT and outsources the data to the cloud server through the patient's smartphone. When tested by the authors, the scheme had less energy consumption compared to other related schemes.
- Intrusion Detection

As stated above, IoMT is rapidly expanding. IoMT is opening more avenues for attacks. Without an effective intrusion detection system, an attacker could steal sensitive data or severely affect patients' health. The authors of [90] propose a novel mobile agent-based intrusion detection system. The agents will employ machine learning algorithms in order to look for the signs of a breach. The agents are composed of a sensor agent, a cluster head agent, and a detective agent. Through the use of data collection and principle component analysis, the agents work together to find abnormalities in a network. By emulating different use case scenarios the authors were able to obtain promising results when considering accuracy.

- Security Evaluation
  Along with intrusion detection, there is a strong need for security evaluations in IoMT. An insecure medical device could cause massive amounts of health complications to large groups of people in a very short period of time. The authors of [91] propose a hierarchical model consisting of three steps. The first step is to use a fault tree (FT) on the infrastructure of the IoMT, which consists of cloud/fog/edge member systems. The second step is to go through the subbranches of the same member systems. The last step is to use FT on the continuous-time Markov chain of devices in the subsystems. The proposed model takes into account a variety of different failure points, including attacks on the system. The proposed evaluation method has the opportunity to greatly improve the security of current and future IoMT in the realm of cloud/fog/edge member systems.

In addition to security, some recent research works focusing on the Internet of Medical Things have worked on improving other design objectives such as performance [92].

Internet of Health Things

In the following, we discuss the security challenges and mechanisms of the Internet of Health Things (IoHT):

- Security Mechanisms
  - Encryption
    The authors of [93] propose a symmetric key encryption to be used in IoHT. The method has a lower computational and communication cost than its asymmetric counterpart. The authors solve this issue through the use of a low memory symmetric key generation model that mimics group secret key agreements. The authors of [94] break down flaws in a current encryption technique based on chaotic maps, a conditional shift algorithm, and a modified Mandelbrot set [95]. When simulating an attack, the authors only needed one plaintext-ciphertext pair. Using this information, the authors performed a chosen-plaintext attack (CPA) and were able to crack the scheme with little computational time. To improve the system, the authors of [94] suggest using confusion and diffusion based on Shannon's Theory [96]. Using the chaotic system, a substitution box can be created to satisfy the properties of confusion. To implement diffusion, a key from the Mandelbrot set can have XOR applied to the chaotic sequences and the image layer. The conditional shift algorithm should not use XOR on the key and original image. Using these improvements the authors agree that the initially proposed scheme can be implemented and used securely.
    Radio-frequency identification (RFID) is a resource constrained device that has had improvements in protection recently. Many access control systems use this type of device for high level security purposes. Such a device requires a lightweight cryptographic algorithm. The authors of [97] propose an algorithm

called SLIM, which is a 32-bit block cipher based on the structure of the Feistel network. Since it is a block cipher, it uses the same key for encryption and decryption allowing for it to be more lightweight. SLIM has demonstrated a strong ability to prevent attacks on RFIDs.
Another scheme to achieve security in IoHT is ciphertext-policy weighted attribute-based encryption (CP-WABE). But this system has several issues, including being non-scalable and requiring high computational cost, time, and memory. The authors of [98] propose some changes that, through theoretical and experimental analysis, have proven to be more efficient than CP-WABE. To resolve these issues, the authors use 0–1 encoding [99]. To make sure the scheme can run on a more inefficient system, offline/online encryption and outsourced decryption are used. Through experimental testing, the authors prove the scheme is more efficient than existing schemes.

- Signcryption
  One of the greatest concerns for security in IoHT is the authenticity of a patients' health records sent over the Internet. Along with this is the anonymity of the sender and receiver of the data needing to be preserved. The current methods of signcryption that use certificateless cryptography do not allow for security anonymity and the anonymity of the receiver at the same time. To solve this, the authors of [100] propose a form of signcryption based Hyperelliptic Curve Cryptosystem (HCC). The use of HCC in the proposed model creates lower computational costs to the system than in current systems that use cryptographic techniques such as RSA, elliptic curve cryptography (ECC), and bilinear pairing. Using the Random Oracle Model of testing, the authors were able to guarantee a high level of security when considering receiver anonymity, confidentiality, and unforgeability.
- Data Provenance
  Provisions in Data Provenance are important if it is to be accepted by stakeholders. The proposed system by the authors of [101] suggests the use of a lightweight federated learning and differential privacy to protect the privacy and security of the data. The method would work in conjunction with blockchain smart contracts to manage the authentication of federated nodes, trust management, and edge training. To fully support the encryption of the dataset, federated nodes use additive encryption while the blockchain performs multiplicative encryption. The system was tested with deep learning applications and COVID-19 patient datasets. The authors claim that these tests provide strong potential for use in the IoHT.

Although security is a critical design objective in the Internet of Health Things, it is not the only one. Researchers have studied other objectives such as performance [102], timeliness [103], and reliability [104] as well.

Internet of Bodies

In an Internet of Bodies, different kinds of worn, implanted, embedded or swallowed devices located in, on or around the human body are interconnected over a network. The Internet of Bodies has received a research focus in recent years. In one article [6] the authors deploy a programming framework for combining information from several source devices. This allows doctors to monitor and use multiple forms of data to better schedule computer-to-human interactions. In [105], the authors propose orthogonal and non-orthogonal capacitive body channel access schemes. A handful of optimization protocols are put in place to optimize the throughput of information while maintaining lower power costs. The

methods used are max-min rate, QoS sufficient operational regimes, and max-sum rate. The proposed scheme is tested sufficiently and proven to not degrade performance with larger networks. In our survey, we have not come across any paper reporting significant work on the security of this extension, except a few ones briefly discussing confidentiality in the physical layer [106,107].

Internet of Bio-Nano Things

The Internet of Bio-Nano Things is a recent extension of the IoT [108]. It is used in molecular biology [109], disease diagnosis [110], and related areas.To the best of our knowledge, the security of this extension has not been studied in any existing research report.

3.2.2. Extensions with Applications in Transportation

Internet of Vehicles (IoV)

The IoV is a distributed network of connected cars, RSUs, and central Cloud platforms. The IoV makes it possible to integrate smart vehicles with the Internet and, consequently, their environments, such as other vehicles, pedestrians, public infrastructures, computing nodes, and sensors. The IoV should definitely be considered as a significant trend in recent research on the IoT, especially since software-defined Internet of Vehicles has received research attention in recent years [111].

Although a wide range of objectives such as performance, mobility, reliability, and QoS have been considered in the design of the Internet of Vehicles, security is probably the most important one [112].

Security challenges faced by the Internet of Health Things, as well as security mechanisms used in this area, are listed below:

- Security Challenges
  - Privacy

    IoV is the collection of sensors and devices located in cars that connect to each other or to a central location. The data collected by these sensors usually consist of location information and the identity of the vehicle. The privacy of this information is paramount to the safety of the vehicle's owner. One method proposed by the authors of [113] is a Concerted Silence-based Location Privacy-Preserving Scheme. The method would create an unlinkable connection between the location services of a vehicle and the safety functionality of the vehicle. The identity of the vehicle on the network must enter a silence period in which the location of the vehicle is not shared before it is able to link to the location of the car. This will allow for a bit of unpredictability in location without making it impossible for there to be a link between the two. In the testing, it was proven to be successful in prevention when simulated against a global passive attacker. The authors of [114] propose a different method based on double k anonymity (reduces the correlation between requests and users while maintaining service quality) to help secure the link between the identity of a vehicle and its location. The method makes use of a cloud server as an intermediate stop for data between a vehicle and a service provider. In the cloud server, requests from the vehicle are reduced through the use of permutation and combination methods that involve the use of randomly generated matrixes. The authors tested the algorithm extensively to prove its safety and time efficiency.

    In location services of IoV, Geo-indistinguishability (Geo-Ind) is an important privacy concern. This provides location privacy but does not work if exposed to poorly reported locations. Testing performed by the authors of [115] has shown a probability of over 50% that the true location is reported incorrectly. To

correct Geo-Ind, the authors recommend adding an additional mechanism called Perturbation-Hidden. This would allow for the pseudo-locations of the user to be guaranteed. The mechanism used to perform this task will be a differential private exponential approach. To attain 100% plausible pseudo-locations, the authors implement dynamic programming.

Blockchain's involvement in the IoT has been important in recent years as more schemes are developed using its decentralized nature, which is fully secure, and information management abilities. The authors of [116] propose a scheme that uses blockchain in conjunction with federated learning to securely transmit learning model parameters instead of the actual data. Federated learning and blockchain, when integrated together, can prevent issues each of them have on their own. Federated learning on its own is susceptible to poisoning attacks, and blockchain is overly robust. The combination of the two allows for the system to work effectively and securely.

As mentioned earlier, routing vehicles through the use of location-based data brings about several privacy concerns. To combat these many challenges, the authors of [117] propose a Privacy-Preserving-based Secured Framework for the Internet of Vehicles (P2SF-IoV). The proposed method first uses blockchain technology to securely transmit the data. The blockchain then implements a deep learning algorithm known as the SLSTM technique. This is used to catch other types of attacks, such as malicious nodes or intrusion. The performance of the deep learning algorithm is then evaluated using IoT-Botnet and ToN-IoT datasets to help improve accuracy. The authors compare this method to blockchain and non-blockchain methods and found that it generally outperformed them in terms of detection rates, accuracy, and false alarm rates.

Vehicle-to-everything (V2X) communication is the ability of a vehicle to communicate with an entire network, which is composed of infrastructure, other vehicles, and pedestrians. An area that is important to maintain the security of such a network is authentication. In [118], the authors propose a scheme that takes advantage of blockchain to maintain privacy while lowering communication and storage costs. The authors use a form of blockchain known as CyberChain. This is coupled with a Privacy-Preserving Parallel Pedersen Commitment (P4C) to allow for stronger privacy. To further accelerate the authentication process, the authors use Diffused Practical Byzantine Fault Tolerance. These two algorithms allow for the low latency that is required in time-sensitive IoVs. Through simulation and qualitative analysis, the authors show that the proposed scheme has lower latency, communication and storage costs, and greater privacy than other similar methods.

In recent years, edge computing has become the center of attention in IoV. It eases congestion in vehicle networks, using end-to-end communication. This is performed by transmitting information to end nodes instead of the server, thereby reducing latency. The authors of [119] propose a secure service offloading method (SOME) that uses edge computing but is able to tackle some of the traditional edge computing issues. The scheme uses a software-defined network (SDN) to handle issues with quality of service, including resource conflicts and communication interruptions. These issues can cause the degradation of other similar schemes. Issues with privacy related to SDN cause a need for modification of current SDN systems. These are handled through the use of an offloading time for drivers, which creates a gap in the location of the vehicle and what can be observed by a server. SOME is evaluated through experiments conducted by the authors.

In most instances, the privacy of the IoV focuses mainly on location information. In some taxis, facial imaging data are collected. To protect these data, a new scheme that generates and restores facial images is proposed by the authors of [120]. The method first runs numerous perturbations based on the semantics of the image. Then, it is run through an adversarial network to generate a scrambled version of the original image. The key is then concealed steganographically in the image. A restorative network is able to read the key and understands how to decode the received image. Through experimental testing, the proposed scheme shows high detection resistance, better quality, and more secure filtering defense. To address the issues of MITM, impersonation, unlinkability, and traceability attacks, the authors of [121] suggest the use of a batch verification-based authentication mechanism that takes advantage of ECC techniques. This allows a vehicle to authenticate neighboring vehicles. The authors have compared this scheme to relevant schemes and have concluded that the proposed scheme offers better security and functionality than other similar methods.

- Trust

There are many issues with current systems of large network IoV communication. In the paper [122], the authors discuss some of the challenges faced by current models and other foreseeable challenges that these networks face. The challenges are broken into four categories including privacy of information, privacy of multi-party, trust, and consent of information sharing. Privacy of information must take into account the large volume of personal information being shared in the network. To create privacy the system implemented must use minimal amounts of information as an attack could leave this information vulnerable. The concern of multi-party privacy is taken into account as third party services can be breached and expose large amounts of personal data. Trust must be managed to allow nodes to safely share data with each other. The trust management system needs to be real-time to prevent bottlenecking in many systems. Lastly, consent to share information should be given by users when using these systems. Each of these categories is vital to the creation of a more secure system but may also have some trade-offs in terms of speed and efficiency in the network. The networks proposed below each take a different stance on what is important in these systems and how it should be approached.

Trust management is a tool used in networks that prevents malicious nodes from gaining access to sensitive information. In a study conducted in [123], the authors propose a novel hybrid trust management scheme. The scheme uses two steps to evaluate the trustworthiness of a node. The first step analyzes the trust of the node in the transport layer. The second step evaluates the trust of the node in the application layer. Through testing, the authors have concluded that the proposed scheme has a trust level of 75%, which is a notable improvement compared with state-of-the-art trust methods.

As more infrastructure and vehicles are being connected, the networks of communications are becoming more complex which makes it more difficult for messages to be reliable. The authors of [124] propose a trust management system that uses blockchain along with a reputation value scheme to gauge the probability that a message is accurate. Credibility and the ability of a vehicle to be able to influence the system is based on the reputation value. A value is decreased when the system receives false messages. The performance of the system is tested through simulations and proven to be accurate at detecting and limiting malicious vehi-

cles. Through the use of the blockchain-based method, the authors have created a secure way of storing data.

Video surveillance has been an increasing technology in IoV. The issue is that transmitting such large amounts of video data is strenuous on the resource limited systems in IoV. As a vehicle does not need to communicate directly to a server but can send video data to a much closer edge node, the use of edge computing can be used to resolve the issue. Many of these systems have trust-related issues during communication that can reveal sensitive data. In [125] the authors propose a trust-aware task offloading method designed to improve edge computing methods. This method is used to balance the load on edge nodes through the use of the Strength Pareto Evolutionary Algorithm 2 (SPEA2), which minimizes response time and increases layers of privacy. In experimental testing, the scheme was proven to be time efficient and has a high level of trust.

Trust management is important to the safety of people who use IoVs. One malicious user is capable of putting many lives in danger. There are many issues with current trust management systems, and they may cause failure in current schemes, including the lack of scalability, single points of failure, reduced quality in the system, and lack of availability. These systems can also inhibit real-time accuracy. The authors of [126] propose a method of blockchain-based adaptive trust management through the use of smart contracts that is able to combat the current issues in traditional trust management systems. The blockchain is used to securely mange the trust network and an incentive algorithm is employed to convince users to perform well. The use of blockchain sharding can reduce stress on the main blockchain and increase throughput of data. The current work has been tested and proven feasible in real world applications. Another Blockchain-based trust management system using smart contracts is proposed by the authors of [127]. The proposed scheme also uses physically unclonable functions (PUFs), certificates, and dynamic Proof of Work (PoW) algorithms. The blockchain is used to manage trusted vehicles. Once a vehicle has established trust, PUFs assign the vehicle a unique ID. RSU establishes certificates to preserve the privacy of vehicles. Dynamic PoW allows for the system to scale to the level of traffic, which, in turn, takes up fewer resources when it is not needed. Through security and performance analysis the system is proven to be feasible in IoV and is superior when compared to similar methods of trust management.

Many location-based emergency services used in the location of vehicles are very large IP-based networks. The issue with these systems is that they have high amounts of latency, problems with evenly disseminating information, and are vulnerable to attacks on the systems' trust. The authors of [128] propose an emergent semantic-based information-centric fog system. To help increase trust, the authors implement a semantic-based trustworthy routing scheme. This scheme would allow the system to detect fake nodes in the system. To do this, the authors implement fog nodes to maintain three different data structures: a forwarding information base, a pending interest table, and a content store. Using this information, the scheme is able to analyze the traffic effectively and find fake nodes from the network. Through testing, the system had a decrease in failure rate by 50% when compared to the traditional systems without fog networks or clouds.

As mentioned earlier, intelligent routing is an important system in IoV that could allow for a reduction in wasted time. That being said, with an increase in the IoV, there is a large influx of data that needs to be processed in real time. To help

combat this, the authors of [129] address issues in security, trust, and privacy, as well as propose a deep learning model to process the data. To do this it is proposed to use a lightweight 1D convolutional neural network (CNN) model. Through testing, it was shown to cause very little delay in real-time trust management.
Large scale networks in IoV are becoming an increasingly tough challenge for having good network performance while still managing trust in the network. In the article [130], the authors discuss a hardware trusted model to build a trust chain. This would allow for a high level of protection, a tested running environment, and trusted state attestation (the ability to prove its identity). To prevent more latency created by the trust management system, it is proposed to use a remote novel batch approach. Simulation testing has proved that the trustworthiness of the network is intact while not creating an overly latent network. As discussed above, larger networks create issues as each node in the network must be verified using a trust management scheme. The authors of [131] propose a scheme that takes advantage of the blockchain to limit the bottlenecking that can occur in other schemes. Blockchain allows for a system to be traceable, untamperable, unforgeable, and transparent in a network of vehicles. Through the use of the Dirichlet distribution, reputation regression, and revocation punishment, the scheme can manage and classify the trust of vehicles in the network. This model shows a strong ability to find malicious nodes in a network when tested via simulations.

- Attack Resilience
  In the IoV, the ability of a vehicle to defend against an attack is paramount to the safety of the passengers. One such attack, known as the Sybil Distributed Denial of Service (DDoS) Attack, has shown the vulnerabilities of edge node detection in current systems. The authors of [132] propose a Real-Time Edge Detection Scheme for Sybil DDoS. The authors designed an algorithm called Fast Quartile Deviation Check (FQDC) to catch and locate an attack. This algorithm is based on entropy theory and a modified version of other deviation algorithms such as Quartile Deviation [133,134]. Generalized Extreme Studentized Deviate (GESD) [135], Linear Regression and Confidence Interval. The authors modify the algorithm to have simple calculations, quick response, and low omission rates, to make it more applicable to IoV. When tested, the system detected all Sybil DDoS Attacks with an average alarm time of under 5 s.
  Another important area for attack resilience in a system is when considering vehicle-to-vehicle (V2V) communication. The authors of [136] propose a blockchain-based scheme to authenticate vehicles in real time. Since V2V communication must be in real time, the proposed scheme is free from low latency and heavy computation complexities through the use of blockchain technology. This technology creates blocks of information that are each hashed and shared with the corresponding vehicles. The hash function used in this scheme is SHA-1. Using the Pearson Correlation Coefficient, the correlation of communication rate is 0.9749 without an adversary and is calculated as 0.1282 when there is an adversary. This is performed while considering the Received Signal Strength Indicator. This proves that the scheme is an effective method of attack resilience.
- Confidentiality
  Improvements in sensor-enabled vehicles have led to the increased need for physical layer security (PLS). With the growing density of vehicular networks, PLS will become significantly more important. The authors of [137] propose a PLS framework for a network consisting of a legitimate receiver and an eavesdropper.

To capture the mobility of the communication channel, a double-Rayleigh fading channel is implemented. To measure the performance of the scheme average secrecy capacity and secrecy outage probability are presented. The two performance measures are then provided in alternative forms to be able to use them with a moment generating function. The tests show that the number of vehicles with signals that interfere will affect the system and that there is a correlation between the performance and the uncertainty of an eavesdropper's vehicle location.

- Security Mechanisms
  - Anomaly Detection
    Anomaly detection is the monitoring of data collected by a system to detect either false data or malicious activity. The use of SDN can be used to create systems that can help catch attackers that are targeting a specific node in the network. The authors of [138] propose a hybrid method that uses probabilistic data structures. The scheme is composed of four phases: (i) A monitoring scheme that takes advantage of Count-Min-Sketch as the probabilistic data structure that monitors and filters incoming traffic; (ii) A Bloom filter-based control scheme that is used to authenticate the nodes deemed suspicious; (iii) A quotient filter that is used to store malicious nodes; (iv) A hypperlog counter that measures the flow passing through switches to find malicious nodes with a high level of connection. Through experimental testing, the scheme has proven to be a strong candidate for anomaly detection when considering speed, accuracy, and efficiency in detection. Controller area network (CAN) bus anomaly detection is a form of detection specifically for attacks on the CAN bus protocol in certain vehicles. Many of the current CAN anomaly detection systems have poor performance rates. This tends to be from the lack of abnormal IoV data. The authors of [139] propose a method for message classification in IoV that establishes a weak model to classify redundant data. The method also allows for the classification of a broad range of data. The proposed method is able to decrease computational costs as well as time without taking away from the accuracy. The authors then propose an improved support vector domain description scheme. They add the Markov model and the Gaussian kernel function to reduce redundancies and false negatives. Testing of the method shows an increase in accuracy when compared to other models.
  - Signcryption
    As discussed earlier, edge computing is an advancing technology that has many applications in IoV. The use of edge computing with 5G networks allows for a scheme free from latency. In [140], the authors propose a multi-message and multi-receiver signcryption scheme that uses multicast channels. The issue with typical multicast channels is that they are prone to many attacks due to the fact that they are more exposed. The proposed scheme uses a certificateless setting to help with these challenges. This is because a key's security is dependent on the security of a channel. The method the authors use creates a pseudo partial key to be used on a public channel. The method also uses HCC because of the smaller key size allowing the scheme to be lighter weight. Through testing, the scheme shows that it has high security with a low cost of computation.
  - Authentication
    Security in the IoV is something that has not been studied enough in recent years. In [141], the authors propose a method of authentication through the use of a fog-based identity scheme. They do this through the use of two layers. The first layer of the scheme is a security authentication scheme outside the fog. The second layer is a security monitoring layer for all of the other vehicles in the network.

The authentication method used is a two-way form between the identity of the vehicle and a deep learning algorithm that conducts real-time security. Through testing, the scheme was proven to be accurate and able to adapt to the increasing number of high-speed networks in IoV.

Ad hoc networks allow for vehicles to connect in real time. This allows high levels of communication, but most of these communications happen on open channels. There are plenty of attacks, such as eavesdropping, which can take advantage of these channels, leaving users vulnerable. To help protect the location and identity of the vehicle, the authors of [142] propose a new key agreement and mutual authentication scheme using elliptic curve cryptography. Vehicles are grouped into clusters based on the location of their closest road-side unit. In each cluster, there is a designated cluster head. One area of authentication and session key creation is between a vehicle and its cluster head. The second area of authentication is between the vehicle and other vehicles around it. After analysis, the authors found that the scheme was able to defend against many of the attacks that happen on open channels for IoV. The authors of [143] propose a similar form of mutual authentication called three-byte-based Media Access Control. The architecture of the network is split into two chains: local and public. Similar to the previous scheme, the local chain is controlled by the cluster head in terms of authentication and communication. The public chain is controlled by the base station. To communicate the vehicles use their Media Access Control address and can alter the authentication by using the last 3 bytes of it. The constant use of those bytes allows the network to constantly authenticate and keep a high level of integrity. The system is able to remain lightweight as most of the heavy computation is performed through base stations and cluster heads. The scheme proved to be a usable method of authentication as it had very high detection rates, low computational costs, and low latency.

There are many different authentication methods but many are not lightweight which is very important in IoV (and many other resource-constrained devices). The authors of [144] introduce a lightweight key authentication protocol that enables a server and device to share a secret key. This can be used to create a secure session between the server and the device in a way that is more lightweight. Testing shows that the proposed scheme is more efficient in computation and communication costs than current systems while still maintaining security. This is performed through the use of XOR operations and SHA-3.

Quantum computing is a growing technology that raises concerns in most facets of cybersecurity. This could allow for solving some major cryptography problems in polynomial time. The authors of [145] propose a quantum-defended scheme that uses a novel certificateless data authentication protocol. The scheme is protected from quantum attacks using lattice-based cryptography. The use of this in conjunction with a blockchain allows the scheme to be secure while being more energy efficient and storage efficient than other methods for lightweight use in IoV.

To maintain the safety of the IoV, communication is happening constantly between vehicles and the infrastructure. This makes authentication important to the integrity of the system. To create a system that is able to keep the identity and location of a vehicle separate while allowing the authentication of the vehicle, the authors of [146] propose a conditional anonymous authentication method. The system uses a third party, called tracer, to allow for the scheme to reveal malicious vehicles falsely authenticating. The scheme uses group signatures and

pseudonyms to allow for a tracer to strongly identify malicious actors. For the authentication portion of the scheme, the authors propose a privacy-preserving authentication method that works in tandem with the third party tracer scheme to block abusive behavior on the network. The scheme uses multiple tracers when revealing a vehicle's identity in order to prevent the wrongful reveal of a trusted user on the network. The scheme uses a tracing key in a distributed manner that makes it impossible for a single tracer to reveal a vehicle. Through testing, the scheme was proven to be abuse-resistant and secure against malicious attackers.

- Fraud Detection

  Fraud detection has ample uses in IoV. In [147], the authors propose a spatio-temporal cost combination-based framework. This can be used in the detection of fraud in taxi driving. When the taxi first connects to the network, a predicted trajectory is created to determine the route the taxi would typically take. This is then used with a statistical model that is based off of three elements: time of travel, distribution trajectory, and the cost of travel. The real-time data are then collected and used to create graphs that can be monitored for abnormalities against the predicted statistical model. This is an example of an outlier detection algorithm being used to find a fraudulent actor in a network.

- Encryption

  SDNs are widely used in network management systems. The authors of [148] have previously presented a routing protocol that is able to use road-side units (RSU) in ad hoc networks for vehicles to route communications [149]. The authors upgrade the previous work with a scheme they call SURFER. The scheme takes advantage of the SDN architecture as well as a blockchain of RSUs to more efficiently route packages. The authors implement the scheme in two different ways. The first method is to utilize SURFER entirely inside the RSU network. This is similar to the previous work in all instances of communication except for infrastructure-to-infrastructure communication. The second method is to utilize the SURFER within the entire IoV network. This is a different communication method than the previous work. Each of the SURFER methods was proven to be effective through testing in the security and management of packet communication. SURFER-1 has a lower overall control overhead, traffic flow, and packet loss than SURFER-2, but the overall performance remains similar.

  With everything becoming connected into the infrastructure of IoV, security is becoming a big concern to the safety of these large scale networks. For this to be possible, much of the communication must happen over open channels. The authors of [150] propose a method using a blockchain-assisted certificateless key agreement protocol. As discussed in previously mentioned schemes, the authentication agreement happens with the cluster head and then with an RSU in order to establish secret keys. The cloud server collects information from the RSU to create a transaction. These transactions form blocks, which are then voted on using the practical Byzantine fault tolerance (PBFT) consensus algorithm [151] to apply the block into the blockchain. The scheme was tested through formal analysis and informal analysis, each of which proved that this scheme provides better security, lower communication costs, and offers more functionality than other similar models.

  The introduction of 5G has allowed for many advancements in real-time communication offered in IoV infrastructure. It is important to authenticate all of the information coming in to the system to allow for this kind of infrastructure to be usable. Many of the industry standard schemes have large amounts of delays,

lack of privacy, and reduced efficiency in communication. To handle this the authors of [152] propose the use of ECC along with Ant Colony Optimization On-demand Distance Vector protocol for the purpose of routing. The scheme takes advantage of three different components. The first one is the use of Certificate Authorities (CA) for key generation. The vehicle's unique number plate is used to create private-public key pairs when ECC is applied. The second component is the ability of the system to detect malicious vehicles. To do this, the system sends periodic messages and checks for an appropriate response. If the system receives multiple inappropriate responses, the vehicle is marked as malicious. The last component is the Ant Colony Optimization On-demand Distance Vector routing. The On-demand Distance Vector routing portion of the method is reactive and uses route discovery and route maintenance to find the best route. This is improved with Ant Colony Optimization which allows for a source vehicle to find the best route to a destination vehicle through multiple different vehicles. Through simulation testing, the scheme has shown higher throughput, lower delays, and lower routing overhead than other similar state-of-the-art methods.
In many cities, there is a missing component of privacy of user-data in toll transponders. In [153] the authors propose a privacy risk reduction model to improve the current toll transponder infrastructure in the city. The scheme uses a fully homomorphic encryption protocol. The scheme would be a post-quantum encryption method that works with a blockchain model. The privacy of this scheme is evaluated and found passable when compared to the European General Data Protection Regulation and the California Consumer Privacy Act requirements.

- Misbehavior Detection

  Misbehavior detection is similar to fraud detection in that it is used in finding harmful or potentially harmful actors in a network. Misbehavior detection monitors behavior in a network and flags traffic that is abnormal. Deep learning has also gained a lot of attention for misbehavior detection because of its non-linear mapping ability. The issue with this is that deep learning takes time to train and is very hard to scale. The authors of [154] propose a form of misbehavior detection that uses a broad learning system (BLS). This method performs a similar task to deep learning but consumes fewer resources and is in real time. Key features are found in raw data and used to establish the BLS. The system is updated with newly generated data using incremental learning. Through experiments, this scheme performs better than other deep learning algorithms in terms of time and computation costs while remaining accurate. Unlike deep learning, the proposed scheme is also scalable for use in the IoV.
  Many IoVs are vulnerable to cyber-attacks. This makes data integrity an important part of any IoV system. Many of the conventional ways of checking data integrity will not work in IoVs in terms of overhead and computation cost. Since many methods do not work in the IoV, there is a lack of protection, and an RSU can be hijacked. In [155], the authors propose a lightweight method to check data integrity and find malicious RSUs. The scheme uses a probabilistic model for checking messages between intelligent vehicles and RSUs to find malicious RSUs. The scheme uses information over a period of time to create the model. The scheme then uses a generalized likelihood ratio test to find the RSUs that are malicious as well as check the integrity of messages. Through simulation testing, the scheme shows a slight drop in latency and the number of bits communicated. The scheme also offers a 99% probability of detection.

- Intrusion Detection
  It is not always possible to make a system that is completely impervious to intrusion. That is why it is important to create a detection system that can find when a malicious actor has infiltrated a system. The authors of [156] propose a multitiered hybrid intrusion detection system. The system uses a signature to check the identity of actors in a system. The system also uses an anomaly detection algorithm to identify both known and unknown attacks in a system. Using testing, the scheme has proven to be a strong detection method against many different attacks and is capable of being implemented in real-time systems. Data vulnerability is something that is heavily focused on in the realm of the IoV. Controller area networks (CAN) are the most popular system implemented in vehicles today to allow for sensors in a single vehicle to work in conjunction. Many of these CAN implementations are not secure enough and are vulnerable to attacks, including DoS and Fuzzy attacks. In [157] the authors propose the use of deep learning techniques in intrusion detection to protect CAN. To detect malicious attacks the scheme is based on a VGG-16 architecture developed by a group of researchers at the University of Oxford in 2014. The scheme is trained on the CAN-intrusion dataset to train the deep learning algorithm on types of intrusion on CAN systems. Experimental testing has shown that 96% of intrusions are caught, and false positive rates are lowered in modern CAN intrusion detection systems.
- Falsification Detection
  In IoV the ability for smart traffic routing is made possible by the ability of each vehicle to share its route. These can be useful in routing shipments, but issues arise in most systems because of a lack of storage. This issue can be made worse by the falsification of data being pushed to such a system and overloading the storage. The method proposed by the authors of [158] is a heuristic distributed scheme. The routes submitted by a user either penalize or reward them based on the contacts' confirmation. Through the use of a time-homogeneous semi-Markov process, the system can check the accuracy of mobility patterns and then submit them to the cloud server via RSUs. The cloud then has the capability of calculating whether a vehicle is malicious. Theoretical models and simulations show that the model can effectively identify falsified data.
- Threat Hunting
  With IoV infrastructure becoming larger and more vast in devices, security threats are becoming extensively hard to predict. This leaves IoV open to a lot of different cyber-attacks. The authors of [159] investigate intelligent attacks on IoV and model the process of attack and defense through the Stackleberg game. The Stackleberg game allows the authors to minimize attacks while increasing defense. Through the model the authors were able to effectively create a defense model that was not influenced by what type of attack was performed, allowing for uniform defense. The solution proposed allows for balanced work and does not degrade the performance of the system.

Internet of Autonomous Vehicles

Improvements in video analytics in recent years have allowed for a tremendous amount of growth in the safety of autonomous vehicles. These improvements come with the added challenge of securely and reliably relaying video data. The authors of [160] propose a framework that implements both blockchain and multi-edge computing in autonomous vehicles. The use of these methods allows for a reduction in latency in the scheme. The

use of deep reinforcement learning is optimized through the use of two different processes. The Markov decision process is used in reducing latency and allowing for a greater amount of throughput. Then, an asynchronous advantage actor–critic algorithm improves the resource allocation of the model. Through testing, the authors were able to show that the scheme was effective at moving data quickly.

Internet of Connected Vehicles

Internet of Connected Vehicles (IoCV) has been used in urban services [161] and related areas.

Among security challenges and mechanisms related to the Internet of Connected Things, one may refer to the following:

- Security Challenges
  - Privacy
    Edge computing is a growing technology in the IoCV that takes much of the burden of communication off of the vehicles that tend to have a low amount of resources. Many of these edge computing systems have issues with privacy, including untrusted edge nodes, which can leave location data vulnerable to attackers. Most proposed systems offer security with trusted nodes but do not discuss the unavoidable untrusted nodes that are important to the system. The authors of [162] argued that the need for security and privacy provisions in the Internet of Connected Vehicles increases with mobility. They focused on the privacy considerations of communications between IoT layer vehicles and potentially untrusted edge controllers as these communications contain private information such as location and speed. They reviewed related privacy preservation approaches and observed that existing approaches assume both parties (vehicles and edge controllers) to be trusted, which is not the case in some real-world scenarios. To bridge this gap, they developed a differentially private data streaming system that injects noise into the IoT layer instead of the transportation infrastructure. Their method scales the noise on the basis of the data correlation. They evaluated their method and demonstrated that it outperforms state-of-the-art approaches.
    One of the biggest risks that the IoV faces is the lack of security in the intelligent terminals that are in all smart vehicles. These terminals can be taken attacked by malicious groups and threaten the safety of the vehicle. In [163] the authors propose two authentication protocols to protect the intelligent terminal. The first authentication protocol used is to examine the behavior of the user when using and entering the network. The second layer of authentication is a password. For this authentication method to be effective, the behavior must be kept private. No part of the authentication protocol reveals this information. In analyzing the protocol, it is shown to be effective in terms of computation and communication costs.
  - Attack Resilience
    Trust management is an important system in the IoCV but tends to be quite inefficient as they tend to assume that the number of road-side units are limited. The authors of [164] create a scheme and assume that RSUs are able to provide efficient communication to any vehicle. They propose a system in which all vehicles contact RSUs directly to obtain all traffic communications. This allows for a more reliable and controlled spread of traffic information that can be checked more easily for malicious activity. The method uses market trading in order to reduce the spread of malicious activity and reward the sharing of information

by weighing communications based on trustworthiness. Simulations prove the scheme to be effective at blocking malicious information from spreading.

Internet of Electric Vehicles

Internet of Electric Vehicles (IoEV) has been studied in many recent research reports [165]. A lot of articles focus on the safe transfer of energy from one vehicle to another or from vehicle to infrastructure. The authors of [166] propose a system of energy transfer that takes advantage of blockchain. All transactions are performed using smart contracts and are recorded through the blockchain. The smart contracts allow for optimal pricing and optimal energy allocation. A bidirectional auction approach based on the Bayesian approach is used to create a smart way of setting prices. Simulations can prove that this system improves the current energy sharing system drastically. Energy management is also an important design challenge in IoEV; see [167] for the details. There are no research works focusing on the security challenges or mechanisms in the Internet of Electric Vehicles.

3.2.3. Extensions with Applications in Physical Security

Internet of Surveillance Things

There are only a few research works focusing on the security of this extension:

- Security Challenges
  - Trust

    Image processing over multiple devices in the surveillance of smart cities is an important task in increasing safety. The ability of a system to be able to find similarities and differences in an image found from vastly different interconnected surveillance devices is called saliency detection and is currently lacking in IoST. In [168] the authors propose a scheme that uses co-saliency which allows the use of more accurate saliency in IoST than other saliency enabled devices. The first contribution is a neural network that is able to find semantics with different repetitive fields on a single device. The authors then offer a two-path communication system between IoST to allow for the comparison of surveillance information of different devices. The last contribution is a network refinement method that helps improve neural networks and better label semantic features. Using three public datasets, the authors showed that their proposed method was superior when compared to four other state-of-the-art schemes: CBCS [169], CBCS_S [169], CSHS [170], and CSDW [171].

3.2.4. Extensions with Applications in Industrial Control

Internet of Controllable Things

In recent years, Internet of Controllable Things (IoCT) has been studied in some research work. In [172] the authors propose an ensemble learning method and resource allocation scheme for the purpose of effectively scheduling remote automated observing systems (RAOS). RAOS are used to monitor environmental and meteorological elements for the purpose of efficiently collecting information. Bagging, AdaBoost, and Snapshot are all ensemble methods to capture features of clouds. These features are then applied to a CNN for classification. A cloud-edge framework is used in order to reduce communication stress on RAOSs as large amounts of data are transposed to the server. The scheme is tested experimentally and shows a high level of accuracy in cloud classification and is able to improve task allocation.

The authors are not aware of any research report relating to the security of the Internet of Controllable Things.

3.2.5. Extensions with Military Applications

Internet of Battlefield Things

Recent literature comes with some research work focusing on Internet of Battlefield Things (IoBT). Knowledge of enemy locations on a battlefield can heavily favor troops in battle. The authors of [173] propose a localization method for enemies, which uses soldier's locations and the direction in which they are shooting. This is performed through the use of particle swarm optimization and *k*-nearest neighbor (KNN)-based clustering algorithms. Together, they are able to predict the general area in which an enemy may be located. Testing of the algorithms shows promising results in terms of real-time results and accuracy for the prototype. A lot of these large scale systems are deployed using mobile edge connections. In the IoBT, there are many electronic countermeasures that can prevent a normal edge network from working. The authors of [174] propose a scheme that allows for connections in the edge network to move when a node is destroyed to allow for a more continuous connection. The problem is broken down into a lot of smaller sub-optimization problems using a heuristic algorithm to allow for the optimal connection. The proposed scheme is shown to have a lower time and energy consumption over the typical edge computing network when electronic countermeasures are in place. Among the design challenges of this extension, one may refer to energy efficiency, latency, and robustness [175]. So, each scheme needs to take these into account.

In our reviews, we have not found any research work related to the security of this extension.

3.2.6. Extensions with Applications in Agriculture

Internet of Trees

Internet of Trees is a recent extension of the IoT that can be used to monitor the health of trees. Trees and plants can be outfitted with sensors, which allows farmers to decrease over-watering and improve the quality of the plants that are being produced. The authors of [176] propose a system that works with electromagnetic sensors that use spectral dispersion to measure moisture content. The sensors are linked together to better understand how a group of trees may need to be watered most effectively. The network of trees is combined through a representative network system based on a long-range (LoRa) protocol. The system is proven to be low-cost as energy is collected through solar and can reduce the amount of water used in the agriculture of trees.

Security challenges and mechanisms of this extension have not been adequately studied in the literature.

Internet of Agro Things

Internet of Agro Things (IoAT) has been studied in some recent research works. Crop production and yield is increasingly important in areas that have limited land for production. The ability to monitor crops and understand what can be done to increase output can be enhanced with networks of sensors in the IoAT. In [177] the authors propose a CNN that is able to perform analysis on crop images. The sensor nodes collect images of plants to send to the CNN and are solar powered, reducing energy consumption. When tested in a 3-moth trial, it was shown to be 99% accurate and was able to sustain harsh weather.

The authors are not aware of any reported research focusing on the security of this extension.

3.2.7. Extensions with Applications in Entertainment

Internet of Media Things

Internet of Media Things has been studied in some recent research works [178].

Some variants of the Internet of Media Things are studied below:

- Internet of Video Things
  The Internet of Video Things connects things with visual sensors [179].
  Objectives such as scalability [180] have been considered in the design of the Internet of Video Things.
- Internet of Audio Things
  Internet of Audio Things refers to a network connecting physical objects called Audio Things with computing devices embedded inside them aiming at the production, transmission, and analysis of audio in distributed environments. There is a survey in this regard studied in Section 2.1.2 of Section 2 [25].

The Internet of Media Things has not been adequately studied from a security perspective.

Internet of Multimedia Things

The Internet of Multimedia Things is a recent extension of the IoT [181].

Researchers have considered the following security challenges and mechanisms in the design of this extension:

- Security Challenges
  - Confidentiality
    Low-cost compression while maintaining the confidentiality of the Internet of Multimedia Things would allow for major advancements in entertainment. The authors of [182] propose a low-cost and confidentiality-preserving multi-image compressed acquisition model. The scheme evenly groups images together using the sigmoid sequence, and each group is randomly assigned compressive sensing. The groups are then combined into a larger image and then encrypted to increase confidentiality. The image is sent to the cloud and run through a decryption algorithm. The cloud is able to use the designated reconstruction algorithm to recreate the image. Through simulations, the scheme has proven to be effective in confidentiality and cost in transmission of the images.
- Security Mechanisms
  - Authentication
    The Internet of Multimedia Things has many applications in other fields, including healthcare, surveillance, and the automotive industry. Each of these industries transmits large amounts of multimedia data. The authentication of edge devices on a network while protecting the privacy of user information is a large focus of the industry. In [183] the authors propose a multi-layer framework based on edge computing to solve the problem. The scheme provides security through a four-way handshake that happens between pre-made clusters. To keep privacy, the framework uses aggregation based on frame matching and a Label Distribution protocol-based technique that adds noise to the aggregation. When compared to existing privacy-preserving schemes, the proposed framework outperforms them based on a lower rate of error and data load.

3.2.8. Extensions with Social Applications

Internet of People

The Internet of People is a recent trend in research on the IoT that has led to a variety of different discoveries. The authors of [184] propose a method to improve the current recommendation systems that are becoming used more in areas such as social media searches. The algorithm they propose takes a user's relationship in a network and the

item's relationship in a network. To adjust weights of items in the system a tuning parameter is added. Objects that are not yet seen are extracted and ranked based on resource scores. Testing shows a high accuracy on top recommended items for given datasets.

Similar to the above, the authors of [185] create an interest detection framework based on social networks. Using similarities between different likes and dislikes of a user, a proximity function is able to create links between items. The scheme uses a greedy community detection algorithm to further find users with common likes and dislikes. Lastly, a link detection algorithm is used to create links between items that are commonly linked together using community information. When tested experimentally, the proposed method outperforms other deep learning schemes built for similar purposes.

To the best of the authors' knowledge, security challenges and mechanisms of this extension have not been adequately studied in existing research works.

Internet of Scholars

Internet of Scholars (IoS) has appeared in a few recent research reports. Scholars are having a more difficult time finding needed publications and scholarly connections as more publications are released. A recommendation tool specifically for scholars can be very useful. The authors of [186] introduce the idea of a scholarly friend recommendation system. Using academic social networks, the authors hope to help scholars find people who do research in areas that could benefit each other. The authors first construct an attributed social network using digital libraries. Attributed random walk is used to model scholar attributes and network structure. To create recommendations, a graph recurrent neural framework is used. The effectiveness of the model is shown when tested on information collected from ResearchGate and LinkedIn.

In our review, we have not found any research work focusing on the security of the Internet of Scholars.

Internet of Mobile Things

Internet of Mobile Things has also been recently studied in the literature. There are many applications that involve networks of mobile devices. Issues arise due to the computational limitations these devices have, which makes it difficult to send large amounts of data. In [187] the authors propose a scheme for fog computing based on Fountain codes, reducing latency and processing time of receiving positions of mobile devices. The fog computing scheme is able to offload tasks using its high computation power. The scheme takes advantage of maximum distance separable code allowing for the scheme to be highly flexible with low complexity. Testing shows that through the use of the Fountain code-based scheme the loads of transmission and communication are reduced.

This extension has not been studied from a security perspective in existing research works.

3.2.9. Extensions with Applications in Smart Homes

Internet of Kitchen Things

Internet of Kitchen Things (IoKT) has been of interest to some researchers in recent years. Many kitchen devices are being added into the world of the IoT such as refrigerators and ovens. When connected to a network, it offers a great amount of convenience to the users. It can allow users to preheat their ovens from work or see what items they need in the refrigerator while at the store. One area they struggle with is understanding the people they work for. The authors of [188] introduce the idea of TupperwareEarth which aims to reduce cooking tasks for users based on the network of IoKT. The system is designed to allow for real-time management of inventory. The scheme uses an ontology-based database to allow

the device to suggest recipes based on users' inventory, appliances, and preferences. User studies have proven it to be a useful tool in the kitchen.

Our survey has not led to the identification of any published research on the security of this extension.

3.2.10. Extensions with Applications in Critical Infrastructures

Internet of Energy

Some research work has discussed the Internet of Energy (IoE) as an extension of the IoT. As more data are transmitted, there are more areas for error such as receiving low-quality data. Further adding to issues, most devices must use edge networks to offload higher computational tasks. A lack of privacy among edge nodes, low-quality data being transmitted, and low-quality results from low-quality data all arise due to edge computing. The framework proposed by the authors of [189] consists of three main parts. A data quality evaluation is used to provide high-quality data to the blockchain. The next part is data repairing to fix any incomplete or low-quality data before being added to the blockchain. The last is distributed reinforcement learning for task arrangement for offloading tasks in an effective way that reduces the burden on nodes in the network. Numeric results show that the scheme is effective at offloading tasks.

Another scheme proposed by the authors of [190] is used in the preserving of energy due to shortages caused by COVID-19. The proposed scheme is able to better allow for the distribution of energy across a grid based on the needs of each area. Using edge-based architecture, the scheme creates an energy efficiency framework. Using an interface, users can monitor consumption and environmental data. Energy saving strategies based on the user's habits are also given to reduce potential waste. These calculations are created from a rule-based algorithm. This is one of the first instances, as far as the authors know, of implementing an energy saving recommender. The scheme proves effective as a prototype in giving effective strategies to lower energy usage.

To the best of the authors' knowledge, there is no published research related to the security of this extension.

3.3. IoT in the Sea

3.3.1. Internet of Ships (IoS)

The IoS refers to the interconnection of a large number of smart, physical devices or infrastructures associated with ships, ports, or maritime transportation systems, aiming at improved shipping industry in terms of efficiency, safety, and environmental sustainability. The IoS has found its applications a broad spectrum of scenarios, including collaborative decision making, route planning and optimization, cargo tracking, safety enhancements, automatic fault detection, preemptive maintenance, energy-efficient operations, automatic berthing and environmental monitoring [41].

There have been many recent developments in the IoS. Fault diagnosis in IoS is something that has been studied and handled through the use of deep learning to improve performance in shipping. In [191] the authors propose a fault tolerance scheme that uses a privacy-preserving federated learning approach. The scheme is able to, without data leakage, manage shipping agents to develop a model by sharing parameters. Federated learning is used to help with a lack of insufficient data to help in training a deep learning model. To protect fault data, the authors encrypt the parameters using a Paillier-based communication scheme. The fault diagnosis is handled by a control algorithm. This algorithm is adaptive and changes the model for training. Analysis of the method proves this to be an effective fault diagnosis scheme when tested on a fault dataset.

The Internet of Ships has not been studied from a security perspective in the current literature.

3.3.2. Internet of Underwater Things

The Internet of Underwater Things (IoUT) has been used in data aquisition [192], smart oceans [193] and similar areas.

Researchers have considered the following security challenges and mechanisms regarding the IoUT:

- Security Challenges
  - Privacy
    The IoUT is the network of devices used in sensing, communication, and controlling the environment. Recently, proposed schemes focus on information collection and position estimation in the IoUT. The localization systems proposed in these are based around an anchor node. In these schemes, location privacy is not correctly protected, which makes the anchor node vulnerable to attack. The authors of [194] propose a privacy-preserving localization system. The scheme uses a privacy-preserving asynchronous transmission protocol to detect malicious anchor nodes and hide the location information of anchor nodes while not being synchronized to a clock. To localize the target location, a privacy-preserving estimator with ray compensation is used to avoid localization bias. Through testing simulations and experiments, the authors prove the scheme to be an effective system of localization.

In addition to security, energy efficiency [195] has been considered as a design objective in recent research on the Internet of Underwater Things.

3.4. IoT in the Sky

3.4.1. Internet of ViSAR Vehicles

Industrial Video Synthetic Aperture Radar (ViSAR) is a new technology that is used in Unmanned Aerial Vehicles (UAV) for real-time surveillance. This has useful applications in monitoring natural disasters at night without the need for a source light. Most ViSAR vehicles take a large amount of bandwidth and have a low data rate of communication, making an effective system hard to design. The authors of [196] propose a loss-less data collection technique that eliminates redundant information from being communicated back, lowering the costs of data exchange. The scheme takes advantage of the method of reversible watermarking and combines it with dual-phase interpolation-based embedding. This method will use a greedy network of weights. Through the use of simulations, the proposed method is proven to be better than previous methods in terms of reliability, efficiency, and speed.

Our reviews have not led to the identification of any research report related to the security of this extension.

3.4.2. Internet of Aerial Vehicles

Air traffic management is becoming an ever-increasing area of focus for aerial vehicles. With this comes the security issues that are beginning to arise as more of these systems are designed. Current systems are unable to handle the amount of communication that will occur as more aerial vehicles need to be managed. The authors of [197] propose a method of advanced automatic-dependent surveillance-broadcasting (ADS-B) that allows for easy tracking and monitoring of aerial vehicles. To do this, the authors take advantage of a grouping-based conflict detection algorithm. The flight paths of aerial vehicles are then predicted using a combination of machine learning algorithms, long short-term memory

(LSTM), and deep sentence embedding-based trajectory prediction. Through testing the proposed scheme was proven to be able to detect conflicts within seconds.

Internet of Drones

A drone is an autonomous aerial vehicle. Internet of Drones are used in a variety of application areas, including civilian and military aerial photography, Cloud and Fog computing, Unmanned Aerial Vehicles (UAVs), Wireless Sensor Networks(WSNs), and mobile computing. Some recent research works have been focusing on the Internet of Drones [198]. The following security challenges and mechanisms have been studied in research works focusing on the Internet of Drones (IoD):

- Security Challenges
  - Privacy
    In recent years, there has been an increase in the use of drones in many different aspects, such as structural evaluations, public safety, and industrial settings. In many cases, the information being relayed back from these drones is sensitive, so it is important to make sure privacy is well-kept. The authors of [199] propose a privacy-aware authenticated key agreement scheme. This scheme does not require drones to store secret keys, which, in turn, creates a method that requires less storage in the limited space of the drones. To the best knowledge of the authors, this is the first time that the physical security of the drone has been studied. Third party communication and mobile edge computing are both supported in the authentication of the UAV. This is performed without losing privacy.
    In IoD, privacy during communication between a moving point and a ground unit is vital to the safety of the user and the drone. In [200] the authors propose a blockchain-based framework for securely managing data. The scheme is used as an access control between a drone and its ground unit by establishing a session key. All communication is published to the blockchain for management and review. A consensus-based algorithm verifies the information published to the blockchain. The Automated Validation of Internet Security Protocols and Applications (AVISPA) tool is used in testing and proves the security of the proposed scheme. Analysis of the scheme further demonstrates its high level of performance and security.
- Security Mechanisms
  - Authentication
    Many of the recently proposed schemes in IoD either degrade the efficiency of these devices or are proven completely insecure. The authors of [201] propose the use of ECC and symmetric key primitives to create a new authentication method between a specific user and the drone. The user is able to access the server through the network and a password. The server then tracks the flying area of the drone and is able to link it to the user once authenticated. To test the security of the method, the authors use the random oracle method.
    When it comes to authentication in IoD many proposed systems use centralized authentication. The issue with this is that these systems typically have single point of failure and struggle with cross-domain authentication. In [202], the authors propose a blockchain-based cross-domain authentication scheme to be used in tandem with 5G. The issues of storage limitation and authentication latency are areas blockchain struggles with. To mitigate these issues, there is a local private blockchain to support local actions. Only authorized individuals are able to view and mange devices on this. The authentication method used is a multi-

signature smart contract. This allows for authentication of terminals by using consortium blockchain. To securely transmit data, the parties negotiate a session key for communication. The method was analysed to prove its effectiveness and efficiency.

- Encryption
  The need for real-time data is useful in some types of drones. Instead of storing information on the server, it is sent directly to the user. For this to happen, there needs to be a high level of privacy. In [203], the authors propose a robust authenticated key management protocol. The scheme uses a high level Authenticated Encryption with Associated Data (AEAD) along with ECC and SHA-1. The scheme validates a user and allows for the creation of a session key for secure communication with the drone. A random oracle model is used to validate that the session key is secure. Compared to related authentication key management schemes, the proposed scheme has lower storage costs, overhead, and computational costs.
  Encryption in drones can be used in the creation of session keys to create secure channels for communication. In the process of creating this secure channel, it is important to maintain the anonymity of the drone and the user. The authors of [204] propose that in any session, there should be a focus on pseudonymity and unlinkability. If a protocol only used pseudonymity, then when communication is analyzed, the user's privacy could be breached. If a protocol only takes into account unlinkability, then a stolen drone could have its session key stolen. On the basis of these principles, the authors propose a system of first key agreement. The protocol works by first sending the drone a pseudonym, being used for the session, to the user. The user then decrypts the pseudonym using the password that the user obtains when registering the drone. The user then sends their pseudonym to the server. The server then creates two session keys sent to the drone with the user's pseudonym. Once decrypted, the drone sends the session key to the user to decrypt and verify with the server, which allows for an authenticated connection. Through testing of efficiency, the authors found that their protocol was more inefficient than other schemes, but when looking at other methods with key exchange protocols providing full forward secrecy, it was one of the most efficient in terms of computational costs.

Internet of Unmanned Aerial Vehicles (UAVs)

A UAV is a remotely controlled aerial vehicle. The Internet of UAVs has been studied in some recent research works [205].

It has found its applications in object tracking and similar areas [206].

The recent literature highlights the following security challenges and mechanisms with respect to the Internet of UAVs:

- Security Mechanisms
  - Malware Detection
    Advanced persistent threat (APT) has become one of the biggest threats to security in recent years. The IoT tends to have less secure structures than most systems, so APT is an especially egregious threat, especially for UAVs. If malware is inserted into a UAV, it is able to then communicate with a command and control center (C&C) which is responsible for communication with the drone. The current ideology behind malware detection is through the monitoring of behaviors when communicating with the C&C. This would typically work, but APT uses a low traffic mode that allows it to mix in normal communication to

confuse the malware detection system. The authors of [207] propose a way of detecting this attack. APT attacks use domain name systems (DNS) to locate C&C centers and will log information on the DNS logs each time. The logs can be observed for signs of malware. With this information, the authors proposed a malware detection scheme using string matching and Fourier transformation. To preprocess the data, the authors convert DNS time stamps of DNS requests into strings. Then to monitor the requests, the authors use a trained random forest model to identify suspicious activity in the logs and to alert to compromised UAVs. Through testing on datasets, analyzed by ATP security experts, the authors have found the proposed method to be 94% accurate.

3.5. IoT in Space

3.5.1. Internet of Remote Things

Internet of Remote Things (IoRT) has been of interest to researchers in recent years. Gateways are a way for terrestrial networks and IoRT to communicate and allow for IoRT services. Each gateway can possibly have different channel conditions, locations, and other varying parameters, which can affect the performance of communication. This makes gateway placement vital to how IoRT is able to communicate. The authors of [208] propose a way to effectively place gateways to minimize access distance and the number of gateways needing to be created. Distributed resource allocation (DRA) algorithms are designed using principles of alternating direction method of multipliers (ADMM). This allows the algorithm to find the total revenue and cost of gateway placement and cost of deployment and optimize them. A genetic-based gateway placement algorithm is then used based on the data given by the previous algorithms to offer a solution. The proposed scheme shows through testing its ability to effectively place gateways in a way that improves communication and lowers costs.

The authors are not aware of any research work related to security challenges or mechanisms of this extension.

3.5.2. Internet of Space Things

Recently, researchers have paid attention to the Internet of Space Things (IoST). Cube satellites are new types of satellites that offer global communication at low costs. They offer advantages over normal satellites, including short development to deployment and lower cost of development and deployment due to the off-the-shelf components. These make them great tools for creating large scale networks. An automatic network slicing framework for space-ground integrated networks is proposed by the authors of [209] to use these cube satellites to their full capabilities. The design tackles challenges such as dual objectives of route computation and is able to allocate resources to avoid service level agreement violations. The system being automatic means it does not require prior information in terms of resource availability to slice. To allow for low signaling overhead, the scheme uses an online segment routing-based approach to route communications. The authors have performed benchmark testing that has shown the usefulness and effectiveness of the proposed scheme for large network communication in the IoST.

According to our reviews, this extension has not been studied from a security perspective.

3.5.3. Internet of Satellites

Some research work has studied the Internet of Satellites in the area of anti-jamming technology as smart jamming has become more of a threat in recent years. The authors of [210] use the Stackelberg game and reinforcement learning to minimize the cost of creating an efficient anti-jamming protocol. To do this, the authors create the problem as a Stackelberg game for anti-jamming. The scheme for anti-jamming is broken into two

parts. To find the best routing that is available, the authors use a deep reinforcement learning routing algorithm. To make fast decisions, a fast response anti-jamming algorithm is implemented. The scheme uses these methods together to make the best decision for anti-jamming. The scheme shows low routing cost and solid anti-jamming protection when tested.

In our survey, we have not identified any published research focusing on the security of this extension.

3.6. Discussions

As suggested by the above discussions, commonly studied security challenges of IoT extensions can be illustrated by Figure 3. As seen in Figure 3, the main security challenges are privacy, trust, confidentiality, and attack resilience.

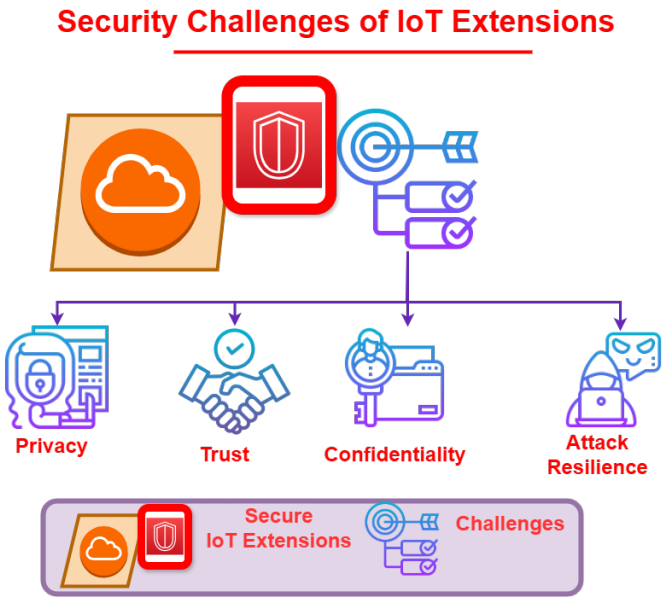


Figure 3. Security challenges of IoT extensions.

Similarly, prevailing security mechanisms used in IoT extensions can be seen in Figure 4. This figure highlights threat hunting, authentication, encryption, signcryption, misbehavior detection, falsification detection, security evaluation, intrusion detection, data provenance, anomaly detection, malware detection, and fraud detection as the main security mechanisms in IoT extensions (studied by the research community).

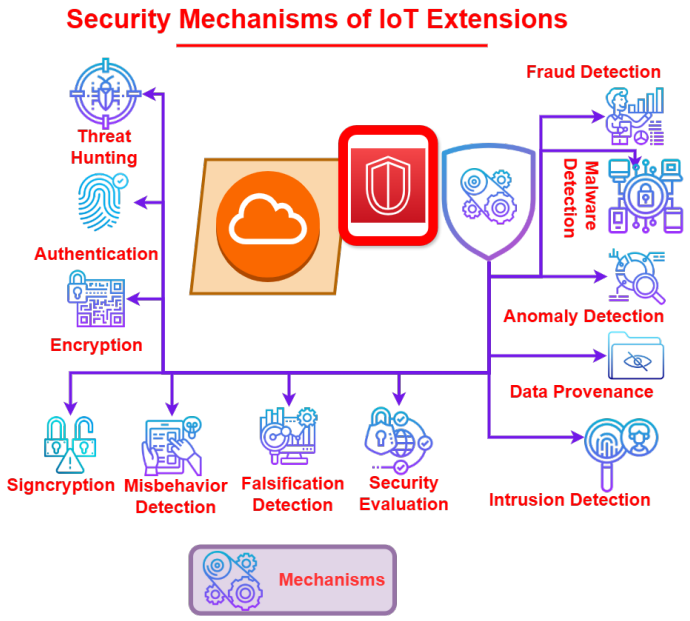


Figure 4. Security mechanisms of IoT extensions.

4. The Security-Oriented Taxonomy

Figure 5 illustrates the security-oriented taxonomy of IoT extensions as suggested by the discussions presented in Section 3. This taxonomy will become deeper and deeper as research goes on.

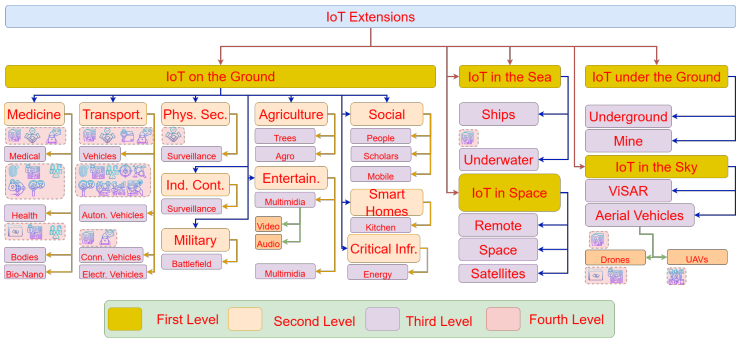


Figure 5. The security-oriented taxonomy of IoT extensions.

The taxonomy of Figure 5 classifies IoT extensions on the basis of their geographical deployment scopes (the first level), applications (the second level), and types (the third and the fourth levels). In some cases, the extensions have not been classified based on their applications. In such cases, the second level has been bypassed. The legend at the bottom of the figure designates the color coding used for representing different levels of the taxonomy.

In this figure, the names of the extensions have been shortened. The full names can be recovered according to the following instructions:

1. In boxes where the label is a noun in the plural form, the prefix "Internet of" should be added before the label. For example, a box labeled "Satellites" represents the Internet of Satellites.
2. For boxes where the label is an adjective in the singular form, and in addition to the prefix mentioned above, the postfix "Things" should be added after the label. For example, the box labeled "Underwater" represents the Internet of Underwater Things".

In Figure 5, and for each extension type, the well-studied security challenges and mechanisms are shown (using icons) above and below the related box, respectively. The

reference icons have already been introduced in Figures 3 and 4, respectively. For example, it can be seen in the figure that three security challenges (Privacy, Trust, and Attack Resilience) and five security mechanisms (Authentication, Encryption, Signcryption, Intrusion Detection, and Security Evaluation) have been studied with respect to the Internet of Medical Things.

5. Future Roadmap

This section tries to provide some directions for future research on secure IoT extensions. In Section 5.1, we mention some aspects of secure IoT extensions that have not been well addressed by the research community. This can be of assistance to those researchers who are interested in research on less-studied areas. To this end, we use the security-oriented taxonomy established in Section 4 (the main file). In Section 5.2, we present a future roadmap as an attempt to anticipate the future of secure IoT extensions. The latter subsection is useful for researchers who want to keep pace with current and future trends.

5.1. Less-Studied Aspects

As clearly seen in the taxonomy of Figure 5, not all existing IoT extensions have been well studied from a security perspective. For example, it can be easily seen that the security challenges and mechanisms have not been studied with regard to extensions deployed on the ground with military, social, or agricultural applications. The same goes for extensions with applications in entertainment, industrial control, smart homes, and infrastructures. Moreover, extensions deployed under the ground or in space have not undergone security-related investigations. Furthermore, there are extensions deployed in other geographical scopes (e.g., the Internet of ViSar Things and Internet of Ships) that have not been studied in terms of security. There are also other extensions with many unstudied security challenges or mechanisms. The lack of adequate studies on the security of the above-mentioned extensions makes room for future research.

5.2. A Future Look-Ahead: The Promise of AI

We anticipate that research on secure IoT extensions will quickly move toward *Quantum-Inspired AI-assisted secure IoT extensions* in the near future. The reason behind such anticipation is the existence of the trends discussed in Sections 5.2.1–5.2.3.

5.2.1. AI-Assisted IoT Extensions

AI-Assisted Internet of Vehicles

The IoV is a growing area where many different advancements and devices are being connected to the networks. UAVs are something that has a wide capability of monitoring traffic patterns and parking capacity in parking lots. The issue is that the privacy of communication of these two devices is vulnerable to attack. The authors of [211] propose a method based on Federated Learning (FL) to allow for privacy-preserving collaborative machine learning across networks allowing for UAVs to be used in IoV. The scheme uses a multi-dimensional contract that creates an environment for truthful reporting of information. The Gale–Shapley algorithm is used to identify the UAV that provides the most information at the lowest cost in a sub-region. Simulation verifies the efficiency of the matching used in the scheme while providing an optimal amount of security.

Resource allocation in intelligent transportation systems (ITS) is hard to manage due to the many different vehicular applications and time-varying network statuses. The authors of [212] believe that artificial intelligence algorithms are able to solve those challenges. The system they propose is an intent-based traffic control system. The system uses 5G-driven deep reinforcement learning algorithms to improve edge computing and content caching.

The system uses base stations and RSUs to execute tasks and deliver information to take the computation strain off the vehicles. To keep a high performing network of mobile operators and a high level of quality of experience a function optimizes both through a resource allocation algorithm. A mobile edge computing (MEC) protocol is used in the servers to create a mobility-aware and cache-efficient scheme. The MEC uses a Deep Deterministic Policy Gradient model to optimize task assignment and resource allocation. The scheme was tested experimentally using real traffic data and proven to be effective as an ITS.

Cooperative positioning (CP) allows for better lane alignment of vehicles, which improved the GPS, but in most schemes, they lack security and robustness. The authors of [213] propose a blockchain-enabled IoV that uses CP to improve GPS accuracy. The combination of the IoV and blockchain improves congestion in the network and improves security. The scheme uses a deep learning algorithm to predict the distance between the intelligent vehicle and a traffic sign. To ensure security, a smart contract system is implemented. Through simulation testing, the scheme was proven to be effective and accurate in positioning and secure when compared to other similar methods.

License plate numbers are used as unique identifiers on the roads. With so many new vehicles being added to the roads, it is important to have a way to securely use license plate recognition (LPR) to make the road ways safer. To increase the safety and usability of such systems, there needs to be sufficient privacy and resource allocation. In [214] the authors propose a federated learning-based LPR. The scheme will use the computing resources of a mobile device to lower latency and consumption. The scheme is designed to be deployable on mobile devices while maintaining accuracy. A correctional algorithm is designed to adjust for the angle in which the device reads license plates in order to maintain accuracy. Privacy and effectiveness of the model are validated through experimental testing.

Due to high mobility environments and multihop ad hoc networks, IoV suffers from weak links for communication. Many of the current proposed schemes in the literature fail to provide effective routing that can predict connectivity between two vehicles. The authors of [215] propose a machine learning and analytical compatibility-based ad hoc routing protocol. The scheme is able to estimate the compatibility time of all of the routes and choose the best one that allows for a longer connectivity time. This is to ensure the messages do not get interrupted as often. Location, speed, and directions are all factored into the equation in determining the best connection. When compared to similar schemes, the proposed method uses fewer paths of connection, ensuring more reliable communication.

The DDoS attack is currently one of the biggest threats to the IoV, flooding networks by exhausting caches and using up computing resources. This can, in most cases, be solved with a strongly developed intrusion detection system. Many of the challenges include the amount of resources IDS eats up, short links to vehicles, and limited cache and storage. In [216] the authors propose a way of fixing these issues through an effective data-driven IDS. This scheme will monitor RSU links instead of nodes on the network to avoid using up limited node resources. A convolutional neural network (CNN) is used for intrusion detection with seven layers. The CNN is constructed as a Bayesian hierarchical model to prove the convergence of the architecture.

AI-Assisted Internet of Connected Vehicles

Localization services are important to today's IoCVs and can improve the quality of transportation. The issue is that with most systems there are large amounts of overhead costs that prohibit them from being effective. The authors of [217] design a Behavior-based Clustering Method (BCM) to be a solution. The method observes vehicles in different time intervals and puts them in non-overlapping clusters based on their behavior. The authors then propose a Clustering-learning-based Predictive Localization (CLPL) algorithm

to predict distribution based on the BCM. This allows it to make long-term predictions. The scheme is compared to other approaches such as Co-operative Vehicle Localization Algorithm (CVLA) and neighbor-aided localization (NAL). The proposed algorithm outperforms them in terms of quickly stabilizing smaller clusters that include larger amounts of vehicles.

Localization services provide many different types of advantages to the IoCVs. One such advantage is the ability to collect data and map traffic. Traffic forecasting is not possible without internal connections between vehicles. Many of the current systems that do this are not dynamic enough to accurately predict realistic traffic scenarios. To solve this problem, the authors of [218] propose a graph neural network-driven traffic forecasting model (Gra-TF). The scheme uses graph convolutional networks (GCNs), Chebyshev networks (ChebNets), and graph attention networks (GATs) to find different predictions, and then the results are fused to build a more accurate and dynamic model. Based on conditions each model is weighed differently in the neural network when training. The authors believe this is the first application of a distributed learning-based approach to this problem. When tested on real traffic data from Los Angeles and compared to GATs and GCNs, the proposed scheme is able to perform thirty to forty percent more accurately.

AI-Assisted Internet of Medical Things

In the realm of IoMT, AI has the ability to predict the chance a patient gets lung cancer by looking at computed tomography. Current applications are still in development and have a low detection rate. The authors of [219] propose an integrated deep learning algorithm. CT images are first preprocessed through a variety of methods, including segmentation, and then, using intelligent algorithms, lung parenchyma is extracted. CNN and a residual network are trained using the images on a variety of cancer positive and negative images. Once trained, the features from the networks are imported into a long short-term memory (LSTM) model. Testing of the model has proven it to be promisingly effective in detection and is able to mitigate issues of interference.

Deep learning has many applications for finding and predicting health irregularities. One such application in the early detection of cardiovascular disease. In a study conducted in [220], the authors propose STM32 micro controller combined with temperature, a sphygmomanometer cuff, and a pulse sensor to create an effective prediction scheme. The scheme uses supervised learning that applies regression analysis. The model is trained to find correlations between independent and dependent variables in order to create a neural network capable of identifying cardiovascular disease based on information collected from IoMT. This study shows the effectiveness of the proposed model and its applications in vascular heart disease scanning.

Blockchain and federated learning are commonly used today in creating a secure data sharing model. The main issue with current models is they do not perform well when data in clusters is sparse. To improve this a larger network consisting of more devices can be used but this can increase latency. The authors of [221] propose a way to fix this by taking larger clusters and splitting them into smaller clusters based on geography. The scheme used is a cross-cluster federated learning system. The scheme takes advantage of cross-chain technology to improve the functionality. Experimental analysis proves the feasibility and efficiency of the proposed model.

AI-Assisted Internet of Health Things

Since most devices in the IoHT are limited in storage and computing resources they need to be able to efficiently offload to more capable systems. Edge computing is one solution that is used in many IoHT networks. Issues such as competition among devices,

communication restraints, and lack of global state information (GSI) make these systems ineffective. The authors of [5] look at the offloading problem in edge computing as an adversarial multi-armed bandit (MAB) problem. To solve the problem, the authors create an ultra-reliable and low latency communication (URLLC) aware task offloading scheme. The system is based on the exponential weight algorithm that is for the use of exploration and exploitation. URLLC is a set of constraints that goes beyond what most schemes focus on in terms of efficiency and reliability. The use of URLLC awareness is proposed by using a queue on URLLC constraints to more accurately categorize them. The scheme uses learning-based task offloading to find optimal performance, keeping in mind the URLLC constraints using location information. This is performed by first introducing a problem based on Lyapunov optimization. URLLC task offloading-GSI is used with the ideal case of GSI. The authors extend this by allowing for it to work with non ideal cases of GSI. Intensive simulations and analysis show that the proposed scheme can reduce task queue backlog, eliminate URLLC constraint therefore reducing queuing delay and improving convergence speed, and reduce energy consumption.

Wearable devices such as smartwatches have allowed for an increase in human activity recognition (HAR). In [222] the authors propose a deep-learning enhanced HAR for use in IoHT. The system uses a semi-supervised design in conjunction with an auto-labeling module. This is then used with a long short-term memory (LSTM)-based classification module to analyze weakly labeled data to better train a classifier. The auto-labeling scheme uses a deep Q-network (DQN) applied to a distance-based reward system, which can more efficiently categorize weakly labeled data. The use of LSTM allows the model to better collect sequential data and find hard to see patterns. When tested and compared to other similar methods, the proposed scheme is shown to be effective.

AI-Assisted Internet of Energy

Energy generation by renewable sources tends to be uncertain as it relies on natural factors such as the wind, sun, and weather. To better improve the stability of power systems, distributed generation units (DGs) are used with virtual power plants (VPP) to allow for large scale networks of DGs. The effectiveness of these systems is based on reliable connections between DGs and between the generation side and load side. In [223], the authors propose a deep reinforcement learning algorithm to find online economic solutions in VPPs. The first contribution is the use of a non-linear function to allow for better reliability in a realistic VPP setting. Due to the randomness of DGs in a system the use of a deep learning reinforcement algorithm is able to effectively solve the economic dispatch problem for VPPs. To reduce latency further, the system used to implement this will take advantage of edge computing in three layers. The first two layers are edge computing, while the third layer is cloud computing. The first layer collects information from the generation side and load side of the network. The second layer manages demand responses and energy transfer in a local area. The third layer is used for training the central node and further processing the entire network's communication. When tested against the deterministic policy gradient (DPG) algorithm and deep DPG, the proposed algorithm outperformed them in terms of time complexity.

In the Internet of Energy (IoE), microgrids have become an increasingly popular subject. They are a hierarchical distribution of different types of DGs. Because of the uncertainties tied to renewable energy these systems lack the capability of accurately scheduling power. A hierarchical microgrid model is proposed by the authors of [224]. To allow for a realistic model, the authors consider communication uncertainty. Similar to the previous model, this scheme uses a distribution deep reinforcement learning algorithm to solve the renewable energy accommodation capacity in the model. The scheme uses a

temporal difference generation adversarial network as opposed to the previous scheme's edge computing network. The proposed network is able to adapt to the deep reinforcement algorithm, improving its speed and allowing it to use the optimal strategy. Simulations show the effectiveness of the proposed scheme to increase the capacity of power scheduling and renewable energy accommodation.

Safe operation of power systems relies on many aspects one being transient stability assessment (TSA). One of the biggest threats to a system is a major collapse. Other methods are only able to assess the state of the TSA. They are unable to infer events that could lead to such a collapse. In [225] the authors propose a Gated Graph Neural Network to track TSA as well as infer events that could lead to collapse. A Conditional Generative Adversarial Network (CGAN) is used to create a training set that allows for effective recognition of transient instability. The model was tested using the New England 39-bus system and was able to effectively identify the event that could lead to instability in the network.

AI-Assisted Internet of UAVs

UAVs have become an emerging technology with lots of applications and one such application is in sensing. With the use of a cellular Internet of UAVs they could openly communicate across cellular networks and allow them to communicate with base stations further out. To take advantage of cellular networks the authors of [226] propose a scheme that allows UAVs to use cooperative sensing and transmission to decrease latency in information communication. The main challenge the scheme faces is cooperative sensing and transmission can interfere with trajectory of UAVs. The model uses a trajectory design problem based on the Markov decision process and use a deep reinforcement learning algorithm to solve it. The use of deep reinforcement learning is proven to outperform deep deterministic policy gradient and a deep Q-network algorithms when tested in this application.

Another application of UAVs is in the field of monitoring large fields of agriculture. Due to the large amount of data collected, nodes can not meet the needs of the drones. To fix the related issues, the authors of [7] propose a data collection method for air-to-ground communication. The proposed scheme is a bandwidth-weighted traffic pushing optimization (BWPTO) algorithm that uses a deep Q-learning (DQL) network to allow for the network to adapt to future changes. The ability of the network to adapt allows for maximum efficiency in data distribution. Mathematical experiments show optimal routing and a dynamic data collection system that is effective in air-to-ground communication.

In a study conducted in [227], the authors use UAVs to track target vehicles by employing a pretrained CNN. This method is highly effective but consumes large amounts of resources due to the need for accuracy and delay requirements. The authors employ the use of a mobile edge computing scheme to offload the heavy computational cost of the CNN. The system will allow for the UAVs to do low level computations but pass off more complex and consuming tasks of the CNN to edge nodes in the server. To effectively distribute the tasks a weighted-sum cost algorithm is used taking the parameters of tracking delay and energy consumption. The algorithm is able to maximize quality and avoid interference errors. Numerical and analytical results show the effectiveness when comparing this model against a model that does not offload high computational tasks of the CNN.

AI-Assisted Internet of Remote Things

The Internet of Remote Things (IoRT) has many challenges due to its remote location sensors. One solution to solving inaccessibility is to use satellites that offer a wide area of coverage. The issues to overcome for satellites to be viable include dynamic environments, which affect solar in-feed and channel conditions. The authors of [228] offer the solution of

a model-free reinforcement learning (RL) framework that can be used for joint resource scheduling. This would allow the most amount of data to be transmitted over the network. For effective use of model-free RL the authors make several contributions. The first contribution is formulating a resource allocation for the IoRT data scheduling (RAIDS) problem. This allows for model-free RL to adapt to realistic environmental factors and is rewarded for optimizing performance based on conditions. The system is rewarded based on a state-action reward-state-action (SARSA)-based actor–critic reinforcement learning strategy. This will allow the system to optimize resource allocation and create an environment that allows for the most data to be uploaded in a single period. Simulations have proven the effectiveness of the scheme in terms of learning and resource allocation.

AI-Assisted Internet of Underwater Things

The IoUT is an area that struggles with localization due to its mobility, asynchronous time clock, and stratification. Sensor node estimation has to be fairly exact for IoUT to be effective at sensing and communication. In [229] the authors propose some concepts to solve issues related to the uncertainties of location estimation. The authors provide a hybrid network that includes surface buoys, autonomous underwater vehicles (AUV), and sensor nodes. The scheme employs an AUV-aided asynchronous localization protocol that is able to use ray compensation and motion to handle the asynchronous clock, mobility, and stratification in IoUT. An RL-based localization algorithm can be used to attain the most optimized solution for communication between sensor nodes, AUVs, and surface vehicles. When tested the scheme is proven to have stronger localization performance than other similar methods.

AI-Assisted Internet of Controllable Things

Underwater communication is important to the exploration of the world's oceans. Most communication suffers from large latency due to the environment it is communicating in. Underwater optical communication is a way of communicating through the use of light. This allows for a very low latency and an easy way to transmit data. To be able to do this the authors of [230] propose a communication system based on single and superposition of Laguerre–Gaussian modes. The system uses a CNN for the purpose of identifying the mode in an underwater environment. The CNN is trained using transfer learning to increase the training speed. When tested the system is shown to have a package drop rate of 0% in clear and turbid water. The scheme is 90% accurate in different water turbulent conditions.

URLLC is extremely important to communication between devices in the Internet of Controllable Things. The authors of [231] propose a fast-convergent deep reinforcement learning for joint subcarrier-power allocation. This will be used in building a device-to-device (D2D) network. Each subcarrier is able to connect to multiple D2D pairs, and D2D pairs can connect to multiple subcarriers. The authors model the problem as a Markov decision model. The proposed solution is a double deep Q-network (DQN)-based resource allocation algorithm. If a system is missing full channel state information (CSI) then DQN-based resource allocation still allows for the system to be optimized. The system is very scalable as most communication happens between neighbors, vastly reducing overhead. D2D pairs act as learning agents for the system, allowing it to train quickly. Simulation testing shows that the subcarrier-power allocation can be performed in real time, given delayed CSI and quality of service feedback.

AI-Assisted Internet of Vessels

As discussed in previous sections, communication in underwater environments is difficult as it changes rapidly. The authors of [232] propose an orthogonal frequency division multiplexing (OFDM) auto-encoder that uses CNN-based channel estimation. The

CNN allows the OFDM auto-encoder to optimize learning and improves block error rate. LSTM layers are used for channel coding gain. The LSTM layers encode the message before transmission and are able to extract correlated information for detection. The proposed method solves gradient vanishing, which occurs in CNNs and has a high level of accuracy.

AI-Assisted Internet of Video Things

The Internet of Video Things (IoVT) has many applications in many different field ranging from vehicles to surveillance. One such category of study is using the IoVT to understand human behavior. A system able to do this requires a large amount of computational resources, which many IoVTs do not have. In [233], the authors propose a novel practical hierarchical and multi-modal architecture to understand human behavior. To encode the spatial and temporal information from videos, the scheme uses a deep learning model. For the purpose of language description, the model uses deep RL. Tensor-Train decomposition is able to factorize a hidden inference weight matrix, reducingthe training cost of the model. To optimize tensor decomposition further, a genetic algorithm is used to find the best rank. When tested, the scheme is proven to be able to compete with other state-of-the-art schemes.

5.2.2. AI-Assisted Secure IoT Extensions

AI-Assisted Secure Internet of Vehicles

As discussed in Section 3.2.2 (the main file), privacy in the Internet of Vehicles is important to a secure IoV network. In the IoV, the main concerns with privacy are user identity and location when using localization applications. Many of these systems either do not securely mask this information or use delay as a way to provide location privacy (this makes a real-time system impossible). To tackle these issues, the authors of [234] propose a data collection and preprocessing scheme that uses deep learning algorithms. The architecture of the network is based on edge computing. An adaptive transmission algorithm is used and adapts to the best method based on the quality of service evaluation. The scheme will use semisupervised learning for data augmentation and label guessing. It is able to identify data that are similar and process it faster reducing a time delay. Federated learning is used in the cloud server, which collects information from edge nodes so as to provide more privacy for users. Experiments show that the scheme is able to effectively reduce data uploaded by reducing redundant data, which, in turn, reduces the latency of the system.

Another important aspect of security is the ability of a system to identify and remove misbehaving actors in the network. In [235], the authors propose a deep learning-based classification framework that works with edge computing to find vehicles that are sending communication that may be harmful to the network. The deep learning algorithm is a combination of stacked LSTM and CNN-LSTM. Together, they are able to find complex patterns in communication, allowing them to identify and remove misbehaving vehicles from the network. The deep learning algorithms are also able to classify the misbehaving actors into faults and attacks. Edge computing removes the strain of computation and communication from the vehicles to allow for a less latent and better-performing system. Testing of the scheme shows that it is a better option for fault and attack detection than other similar methods.

Ad hoc networks in IoV are dynamic network topologies that have led to much of the advancement in IoV. High mobility, heterogeneity, and unstable connectivity make these networks unreliable in some settings. The authors of [236] propose the use of an edge-computing-based secure, efficient, and intelligent multitier heterogeneous IoVs network. Like the previously proposed scheme, this scheme uses a stacked LSTM to identify

malicious actors in the network. A testing of the network shows the lack of strain on the vehicles, and the deep learning algorithm shows a high level of accuracy in identifying malicious actors.

It is paramount to the safety of a system that there is correctness of data exchange. Most misbehavior systems, due to rapid dynamics, do not securely defend a vehicle. The authors of [237] propose a data-centric supervised machine learning approach to misbehavior detection with integrated plausibility checks. The system uses two plausibility checks. The first check is location, which checks the GPS against the predicted range of the vehicle. The second one is a movement plausibility check, which checks the velocity of the vehicle calculated from GPS against the velocity the vehicle sends back. Through experimental testing of a variety of supervised machine learning methods, the authors determined that, with the help of plausibility checks, ensemble algorithms outperform the rest in terms of error rates and are implemented into the system. The proposed algorithm is proven to be the most effective in terms of supervised machine learning when tested against the Vehicular Reference Misbehavior (VeReMi) dataset. Tests with and without plausibility checks show that the checks increase the accuracy and performance of the misbehavior detection system.

Large amounts of data are transmitted over IoV networks. When the information can be analyzed together, the quality of service and experience can be improved. Issues such as bandwidth and privacy can make it hard to effectively share the information required for such a system to work. In [238] the authors propose a federated learning-based architecture that is able to help with privacy and better disseminate information across the network. The architecture is a hybrid blockchain that uses the main permissioned blockchain. The blockchain is maintained by RSUs as well as Directed Acyclic Graphs (DAGs), allowing for a better data sharing scheme. Federated learning is used to find the nodes that minimize the total cost of communication. Learned parameters and verification of parameters are then implemented into the blockchain in order to enhance the reliability of the learned models. When tested numerically, the scheme was proven to be effective with regard to accuracy and efficiency.

AI-Assisted Secure Internet of Medical Things

Increased use of machine learning in the IoMT has led to concerns with data privacy. To allow for a more secure system, the authors of [239] propose a privacy-preserving outsourced support vector machine scheme (EPoSVM). A distributed two-trapdoor public-key cryptosystem was used to design a security protocol. To increase the speed of the encryption process, the authors implement a secure data partitioning protocol that limits the bit length, removing the need for a system to collect message length. Then, using the secure protocols, the scheme outsources the training of the SVM to a gradient descent-based training model. Secure Outsourced SVM Classification is performed when the service requester uploads their encrypted data to the cloud for a secure classification. The cloud returns a ciphertext only able to be decrpyted by the service requester. Through testing the scheme is proven to be secure and provide reliable and accurate classifications.

Data privacy is an important concern, but there are other concerns that have to do with the security of IoMT, including trust, integrity of data, real-time processing, and network constraints. Behavior detection and a robust approach to maintaining the integrity of data are important to a secure system. With this in mind, the authors of [240] propose a scheme that eliminates and identifies malicious nodes, thus allowing it to be a robust network. To evaluate the degree of trust for a node, the scheme uses a NeuroTrust method that provides reliability, packet delivery, and compatibility. Through the use of homomorphic encryption, the method can remain lightweight and efficient while protecting data integrity

and confidentiality. Simulations prove the system to be effective in terms of accuracy, computation cost, and ability to identify and remove malicious nodes.

Authentication is an important part of security that needs to be effectively implemented in every system. In [241], the authors propose a lightweight and practical anonymous authentication protocol that can resist machine learning attacks on PUFs. The scheme is split into two steps: registration and authentication. Each device must first be registered with the server. In authentication, the server checks the device's identity and then allows it to enter the server if authenticated. To the authors' best knowledge, this is the first time that a PUF-based authentication scheme can prevent attacks from machine learning algorithms. To test the scheme, it was analyzed with a strict analysis scheme and proven to be able to resist attacks.

The ability of a network to safely encrypt and decrypt images is useful in the medical field as most images include sensitive information. The authors of [242] propose a deep-learning-based image encryption and decryption network. Deep learning is applied to an image-to-image transformation. The encryption method used is one time pad and is sensitive to key change. Region of interest mining is used to find the interested segmentation of the image instead of decrpyting the ciphertext first. After experimental testing using X-Ray datasets, the scheme is proven to be secure and cost-efficient in terms of computation and time. To the authors' best knowledge, this is the first time deep learning has been implemented in the encryption of images in the IoMT.

AI-Assisted Secure Internet of Drones

Drones collect a lot of information such as location and HD images. When connected, they are able to create a large network of distributed information. This makes it paramount for this kind of network to maintain data integrity, security, and privacy. To protect these elements, the authors of [243] propose a blockchain-based security mechanism that allows drones to communicate securely. The blockchain protocol consists of three phases. Registration of a drone or device on the blockchain is the first phase. The second phase is to verify the identity of a device or drone trying to access the blockchain. This is performed through the use of a zero-knowledge proof protocol. The last phase is the transaction phase, which allows for devices to securely communicate over the network. Before any block can be added to the blockchain, it must be mined first to check for data tampering. A mining node is selected using a deep learning-based selection miner algorithm using a deep Boltzmann machine. The scheme was tested using a variety of performance metrics and shown to be a promising way for IoD to securely communicate.

Another relevant research has been reported in [244], where the authors argued that the aggregation of raw data gathered by individual drones in the fog node can incur privacy leakage in Fog-aided Internet of Drones. They proposed a method based on Federated Learning (FL) for local training in drones and sharing training model parameters in the fog in order to preserve data privacy. They augmented their method with techniques for power control in drones in order to keep privacy from being divulged to ground eavesdroppers via wiretapping and parameter analysis during the FL training process.

5.2.3. Quantum-Inspired AI

Although AI has made much progress in recent years, there are still some challenges, including reasoning under uncertainty, adaptive ML, and neuromorphic cognitive models. Quantum-inspired AI, which means using quantum computing for ML and DL algorithms, is one of the solutions that can help AI level up and overcome these challenges. Adopting quantum computing concepts and techniques can improve AI by improving decision

making capabilities in complex scenarios, optimizing ML algorithms, and speeding up the training phase of ML models [245,246].

Quantum-inspired AI has yielded promising results in several applications. For example, the authors of [247] have used Quantum-inspired Reinforcement Learning (QiRL) to plan the trajectory of Unmanned Aerial Vehicles (UAVs). QiRL method adopts a novel probabilistic action selection policy and a new reinforcement strategy, which are inspired by the collapse phenomenon and amplitude amplification in quantum computation theory, respectively. In another work, the authors have applied a quantum-inspired experience relay to traditional deep reinforcement learning [248]. They showed on Atari 2600 games that deep reinforcement learning with a quantum-inspired experience relay can improve training efficiency.

The authors of [249] have developed two quantum-inspired multidirectional associative memories. The first uses a one-shot learning model, and the second uses a self-convergent iterative learning model. They used these models to show the advantages of quantum-inspired multidirectional associative memory, such as stability and reliability. Moreover, a QiRL algorithm for autonomous robot navigation has been proposed in [250]. Experiments show that this approach is more robust than traditional reinforcement learning algorithms.

Finally, a quantum-inspired fuzzy neural network has been presented in [251] for two-class classification. Neurons are added to the hidden layer via fuzzy c-means clustering, with the fuzziness parameter being developed from quantum computing. Additionally, this network uses a modified step activation function. Experiments showed that this scheme outperforms state-of-the-art methods.

Figure 6 illustrates the future of secure IoT extensions as suggested by the trends discussed above.

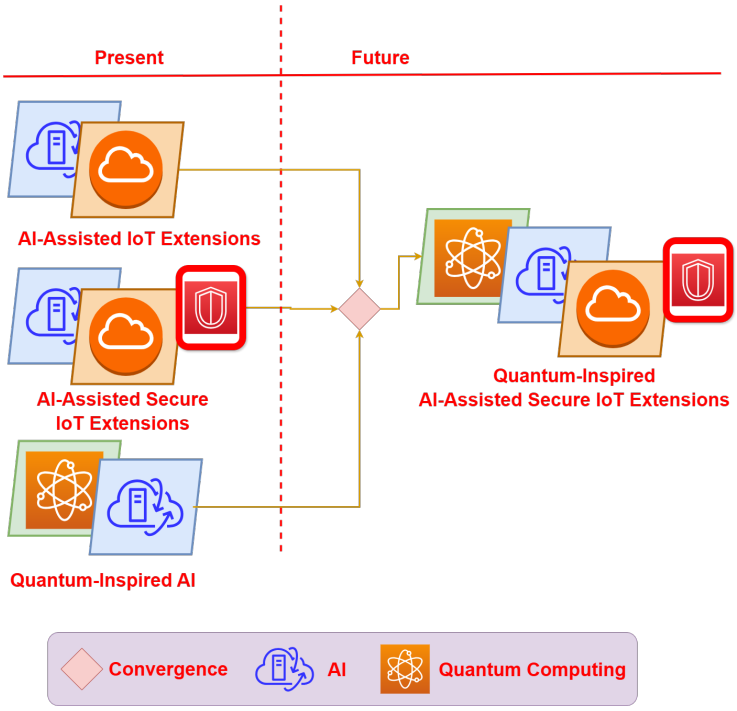


Figure 6. The future of secure IoT extensions.

6. Conclusions and Further Works

The evolution of different computing platforms under the impact of the IoT has led to the emergence of different IoT extensions. These extensions span under the ground, on the ground, in the sea, in the sky, and in space. This proliferation gives rise to a variety

of security challenges and requirements. Although there are some surveys related to IoT extensions, none of them discusses all of the security aspects of all IoT extensions. Moreover, there is no survey focusing on the role of AI in the future of secure IoT extensions. This paper presented a taxonomy on existing IoT extensions, with a focus on security. We studied all security challenges and mechanisms associated with each type of IoT extension. Moreover, we anticipated the future of IoT extensions, given the impact of AI. The work of this paper can be continued by studying other requirements of IoT extensions such as performance, Qos, reliability, scalability, etc.

Author Contributions: All authors have contributed to all activities. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Xu, X.; Shen, B.; Ding, S.; Srivastava, G.; Bilal, M.; Khosravi, M.R.; Menon, V.G.; Jan, M.A.; Wang, M. Service Offloading with Deep Q-Network for Digital Twinning-Empowered Internet of Vehicles in Edge Computing. *IEEE Trans. Ind. Inform.* **2022**, *18*, 1414–1423. [CrossRef]
2. Ibrar, M.; Akbar, A.; Jan, S.R.U.; Jan, M.A.; Wang, L.; Song, H.; Shah, N. ARTNet: Ai-Based Resource Allocation and Task Offloading in a Reconfigurable Internet of Vehicular Networks. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 67–77. [CrossRef]
3. Singh, S.K.; Sharma, P.K.; Pan, Y.; Park, J.H. BIIoVT: Blockchain-based Secure Storage Architecture for Intelligent Internet of Vehicular Things. *IEEE Consum. Electron. Mag. (Early Access Artic.)* **2021**, *11*, 75–82. [CrossRef]
4. Pan, Y.; Fu, M.; Cheng, B.; Tao, X.; Guo, J. Enhanced Deep Learning Assisted Convolutional Neural Network for Heart Disease Prediction on the Internet of Medical Things Platform. *IEEE Access* **2020**, *8*, 189503–189512. [CrossRef]
5. Zhou, Z.; Wang, Z.; Yu, H.; Liao, H.; Mumtaz, S.; Oliveira, L.; Frascolla, V. Learning-Based URLLC-Aware Task Offloading for Internet of Health Things. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 396–410. [CrossRef]
6. Mäkitalo, N.; Flores-Martin, D.; Berrocal, J.; García-Alonso, J.; Ihantola, P.; Ometov, A.; Murillo, J.M.; Mikkonen, T. The Internet of Bodies Needs a Human Data Model. *IEEE Internet Comput.* **2020**, *24*, 28–37. [CrossRef]
7. Zhang, C.; Dong, M.; Ota, K. Deploying SDN Control in Internet of UAVs: Q-Learning-Based Edge Scheduling. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 526–537. [CrossRef]
8. Fang, D.; Guan, X.; Hu, B.; Peng, Y.; Chen, M.; Hwang, K. Deep Reinforcement Learning for Scenario-Based Robust Economic Dispatch Strategy in Internet of Energy. *IEEE Internet Things J.* **2021**, *8*, 9654–9663. [CrossRef]
9. Zhang, Y.; Zhang, H.; Cosmas, J.; Jawad, N.; Ali, K.; Meunier, B.; Kapovits, A.; Huang, L.K.; Li, W.; Shi, L.; et al. Internet of radio and light: 5G building network radio and edge architecture. *Intell. Converg. Netw.* **2020**, *1*, 37–57. [CrossRef]
10. Kontar, R.; Shi, N.; Yue, X.; Chung, S.; Byon, E.; Chowdhury, M.; Jin, J.; Kontar, W.; Masoud, N.; Nouiehed, M.; et al. The Internet of Federated Things (IoFT). *IEEE Access* **2021**, *9*, 156071–156113. [CrossRef]
11. Xu, G.; Song, Z. Performance Analysis of a UAV-Assisted RF/FSO Relaying Systems for Internet of Vehicles. *IEEE Internet Things J.* **2021**, *9*, 5730–5741. [CrossRef]
12. Huang, W.; Song, T.; An, J. QA2: QoS-Guaranteed Access Assistance for Space-Air-Ground Internet of Vehicle Networks. *IEEE Internet Things J.* **2021**, *9*, 5684–5695. [CrossRef]
13. He, X.; Lu, H.; Du, M.; Mao, Y.; Wang, K. QoE-Based Task Offloading With Deep Reinforcement Learning in Edge-Enabled Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst. (Early Access Artic.)* **2021**, *22*, 2252–2261. [CrossRef]
14. Cesarano, L.; Croce, A.; Martins, L.D.C.; Tarchi, D.; Juan, A.A. A Real-Time Energy-Saving Mechanism in Internet of Vehicles Systems. *IEEE Access* **2021**, *9*, 157842–157858. [CrossRef]
15. Ni, Y.; Cai, L.; He, J.; Vinel, A.; Li, Y.; Mosavat-Jahromi, H.; Pan, J. Toward Reliable and Scalable Internet of Vehicles: Performance Analysis and Resource Management. *Proc. IEEE* **2020**, *108*, 324–340. [CrossRef]
16. Javaid, U.; Sikdar, B. A Secure and Scalable Framework for Blockchain Based Edge Computation Offloading in Social Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2021**, *70*, 4022–4036. [CrossRef]
17. Cheng, C.F.; Srivastava, G.; Lin, J.C.W.; Lin, Y.C. Fault-Tolerance Mechanisms for Software-Defined Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 3859–3868. [CrossRef]
18. Draz, U.; Ali, A.; Bilal, M.; Ali, T.; Iftikhar, M.A.; Jolfaei, A.; Suh, D.Y. Energy Efficient Proactive Routing Scheme for Enabling Reliable Communication in Underwater Internet of Things. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 2934–2945. [CrossRef]

19. Gulati, A.; Aujla, G.S.; Chaudhary, R.; Kumar, N.; Obaidat, M.S.; Benslimane, A. DiLSe: Lattice-Based Secure and Dependable Data Dissemination Scheme for Social Internet of Vehicles. *IEEE Trans. Dependable Secur. Comput.* **2021**, *18*, 1–17. [CrossRef]
20. Kong, M.; Lin, J.; Guo, Y.; Sun, X.; Sait, M.; Alkhazragi, O.; Kang, C.H.; Holguin-Lerma, J.A.; Kheireddine, M.; Ouhssain, M.; et al. AquaE-lite Hybrid-Solar-Cell Receiver-Modality for Energy-Autonomous Terrestrial and Underwater Internet-of-Things. *IEEE Photonics J.* **2020**, *12*, 27–41. [CrossRef]
21. Kak, A.; Akyildiz, I.F. Designing Large-Scale Constellations for the Internet of Space Things With CubeSats. *IEEE Internet Things J.* **2021**, *8*, 1749–1768. [CrossRef]
22. Salam, A.; Raza, U. Current Advances in Internet of Underground Things. In *Signals in the Soil*; Salam, A., Raza, U., Eds.; Springer: Berlin/Heidelberg, Germany, 2020; pp. 321–356.
23. Vidyarthi, D.G.A.S.G. Soil Fertility Monitoring With Internet of Underground Things: A Survey. *IEEE Micro* **2022**, *42*, 8–16.
24. Celik, A.; Salama, K.N.; Eltawil, A.M. The Internet of Bodies: A Systematic Survey on Propagation Characterization and Channel Modeling. *IEEE Internet Things J.* **2022**, *9*, 321–345. [CrossRef]
25. Turchet, L.; Fazekas, G.; Lagrange, M.; Ghadikolaei, H.S.; Fischione, C. The Internet of Audio Things: State of the Art, Vision, and Challenges. *IEEE Internet Things J.* **2020**, *7*, 10233–10249. [CrossRef]
26. Yang, G.; Jan, M.A.; Rehman, A.U.; Babar, M.; Aimal, M.M.; Verma, S. Interoperability and Data Storage in Internet of Multimedia Things: Investigating Current Trends, Research Challenges and Future Directions. *IEEE Access* **2020**, *8*, 124382–124401. [CrossRef]
27. Li, T.; Li, C.; Luo, J.; Song, L. Wireless recommendations for Internet of vehicles: Recent advances, challenges, and opportunities. *Intell. Converg. Netw.* **2020**, *1*, 1–17. [CrossRef]
28. Borcoci, E.; Drăgulinescu, A.M.; Li, F.Y.; Vochin, M.C.; Kjellstadli, K. An Overview of 5G Slicing Operational Business Models for Internet of Vehicles, Maritime IoT Applications and Connectivity Solutions. *IEEE Access* **2021**, *9*, 156624–156646. [CrossRef]
29. Storck, C.R.; Duarte-Figueiredo, F. A Survey of 5G Technology Evolution, Standards, and Infrastructure Associated With Vehicle-to-Everything Communications by Internet of Vehicles. *IEEE Access* **2020**, *8*, 117593–117614. [CrossRef]
30. Zhou, H.; Xu, W.; Chen, J.; Wang, W. Evolutionary V2X Technologies Toward the Internet of Vehicles: Challenges and Opportunities. *Proc. IEEE* **2020**, *108*, 308–323. [CrossRef]
31. Ghafoor, K.Z.; Kong, L.; Zeadally, S.; Sadiq, A.S.; Epiphaniou, G.; Hammoudeh, M.; Bashir, A.K.; Mumtaz, S. Millimeter-Wave Communication for Internet of Vehicles: Status, Challenges, and Perspectives. *IEEE Internet Things J.* **2020**, *7*, 8525–8546. [CrossRef]
32. Mollah, M.B.; Zhao, J.; Niyato, D.; Guan, Y.L.; Yuen, C.; Sun, S.; Lam, K.Y.; Koh, L.H. Blockchain for the Internet of Vehicles Towards Intelligent Transportation Systems: A Survey. *IEEE Internet Things J.* **2021**, *8*, 4157–4185. [CrossRef]
33. Qureshi, K.N.; Din, S.; Jeon, G.; Piccialli, F. Internet of Vehicles: Key Technologies, Network Model, Solutions and Challenges With Future Aspects. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 1777–1786. [CrossRef]
34. Qazi, S.; Sabir, F.; Khawaja, B.A.; Atif, S.M.; Mustaqim, M. Why is Internet of Autonomous Vehicles not as Plug and Play as We Think ? Lessons to Be Learnt From Present Internet and Future Directions. *IEEE Access* **2020**, *8*, 133015–133033. [CrossRef]
35. Wei, K.; Zhang, L.; Guo, Y.; Jiang, X. Health Monitoring Based on Internet of Medical Things: Architecture, Enabling Technologies, and Applications. *IEEE Access* **2020**, *8*, 27468–27478. [CrossRef]
36. Qaim, W.B.; Ometov, A.; Molinaro, A.; Lener, I.; Campolo, C.; Lohan, E.S.; Nurmi, J. Towards Energy Efficiency in the Internet of Wearable Things: A Systematic Review. *IEEE Access* **2020**, *8*, 175412–175435. [CrossRef]
37. Pramanik, P.K.D.; Solanki, A.; Debnath, A.; Nayyar, A.; El-Sappagh, S.; Kwak, K.S. Advancing Modern Healthcare With Nanotechnology, Nanobiosensors, and Internet of Nano Things: Taxonomies, Applications, Architecture, and Challenges. *IEEE Access* **2020**, *8*, 65230–65266. [CrossRef]
38. Balghusoon, A.O.; Mahfoudh, S. Routing Protocols for Wireless Nanosensor Networks and Internet of Nano Things: A Comprehensive Survey. *IEEE Access* **2020**, *8*, 200724–200748. [CrossRef]
39. Qiu, T.; Zhao, Z.; Zhang, T.; Chen, C.; Chen, C.L.P. Underwater Internet of Things in Smart Ocean: System Architecture and Open Issues. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4297–4307. [CrossRef]
40. Jahanbakht, M.; Xiang, W.; Hanzo, L.; Azghadi, M.R. Internet of Underwater Things and Big Marine Data Analytics—A Comprehensive Survey. *IEEE Commun. Surv. Tutorials* **2021**, *23*, 904–956. [CrossRef]
41. Aslam, S.; Michaelides, M.P.; Herodotou, H. Internet of Ships: A Survey on Architectures, Emerging Applications, and Challenges. *IEEE Internet Things J.* **2020**, *7*, 9714–9727. [CrossRef]
42. Jonathan Kua and, S.W.L.; Arora, C.; Fernando, N.; Ranaweera, C. Internet of Things in Space: A Review of Opportunities and Challenges from Satellite-Aided Computing to Digitally-Enhanced Space Living. *Sensors* **2021**, *21*, 8117. [CrossRef] [PubMed]
43. Abualigah, L.; Diabat, A.; Sumari, P.; Gandomi, A.H. Applications, Deployments, and Integration of Internet of Drones (IoD): A Review. *IEEE Sensors J.* **2021**, *21*, 25532–25546. [CrossRef]
44. Ning, H.; Shi, F.; Cui, S.; Daneshmand, M. From IoT to Future Cyber-Enabled Internet of X and Its Fundamental Issues. *IEEE Internet Things J.* **2021**, *8*, 6077–6088. [CrossRef]

45. Jia, X.; Xing, L.; Gao, J.; Wu, H. A Survey of Location Privacy Preservation in Social Internet of Vehicles. *IEEE Access* **2020**, *8*, 201966–201984 . [CrossRef]
46. Osorio, D.P.M.; Ahmad, I.; Sánchez, J.D.V.; Gurtov, A.; Scholliers, J.; Kutila, M.; Porambage, P. Towards 6G-Enabled Internet of Vehicles: Security and Privacy. *IEEE Open J. Commun. Soc.* **2022**, *3*, 82–105. [CrossRef]
47. Bagga, P.; Das, A.K.; Wazid, M.; Rodrigues, J.J.P.C.; Park, Y. Authentication Protocols in Internet of Vehicles: Taxonomy, Analysis, and Challenges. *IEEE Access* **2020**, *8*, 54314–54344. [CrossRef]
48. Ghubaish, A.; Salman, T.; Zolanvari, M.; Unal, D.; Al-Ali, A.; Jain, R. Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security. *IEEE Internet Things J.* **2021**, *8*, 8707–8718. [CrossRef]
49. Malamas, V.; Chantzis, F.; Dasaklis, T.K.; Stergiopoulos, G.; Kotzanikolaou, P.; Douligeris, C. Risk Assessment Methodologies for the Internet of Medical Things: A Survey and Comparative Appraisal. *IEEE Access* **2021**, *9*, 40049–40075. [CrossRef]
50. Wazid, M.; Das, A.K.; Shetty, S.; Jo, M. A Tutorial and Future Research for Building a Blockchain-Based Secure Communication Scheme for Internet of Intelligent Things. *IEEE Access* **2020**, *8*, 88700–88716. [CrossRef]
51. Yahuza, M.; Idris, M.Y.I.; Ahmedy, I.B.; Wahab, A.W.A.; Nandy, T.; Noor, N.M.; Bala, A. Internet of Drones Security and Privacy Issues: Taxonomy and Open Challenges. *IEEE Access* **2021**, *9*, 57243–57270. [CrossRef]
52. Zafar, S.; Nazir, M.; Bakhshi, T.; Khattak, H.A.; Khan, S.; Bilal, M.; Choo, K.K.R.; Kwak, K.S.; Sabah, A. A Systematic Review of Bio-Cyber Interface Technologies and Security Issues for Internet of Bio-Nano Things. *IEEE Access* **2021**, *9*, 93529–93566. [CrossRef]
53. Sun, L.; Jiang, X.; Ren, H.; Guo, Y. Edge-Cloud Computing and Artificial Intelligence in Internet of Medical Things: Architecture, Technology and Application. *IEEE Access* **2020**, *8*, 101079–101092. [CrossRef]
54. Xu, X.; Li, H.; Xu, W.; Liu, Z.; Yao, L.; Dai, F. Artificial intelligence for edge service optimization in Internet of Vehicles: A survey. *Tsinghua Sci. Technol.* **2022**, *27*, 270–287. [CrossRef]
55. Misra, S.; Tiwari, M.; Ojha, T.; Raj, Y. PANDA: Preference-Based Bandwidth Allocation in Fog-Enabled Internet of Underground-Mine Things. *IEEE Syst. J.* **2021**, *15*, 5144–5151. [CrossRef]
56. Chen, J.; Sun, S.; bo Zhang, L.; Yang, B.; Wang, W. Compressed Sensing Framework for Heart Sound Acquisition in Internet of Medical Things. *IEEE Trans. Ind. Inform.* **2022**, *18*, 2000–2009. [CrossRef]
57. Hossen, M.N.; Panneerselvam, V.; Koundal, D.; Ahmed, K.; Bui, F.M.; Ibrahim, S.M. Federated Machine Learning for Detection of Skin Diseases and Enhancement of Internet of Medical Things (IoMT) Security. *IEEE J. Biomed. Health Inform.* **2022**, *27*, 835–841. [CrossRef] [PubMed]
58. Qiu, Y.; Zhang, H.; Long, K. Computation Offloading and Wireless Resource Management for Healthcare Monitoring in Fog-Computing-Based Internet of Medical Things. *IEEE Internet Things J.* **2021**, *8*, 15875–15883. [CrossRef]
59. Zhang, T.; Liu, M.; Yuan, T.; Al-Nabhan, N. Emotion-Aware and Intelligent Internet of Medical Things Toward Emotion Recognition During COVID-19 Pandemic. *IEEE Internet Things J.* **2021**, *8*, 16002–16013. [CrossRef]
60. Approach, B.G.M.N. Internet of Medical Things (IoMT) Assisted Vertebral Tumor Prediction Using Heuristic Hock Transformation. *IEEE Access* **2020**, *8*, 17299–17309.
61. Chen, J.; Song, X.; Huang, Z.; Li, J.; Wang, Z.; Luo, C.; Yu, F. On-site Colonoscopy Auto-Diagnosis using Smart Internet of Medical Things. *IEEE Internet Things J.* **2021**, *9*, 8657–8668. [CrossRef]
62. Guo, Z.; Shen, Y.; Wan, S.; Shang, W.; Yu, K. Hybrid Intelligence-Driven Medical Image Recognition for Remote Patient Diagnosis in Internet of Medical Things. *IEEE J. Biomed. Health Inform.* **2021**, *26*, 5817–5828. [CrossRef]
63. Wang, H.; Ding, S.; Yang, S.; Liu, C.; Yu, S.; Zheng, X. Guided activity prediction for minimally invasive surgery safety improvement in the internet of medical things. *IEEE Internet Things J.* **2021**, *9*, 4758–4768. [CrossRef]
64. Egala, B.S.; Pradhan, A.K.; Badarla, V.; Mohanty, S.P. Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control. *IEEE Internet Things J.* **2021**, *8*, 11717–11731. [CrossRef]
65. Wang, S.; Wu, G.; Ning, Z.; Li, J. Blockchain Enabled Privacy Preserving Access Control for Data Publishing and Sharing in the Internet of Medical Things. *IEEE Internet Things J.* **2021**, *9*, 8091–8104.
66. Xie, B.; Xiang, T.; Liao, X.; Wu, J. Achieving Privacy-Preserving Online Diagnosis with Outsourced SVM in Internet of Medical Things Environment. *IEEE Trans. Dependable Secur. Comput.* **2021**, *19*, 4113–4126. [CrossRef]
67. Lu, X.; Cheng, X. A Secure and Lightweight Data Sharing Scheme for Internet of Medical Things. *IEEE Access* **2020**, *8*, 5022–5030. [CrossRef]
68. Yang, L.; Yu, K.; Yang, S.X.; Chakraborty, C.; Lu, Y.; Guo, T. An Intelligent Trust Cloud Management Method for Secure Clustering in 5G enabled Internet of Medical Things. *IEEE Trans. Ind. Inform.* **2021**, *18*, 8864–8875. [CrossRef]
69. Lin, H.; Garg, S.; Hu, J.; Wang, X.; Piran, M.J.; Hossain, M.S. Privacy-Enhanced Data Fusion for COVID-19 Applications in Intelligent Internet of Medical Things. *IEEE Internet Things J.* **2021**, *8*, 15683–15693. [CrossRef]
70. Almogren, A.; Mohiuddin, I.; Din, I.U.; Almajed, H.; Guizani, N. FTM-IoMT: Fuzzy-Based Trust Management for Preventing Sybil Attacks in Internet of Medical Things. *IEEE Internet Things J.* **2021**, *8*, 4485–4497. [CrossRef]
71. Lee, T.F.; Ye, X.; Lin, S.H. Anonymous Dynamic Group Authenticated Key Agreements Using Physical Unclonable Functions for Internet of Medical Things. *IEEE Internet Things J.* **2022**, *9*, 15336–15348. [CrossRef]

72. Manimurugan, S.; Al-Mutairi, S.; Aborokbah, M.M.; Chilamkurti, N.; Ganesan, S.; Patan, R. Effective Attack Detection in Internet of Medical Things Smart Environment Using a Deep Belief Neural Network. *IEEE Access* **2020**, *8*, 77396–77404. [CrossRef]
73. Salem, O.; Alsubhi, K.; Shaafi, A.; Gheryani, M.; Mehaoua, A.; Boutaba, R. Man-in-the-Middle Attack Mitigation in Internet of Medical Things. *IEEE Trans. Ind. Inform.* **2022**, *18*, 2053–2062. [CrossRef]
74. Deebak, B.D.; Al-Turjman, F. Smart Mutual Authentication Protocol for Cloud Based Medical Healthcare Systems Using Internet of Medical Things. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 346–360. [CrossRef]
75. Chiou, S.Y.; Ying, Z.; Liu, J. Improvement of a privacy authentication scheme based on cloud for medical environment. *J. Med. Syst.* **2016**, *40*, 1–15. [CrossRef]
76. Li, J.; Su, Z.; Guo, D.; Choo, K.K.R.; Ji, Y. PSL-MAAKA: Provably Secure and Lightweight Mutual Authentication and Key Agreement Protocol for Fully Public Channels in Internet of Medical Things. *IEEE Internet Things J.* **2021**, *8*, 13183–13195. [CrossRef]
77. Ali, R.; Pal, A.K.; Kumari, S.; Karuppiah, M.; Conti, M. A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring. *Future Gener. Comput. Syst.* **2018**, *84*, 200–215. [CrossRef]
78. Fotouhi, M.; Bayat, M.; Das, A.K.; Far, H.A.N.; Pournaghi, S.M.; Doostari, M.A. A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. *Comput. Netw.* **2020**, *177*, 107333. [CrossRef]
79. Chang, C.C.; Le, H.D. A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks. *IEEE Trans. Wirel. Commun.* **2015**, *15*, 357–366. [CrossRef]
80. Kumari, S.; Li, X.; Wu, F.; Das, A.K.; Arshad, H.; Khan, M.K. A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps. *Future Gener. Comput. Syst.* **2016**, *63*, 56–75. [CrossRef]
81. Sun, J.; Khan, F.; Li, J.; Alshehri, M.D.; Alturki, R.; Wedyan, M. Mutual Authentication Scheme for the Device-to-Server Communication in the Internet of Medical Things. *IEEE Internet Things J.* **2021**, *8*, 15663–15671. [CrossRef]
82. Parah, S.A.; Kaw, J.A.; Bellavista, P.; Loan, N.A.; Bhat, G.M.; Muhammad, K.; de Albuquerque, V.H.C. Efficient Security and Authentication for Edge-Based Internet of Medical Things. *IEEE Internet Things J.* **2021**, *8*, 15652–15662. [CrossRef] [PubMed]
83. Nagarajan, S.M.; Deverajan, G.G.; U, K.; M, T.; Alshehri, M.D.; Alkhalaf, S. Secure Data Transmission in Internet of Medical Things using RES-256 Algorithm. *IEEE Trans. Ind. Inform. (Early Access Artic.)* **2021**, *18*, 8876–8884. [CrossRef]
84. Garg, N.; Wazid, M.; Das, A.K.; Singh, D.P.; Rodrigues, J.J.P.C.; Park, Y. BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment. *IEEE Access* **2020**, *8*, 95956–95977. [CrossRef]
85. Masud, M.; Gaba, G.S.; Alqahtani, S.; Muhammad, G.; Gupta, B.B.; Kumar, P.; Ghoneim, A. A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care. *IEEE Internet Things J.* **2021**, *8*, 15694–15703. [CrossRef]
86. Chen, M.; Lee, T.F. Anonymous Group-Oriented Time-Bound Key Agreement for Internet of Medical Things in Telemonitoring Using Chaotic Maps. *IEEE Internet Things J.* **2021**, *8*, 13939–13949. [CrossRef]
87. Zeng, P.; Zhang, Z.; Lu, R.; Choo, K.K.R. Efficient Policy-Hiding and Large Universe Attribute-Based Encryption With Public Traceability for Internet of Medical Things. *IEEE Internet Things J.* **2021**, *8*, 10963–10972. [CrossRef]
88. Hasan, M.K.; Islam, S.; Sulaiman, R.; Khan, S.; Hashim, A.H.A.; Habib, S.; Islam, M.; Alyahya, S.; Ahmed, M.M.; Kamil, S.; et al. Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications. *IEEE Access* **2021**, *9*, 47731–7742. [CrossRef]
89. Kumar, M.; Chand, S. A Secure and Efficient Cloud-Centric Internet-of-Medical-Things-Enabled Smart Healthcare System With Public Verifiability. *IEEE Internet Things J.* **2020**, *7*, 10650–10659. [CrossRef]
90. Thamilarasu, G.; Odesile, A.; Hoang, A. An Intrusion Detection System for Internet of Medical Things. *IEEE Access* **2020**, *8*, 181560–181576. [CrossRef]
91. Nguyen, T.A.; Min, D.; Choi, E.; Lee, J.W. Dependability and Security Quantification of an Internet of Medical Things Infrastructure Based on Cloud-Fog-Edge Continuum for Healthcare Monitoring Using Hierarchical Models. *IEEE Internet Things J.* **2021**, *8*, 15704–15748. [CrossRef]
92. Santagati, G.E.; Dave, N.; Melodia, T. Design and Performance Evaluation of an Implantable Ultrasonic Networking Platform for the Internet of Medical Things. *IEEE/ACM Trans. Netw.* **2020**, *28*, 29–42. [CrossRef]
93. Coelho, K.K.; Nogueira, M.; Marim, M.C.; Silva, E.F.; Vieira, A.B.; Nacif, J.A.M. LORENA: Low memORy symmEtric-Key geNerAtion Method for Based on Group Cryptography Protocol Applied to the Internet of Healthcare Things. *IEEE Access* **2022**, *10*, 12564–12579. [CrossRef]
94. Munir, N.; Khan, M.; Hazzazi, M.M.; Aljaedi, A.; Ismail, A.A.K.H.; Alharbi, A.R.; Hussain, I. Cryptanalysis of Internet of Health Things Encryption Scheme Based on Chaotic Maps. *IEEE Access* **2021**, *9*, 105678–105685. [CrossRef]
95. Tsafack, N.; Sankar, S.; Abd-El-Atty, B.; Kengne, J.; C., J.K.; Belazi, A.; Mehmood, I.; Bashir, A.K.; Song, O.Y.; El-Latif, A.A.A. A New Chaotic Map With Dynamic Analysis and Encryption Application in Internet of Health Things. *IEEE Access* **2020**, *8*, 137731–137744. [CrossRef]
96. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]

97. Aboushosha, B.; Ramadan, R.A.; Dwivedi, A.D.; El-Sayed, A.; Dessouky, M.M. SLIM: A Lightweight Block Cipher for Internet of Health Things. *IEEE Access* **2020**, *8*, 203747–203757. [CrossRef]
98. Li, H.; Yu, K.; Liu, B.; Feng, C.; Qin, Z.; Srivastava, G. An Efficient Ciphertext-Policy Weighted Attribute-Based Encryption for the Internet of Health Things. *IEEE J. Biomed. Health Inform.* **2021**, *26*, 1949–1960. [CrossRef] [PubMed]
99. Lin, H.Y.; Tzeng, W.G. An efficient solution to the millionaires' problem based on homomorphic encryption. In Proceedings of the International Conference on Applied Cryptography and Network Security, New York, NY, USA, 7–10 June 2005; Springer: Berlin/Heidelberg, Germany, 2005, pp. 456–466.
100. Ullah, I.; Alkhalifah, A.; Rehman, S.U.; Kumar, N.; Khan, M.A. An Anonymous Certificateless Signcryption Scheme for Internet of Health Things. *IEEE Access* **2021**, *9*, 101207–101216. [CrossRef]
101. Rahman, M.A.; Hossain, M.S.; Islam, M.S.; Alrajeh, N.A.; Muhammad, G. Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach. *IEEE Access* **2020**, *8*, 205071–205087. [CrossRef]
102. Silva, F.A.; Nguyen, T.A.; Fé, I.; Brito, C.; Min, D.; Lee, J.W. Performance Evaluation of an Internet of Healthcare Things for Medical Monitoring Using M/M/c/K Queuing Models. *IEEE Access* **2021**, *9*, 55271–55283. [CrossRef]
103. Qin, L.; Xie, Y. Real-Time Monitoring System of Exercise Status Based on Internet of Health Things Using Safety Architecture Model. *IEEE Access* **2021**, *9*, 27333–27345. [CrossRef]
104. Abbasi, U.F.; Haider, N.; Awang, A.; Khan, K.S. Cross-Layer MAC/Routing Protocol for Reliable Communication in Internet of Health Things. *IEEE Open J. Commun. Soc.* **2021**, *2*, 199–216. [CrossRef]
105. Celik, A.; Eltawil, A.M. Enabling the Internet of Bodies Through Capacitive Body Channel Access Schemes. *IEEE Internet Things J.* **2021**, *9*, 15901–15914. [CrossRef]
106. Agarwal, K.; Abeena, R.L.U.; Polachan, K. VLC-LE: Energy-Efficient and Secure Visible Light Communication for the Internet of Bodies. In Proceedings of the International Conference on Smart Applications, Communications and Networking (SmartNets), Harrisonburg, VA, USA, 29 April–2 May 2024.
107. Celik, A.; Eltawil, A.M. The Internet of Bodies: The Human Body as an Efficient and Secure Wireless Channel. *IEEE Internet Things Mag.* **2022**, *4*, 114–120. [CrossRef]
108. Ali, M.; Chen, Y.; Cree, M.J. Autonomous In vivo Computation in Internet-of-Nano-Bio-Things. *IEEE Internet Things J.* **2021**, *9*, 6134–6147. [CrossRef]
109. Dissanayake, M.B.; Ekanayake, N. On the Exact Performance Analysis of Molecular Communication via Diffusion for Internet of Bio-Nano Things. *IEEE Trans. Nanobiosci.* **2021**, *20*, 291–295. [CrossRef]
110. Akyildiz, I.F.; Ghovanloo, M.; Guler, U.; Ozkaya-Ahmadov, T.; Sarioglu, A.F.; Unluturk, B.D. PANACEA: An Internet of Bio-NanoThings Application for Early Detection and Mitigation of Infectious Diseases. *IEEE Access* **2020**, *8*, 140512–140523. [CrossRef]
111. Wan, L.; Sun, L.; Liu, K.; Wang, X.; Lin, Q.; Zhu, T. Autonomous Vehicle Source Enumeration Exploiting Non-Cooperative UAV in Software Defined Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 3603–3615. [CrossRef]
112. Jabbar, R.; Fetais, N.; Kharbeche, M.; Krichen, M.; Barkaoui, K.; Shinoy, M. Blockchain for the Internet of Vehicles: How to Use Blockchain to Secure Vehicle-to-Everything (V2X) Communication and Payment*. *IEEE Sensors J.* **2021**, *21*, 15807–15823. [CrossRef]
113. Benarous, L.; Bitam, S.; Mellouk, A. CSLPPS: Concerted Silence-Based Location Privacy Preserving Scheme for Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2021**, *70*, 7153–7160. [CrossRef]
114. Xing, L.; Jia, X.; Gao, J.; Wu, H. A Location Privacy Protection Algorithm Based on Double K-Anonymity in the Social Internet of Vehicles. *IEEE Commun. Lett.* **2021**, *25*, 3199–3203. [CrossRef]
115. Li, X.; Ren, Y.; Yang, L.T.; Zhang, N.; Luo, B.; Weng, J.; Liu, X. Perturbation-Hidden: Enhancement of Vehicular Privacy for Location-Based Services in Internet of Vehicles. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 2073–2086. [CrossRef]
116. Ghimire, B.; Rawat, D.B. Secure, Privacy Preserving and Verifiable Federating Learning using Blockchain for Internet of Vehicles. *IEEE Consum. Electron. Mag.* **2021**, *11*, 67–74. [CrossRef]
117. Kumar, R.; Kumar, P.; Tripathi, R.; Gupta, G.P.; Kumar, N. P2SF-IoV: A Privacy-Preservation-Based Secured Framework for Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 22571–22582. [CrossRef]
118. Chai, H.; Leng, S.; He, J.; Zhang, K.; Cheng, B. CyberChain: Cybertwin Empowered Blockchain for Lightweight and Privacy-preserving Authentication in Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2021**, *71*, 4620–4631. [CrossRef]
119. Xu, X.; Huang, Q.; Zhu, H.; Sharma, S.; Zhang, X.; Qi, L.; Bhuiyan, M.Z.A. Secure Service Offloading for Internet of Vehicles in SDN-Enabled Mobile Edge Computing. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 3720–3729. [CrossRef]
120. Yang, J.; Liu, J.; Han, R.; Wu, J. Generating and Restoring Private Face Images for Internet of Vehicles Based on Semantic Features and Adversarial Examples. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 16799–16809. [CrossRef]
121. Sutrala, A.K.; Bagga, P.; Das, A.K.; Kumar, N.; Rodrigues, J.J.P.C.; Lorenz, P. On the Design of Conditional Privacy Preserving Batch Verification-Based Authentication Scheme for Internet of Vehicles Deployment. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5535–5548. [CrossRef]

122. Zavvos, E.; Gerding, E.H.; Yazdanpanah, V.; Maple, C.; Stein, S.; m.c. schraefel. Privacy and Trust in the Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 10126–10141. [CrossRef]
123. Ahmad, F.; Kurugollu, F.; Kerrache, C.A.; Sezer, S.; Liu, L. NOTRINO: A NOvel Hybrid TRust Management Scheme for INternet-of-Vehicles. *IEEE Trans. Veh. Technol.* **2021**, *70*, 9244–9257. [CrossRef]
124. Zhang, H.; Liu, J.; Zhao, H.; Wang, P.; Kato, N. Blockchain-Based Trust Management for Internet of Vehicles. *IEEE Trans. Emerg. Top. Comput.* **2021**, *9*, 1397–1409. [CrossRef]
125. Xu, X.; Wu, Q.; Qi, L.; Dou, W.; Tsai, S.B.; Bhuiyan, M.Z.A. Trust-Aware Service Offloading for Video Surveillance in Edge Computing Enabled Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 1787–1796. [CrossRef]
126. Singh, P.K.; Singh, R.; Nandi, S.K.; Ghafoor, K.Z.; Rawat, D.B.; Nandi, S. Blockchain-Based Adaptive Trust Management in Internet of Vehicles Using Smart Contract. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 3616–3630. [CrossRef]
127. Javaid, U.; Aman, M.N.; Sikdar, B. A Scalable Protocol for Driving Trust Management in Internet of Vehicles With Blockchain. *IEEE Internet Things J.* **2020**, *7*, 11815–11829. [CrossRef]
128. Zhang, Q.; Wu, J.; Zanella, M.; Yang, W.; Bashir, A.K.; Fornaciari, W. Sema-IIoVT: Emergent Semantic-Based Trustworthy Information-Centric Fog System and Testbed for Intelligent Internet of Vehicles. *IEEE Consum. Electron. Mag.* **2021**, *12*, 70–79. [CrossRef]
129. Muhammad, G.; Alhussein, M. Security, Trust, and Privacy for the Internet of Vehicles: A Deep Learning Approach. *IEEE Consum. Electron. Mag.* **2021**, *11*, 49–55. [CrossRef]
130. Wang, Q.; Chen, X.; Jin, X.; Li, X.; Chen, D.; Qin, X. Enhancing Trustworthiness of Internet of Vehicles in Space-Air-Ground Integrated Networks: Attestation Approach. *IEEE Internet Things J.* **2021**, *9*, 5992–6002. [CrossRef]
131. Yang, Z.; Wang, R.; Wu, D.; Yang, B.; Zhang, P. Blockchain-enabled Trust Management Model for the Internet of Vehicles. *IEEE Internet Things J.* **2021**, *10*, 12044–12054. [CrossRef]
132. Li, J.; Xue, Z.; Li, C.; Liu, M. RTED-SD: A Real-Time Edge Detection Scheme for Sybil DDoS in the Internet of Vehicles. *IEEE Access* **2021**, *9*, 11296–11305. [CrossRef]
133. Zhongtang, Z.X.H. Two-phase placement algorithm with energy efficiency optimization for virtual machins bsed on data center. *J. Comput. Appl.* **2014**, *34*, 3222.
134. Buller, A.T.; McManus, J. The quartile-deviation/median-diameter relationships of glacial deposits. *Sediment. Geol.* **1973**, *10*, 135–146. [CrossRef]
135. Srinu, S.; Mishra, A.K.; Farooq, S. Improved GESD test for cooperative sensing over impaired cognitive radio networks. In Proceedings of the 2014 annual IEEE India conference (INDICON), Pune, India, 11–13 December 2014; pp. 1–5.
136. Kamal, M.; Srivastava, G.; Tariq, M. Blockchain-Based Lightweight and Secured V2V Communication in the Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 3997–4004. [CrossRef]
137. Makarfi, A.U.; Rabie, K.M.; Kaiwartya, O.; Adhikari, K.; Nauryzbayev, G.; Li, X.; Kharel, R. Toward Physical-Layer Security for Internet of Vehicles: Interference-Aware Modeling. *IEEE Internet Things J.* **2021**, *8*, 443–457. [CrossRef]
138. Garg, S.; Singh, A.; Aujla, G.S.; Kaur, S.; Batra, S.; Kumar, N. A Probabilistic Data Structures-Based Anomaly Detection Scheme for Software-Defined Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 3557–3566. [CrossRef]
139. Li, X.; Zhang, H.; Miao, Y.; Ma, S.; Ma, J.; Liu, X.; Choo, K.K.R. CAN Bus Messages Abnormal Detection Using Improved SVDD in Internet of Vehicle. *IEEE Internet Things J. (Early Access Artic.)* **2021**, *9*, 3359–3371. [CrossRef]
140. Ullah, I.; Khan, M.A.; Khan, F.; Jan, M.A.; Srinivasan, R.; Mastorakis, S.; Hussain, S.; Khattak, H. An Efficient and Secure Multimessage and Multireceiver Signcryption Scheme for Edge-Enabled Internet of Vehicles. *IEEE Internet Things J.* **2022**, *9*, 2688–2697. [CrossRef]
141. Song, L.; Sun, G.; Yu, H.; Du, X.; Guizani, M. FBIA: A Fog-Based Identity Authentication Scheme for Privacy Preservation in Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5403–5415. [CrossRef]
142. Bagga, P.; Das, A.K.; Wazid, M.; Rodrigues, J.J.P.C.; Choo, K.K.R.; Park, Y. On the Design of Mutual Authentication and Key Agreement Protocol in Internet of Vehicles-Enabled Intelligent Transportation System. *IEEE Trans. Veh. Technol.* **2021**, *70*, 1736–1751. [CrossRef]
143. Adil, M.; Ali, J.; Attique, M.; Jadoon, M.M.; Abbas, S.; Alotaibi, S.R.; Menon, V.G.; Farouk, A. Three Byte-Based Mutual Authentication Scheme for Autonomous Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 9358–9369. [CrossRef]
144. Vasudev, H.; Deshpande, V.; Das, D.; Das, S.K. A Lightweight Mutual Authentication Protocol for V2V Communication in Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2020**, *69*, 6709–6717. [CrossRef]
145. Gupta, D.S.; Karati, A.; Saad, W.; Costa, D.B.D. Quantum-Defended Blockchain-Assisted Data Authentication Protocol for Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2022**, *71*, 3255–3266. [CrossRef]
146. Li, J.; Li, Y.; Cao, C.; Lam, K.Y. Conditional Anonymous Authentication with Abuse-Resistant Tracing and Distributed Trust for Internet of Vehicles. *IEEE Internet Things J.* **2021**, *9*, 8749–8762. [CrossRef]
147. Kong, X.; Zhu, B.; Shen, G.; Workneh, T.C.; Ji, Z.; Chen, Y.; Liu, Z. Spatial-Temporal-Cost Combination Based Taxi Driving Fraud Detection for Collaborative Internet of Vehicles. *IEEE Trans. Ind. Inform.* **2022**, *18*, 3426–3436. [CrossRef]

148. Mershad, K. SURFER: A Secure SDN-Based Routing Protocol for Internet of Vehicles. *IEEE Internet Things J.* **2021**, *8*, 7407–7422. [CrossRef]
149. Mershad, K.; Artail, H.; Gerla, M. ROAMER: Roadside Units as message routers in VANETs. *Ad Hoc Netw.* **2012**, *10*, 479–496. [CrossRef]
150. Chattaraj, D.; Bera, B.; Das, A.K.; Saha, S.; Lorenz, P.; Park, Y. Block-CLAP: Blockchain-Assisted Certificateless Key Agreement Protocol for Internet of Vehicles in Smart Transportation. *IEEE Trans. Veh. Technol.* **2021**, *70*, 8092–8107. [CrossRef]
151. Castro, M.; Liskov, B. Practical Byzantine fault tolerance and proactive recovery. *ACM Trans. Comput. Syst. (TOCS)* **2002**, *20*, 398–461. [CrossRef]
152. Safavat, S.; Rawat, D.B. On the Elliptic Curve Cryptography for Privacy-Aware Secure ACO-AODV Routing in Intent-Based Internet of Vehicles for Smart Cities. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 5050–5059. [CrossRef]
153. Karim, H.; Rawat, D.B. TollsOnly Please—Homomorphic Encryption for Toll Transponder Privacy in Internet of Vehicles. *IEEE Internet Things J.* **2022**, *9*, 2627–2636. [CrossRef]
154. Wang, X.; Zhu, Y.; Han, S.; Yang, L.; Gu, H.; Wang, F.Y. Fast and Progressive Misbehavior Detection in Internet of Vehicles based on Broad Learning and Incremental Learning Systems. *IEEE Internet Things J.* **2021**, *9*, 4788–4798. [CrossRef]
155. Abhishek, N.V.; Aman, M.N.; Lim, T.J.; Sikdar, B. DRiVe: Detecting Malicious Roadside Units in the Internet of Vehicles with Low Latency Data Integrity. *IEEE Internet Things J.* **2021**, *9*, 3270–3281. [CrossRef]
156. Yang, L.; Moubayed, A.; Shami, A. MTH-IDS: A Multitiered Hybrid Intrusion Detection System for Internet of Vehicles. *IEEE Internet Things J.* **2022**, *9*, 616–632. [CrossRef]
157. Ahmed, I.; Ahmad, A.; Jeon, G. Deep Learning-based Intrusion Detection System for Internet of Vehicles. *IEEE Consum. Electron. Mag.* **2021**, *12*, 117–123. [CrossRef]
158. Iranmanesh, S.; Abkenar, F.S.; Jamalipour, A.; Raad, R. A Heuristic Distributed Scheme to Detect Falsification of Mobility Patterns in Internet of Vehicles. *IEEE Internet Things J.* **2022**, *9*, 719–727. [CrossRef]
159. Halabi, T.; Wahab, O.A.; Mallah, R.A.; Zulkernine, M. Protecting the Internet of Vehicles Against Advanced Persistent Threats: A Bayesian Stackelberg Game. *IEEE Trans. Reliab.* **2021**, *70*, 970–985. [CrossRef]
160. Jiang, X.; Yu, F.R.; Song, T.; Leung, V.C. Intelligent Resource Allocation for Video Analytics in Blockchain-Enabled Internet of Autonomous Vehicles with Edge Computing. *IEEE Internet Things J.* **2020**, *9*, 14260–14272. [CrossRef]
161. Cao, B.; Chen, X.; Lv, Z.; Li, R.; Fan, S. Optimization of Classified Municipal Waste Collection Based on the Internet of Connected Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 5364–5373. [CrossRef]
162. Ghane, S.; Jolfaei, A.; Kulik, L.; Ramamohanarao, K.; Puthal, D. Preserving Privacy in the Internet of Connected Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 5018–5027. [CrossRef]
163. Wei, F.; Zeadally, S.; Vijayakumar, P.; Kumar, N.; He, D. An Intelligent Terminal Based Privacy-Preserving Multi-Modal Implicit Authentication Protocol for Internet of Connected Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 3939–3951. [CrossRef]
164. Tian, Z.; Gao, X.; Su, S.; Qiu, J. Vcash: A Novel Reputation Framework for Identifying Denial of Traffic Service in Internet of Connected Vehicles. *IEEE Internet Things J.* **2020**, *7*, 3901–3909. [CrossRef]
165. Liu, Q.; Kamoto, K.M.; Liu, X.; Zhang, Y.; Yang, Z.; Khosravi, M.R.; Xu, Y.; Qi, L. A Sensory Similarities Approach to Load Disaggregation of Charging Stations in Internet of Electric Vehicles. *IEEE Sensors J.* **2021**, *21*, 15895–15903. [CrossRef]
166. Luo, L.; Feng, J.; Yu, H.; Sun, G. Blockchain-Enabled Two-way Auction Mechanism for Electricity Trading in Internet of Electric Vehicles. *IEEE Internet Things J.* **2021**, *9*, 8105–8118. [CrossRef]
167. Abishu, H.N.; Seid, A.M.; Yacob, Y.H.; Ayall, T.; Sun, G.; Liu, G. Consensus Mechanism for Blockchain-Enabled Vehicle-to-Vehicle Energy Trading in the Internet of Electric Vehicles. *IEEE Trans. Veh. Technol.* **2022**, *71*, 946–960. [CrossRef]
168. Gao, Z.; Xu, C.; Zhang, H.; Li, S.; de Albuquerque, V.H.C. Trustful Internet of Surveillance Things Based on Deeply Represented Visual Co-Saliency Detection. *IEEE Internet Things J.* **2020**, *7*, 4092–4100. [CrossRef]
169. Fu, H.; Cao, X.; Tu, Z. Cluster-based co-saliency detection. *IEEE Trans. Image Process.* **2013**, *22*, 3766–3778. [CrossRef]
170. Liu, Z.; Zou, W.; Li, L.; Shen, L.; Le Meur, O. Co-saliency detection based on hierarchical segmentation. *IEEE Signal Process. Lett.* **2013**, *21*, 88–92. [CrossRef]
171. Zhang, D.; Han, J.; Li, C.; Wang, J.; Li, X. Detection of co-salient objects by looking deep and wide. *Int. J. Comput. Vis.* **2016**, *120*, 215–232. [CrossRef]
172. Zhang, J.; Liu, P.; Zhang, F.; Iwabuchi, H.; de H. e Ayres de Moura, A.A.; de Albuquerque, V.H.C. Ensemble Meteorological Cloud Classification Meets Internet of Dependable and Controllable Things. *IEEE Internet Things J.* **2021**, *18*, 3323–3330. [CrossRef]
173. Gaikwad, N.B.; Ugale, H.; Keskar, A.; Shivaprakash, N.C. The Internet-of-Battlefield-Things (IoBT)-Based Enemy Localization Using Soldiers Location and Gunshot Direction. *IEEE Internet Things J.* **2020**, *7*, 11725–11734. [CrossRef]
174. Lin, D.; Wu, W. Heuristic Algorithm for Resource Allocation in an Internet of Battle Things. *IEEE Syst. J. (Early Access Artic.)* **2022**, *17*, 200–211. [CrossRef]
175. Yu, C.; Shen, S.; Yang, H.; Zhang, K.; Zhao, H. Leveraging Energy, Latency and Robustness for Routing Path Selection in Internet of Battlefield Things. *IEEE Internet Things J.* **2021**, *9*, 12601–12613. [CrossRef]

176. Ramzan, R.; Omar, M.; Siddiqui, O.F.; Ksiksi, T.S.; Bastaki, N. Internet of Trees (IoTr) Implemented by Highly Dispersive Electromagnetic Sensors. *IEEE Sensors J.* **2021**, *21*, 642–650. [CrossRef]
177. Udutalapally, V.; Mohanty, S.P.; Pallagani, V.; Khandelwal, V. sCrop: A Novel Device for Sustainable Automatic Disease Prediction, Crop Selection, and Irrigation in Internet-of-Agro-Things for Smart Agriculture. *IEEE Sensors J.* **2021**, *21*, 17525–17538. [CrossRef]
178. Éden Battisti, A.L.; Muchaluat-Saade, D.C.; Delicato, F.C. Enabling Internet of Media Things with Edge-Based Virtual Multimedia Sensors. *IEEE Access* **2021**, *9*, 59255–59269. [CrossRef]
179. Chen, C.W. Internet of Video Things: Next-Generation IoT with Visual Sensors. *IEEE Internet Things J.* **2020**, *7*, 6676–6685. [CrossRef]
180. Zhang, X.; Wei, X.; Zhou, L.; Qian, Y. Social-Content-Aware Scalable Video Streaming in Internet of Video Things. *IEEE Internet Things J.* **2022**, *9*, 830–843. [CrossRef]
181. Curry, E.; Salwala, D.; Dhingra, P.; Pontes, F.A.; Yadav, P. Multimodal Event Processing: A Neural-Symbolic Paradigm for the Internet of Multimedia Things. *IEEE Internet Things J.* **2022**, *9*, 13705–13724. [CrossRef]
182. Wang, M.; Xiao, D.; Xiang, Y. Low-Cost and Confidentiality-Preserving Multi-Image Compressed Acquisition and Separate Reconstruction for Internet of Multimedia Things. *IEEE Internet Things J.* **2021**, *8*, 1662–1673. [CrossRef]
183. Usman, M.; Jan, M.A.; Puthal, D. PAAL: A Framework Based on Authentication, Aggregation, and Local Differential Privacy for Internet of Multimedia Things. *IEEE Internet Things J.* **2020**, *7*, 2501–2508. [CrossRef]
184. Mumin, D.; Shi, L.L.; Liu, L.; Panneerselvam, J. Data-Driven Diffusion Recommendation in Online Social Networks for the Internet of People. *IEEE Trans. Syst. Man, Cybern. Syst.* **2022**, *52*, 166–178. [CrossRef]
185. Dhelim, S.; Ning, H.; Aung, N. ComPath: User Interest Mining in Heterogeneous Signed Social Networks for Internet of People. *IEEE Internet Things J.* **2021**, *8*, 7024–7035. [CrossRef]
186. Zhang, C.; Wu, X.; Yan, W.; Wang, L.; Zhang, L. Attribute-Aware Graph Recurrent Networks for Scholarly Friend Recommendation Based on Internet of Scholars in Scholarly Big Data. *IEEE Trans. Ind. Inform.* **2020**, *16*, 2707–2715. [CrossRef]
187. Yue, J.; Xiao, M. Coding for Distributed Fog Computing in Internet of Mobile Things. *IEEE Trans. Mob. Comput.* **2021**, *20*, 1337–1350. [CrossRef]
188. Eom, S.; Zhou, H.; Kaur, U.; Voyles, R.; Kusuma, D. TupperwareEarth: Bringing Intelligent User Assistance to the "Internet of Kitchen Things". *IEEE Internet Things J.* **2021**, *9*, 13233–13249. [CrossRef]
189. Liu, Y.; Guan, X.; Peng, Y.; Chen, H.; Ohtsuki, T.; Han, Z. Blockchain-Based Task Offloading for Edge Computing on Low-Quality Data via Distributed Learning in the Internet of Energy. *IEEE J. Sel. Areas Commun.* **2022**, *40*, 657–676. [CrossRef]
190. Sayed, A.; Himeur, Y.; Alsalemi, A.; Bensaali, F.; Amira, A. Intelligent Edge-Based Recommender System for Internet of Energy Applications. *IEEE Syst. J.* **2021**, *16*, 5001–5010. [CrossRef]
191. Zhang, Z.; Guan, C.; Chen, H.; Yang, X.; Gong, W.; Yang, A. Adaptive Privacy Preserving Federated Learning for Fault Diagnosis in Internet of Ships. *IEEE Internet Things J.* **2021**, *9*, 6844–6854. [CrossRef]
192. Wang, Q.; Dai, H.N.; Wang, Q.; Shukla, M.K.; Zhang, W.; Soares, C.G. On Connectivity of UAV-Assisted Data Acquisition for Underwater Internet of Things. *IEEE Internet Things J.* **2020**, *7*, 5371–5385. [CrossRef]
193. Lin, C.; Han, G.; Du, J.; Bi, Y.; Shu, L.; Fan, K. A Path Planning Scheme for AUV Flock-Based Internet-of-Underwater-Things Systems to Enable Transparent and Smart Ocean. *IEEE Internet Things J.* **2020**, *7*, 9760–9772. [CrossRef]
194. Yan, J.; Meng, Y.; Luo, X.; Guan, X. To Hide Private Position Information in Localization for Internet of Underwater Things. *IEEE Internet Things J.* **2021**, *8*, 14338–14354. [CrossRef]
195. Wei, D.; Huang, C.; Li, X.; Lin, B.; Shu, M.; Wang, J.; Pan, M. Power Efficient Data Collection Scheme for AUV Assisted Magnetic Induction and Acoustic Hybrid Internet of Underwater Things. *IEEE Internet Things J.* **2021**, *9*, 11675–11684. [CrossRef]
196. Khosravi, M.R.; Samadi, S. Reliable Data Aggregation in Internet of ViSAR Vehicles Using Chained Dual-Phase Adaptive Interpolation and Data Embedding. *IEEE Internet Things J.* **2020**, *7*, 2603–2610. [CrossRef]
197. Cheng, C.; Guo, L.; Wu, T.; Sun, J.; Gui, G.; Adebisi, B.; Gacanin, H.; Sari, H. Machine Learning-Aided Trajectory Prediction and Conflict Detection for Internet of Aerial Vehicles. *IEEE Internet Things J. (Early Access Artic.)* **2021**, *9*, 5882–5894. [CrossRef]
198. Mukherjee, A.; De, D.; Dey, N. Dewdrone: Dew computing for Internet of Drone Things. *IEEE Consum. Electron. Mag. (Early Access Artic.)* **2021**, *12*, 52–57. [CrossRef]
199. Gope, P.; Sikdar, B. An Efficient Privacy-Preserving Authenticated Key Agreement Scheme for Edge-Assisted Internet of Drones. *IEEE Trans. Veh. Technol.* **2020**, *69*, 13621–13630. [CrossRef]
200. Bera, B.; Saha, S.; Das, A.K.; Kumar, N.; Lorenz, P.; Alazab, M. Blockchain-Envisioned Secure Data Delivery and Collection Scheme for 5G-Based IoT-Enabled Internet of Drones Environment. *IEEE Trans. Veh. Technol.* **2020**, *69*, 9097–9111. [CrossRef]
201. Hussain, S.; Chaudhry, S.A.; Alomari, O.A.; Alsharif, M.H.; Khan, M.K.; Kumar, N. Amassing the Security: An ECC-Based Authentication Scheme for Internet of Drones. *IEEE Syst. J.* **2021**, *15*, 4431–4438. [CrossRef]
202. Feng, C.; Liu, B.; Guo, Z.; Yu, K.; Qin, Z.; Choo, K.K.R. Blockchain-based Cross-domain Authentication for Intelligent 5G-enabled Internet of Drones. *IEEE Internet Things J.* **2021**, *9*, 6224–6238. [CrossRef]

203. Tanveer, M.; Khan, A.U.; Kumar, N.; Hassan, M.M. RAMP-IoD: A Robust Authenticated Key Management Protocol for the Internet of Drones. *IEEE Internet Things J.* **2022**, *9*, 1339–1353. [CrossRef]
204. Jeong, J.Y.; Byun, J.W.; Jeong, I.R. Key Agreement Between User and Drone with Forward Unlinkability in Internet of Drones. *IEEE Access* **2022**, *10*, 17134–17144. [CrossRef]
205. Pu, C.; Carpenter, L. Psched: A Priority-Based Service Scheduling Scheme for the Internet of Drones. *IEEE Syst. J.* **2021**, *15*, 4230–4239. [CrossRef]
206. Saeed, N.; Alouini, M.S.; Al-Naffouri, T.Y. Accurate 3-D Localization of Selected Smart Objects in Optical Internet of Underwater Things. *IEEE Internet Things J.* **2020**, *7*, 937–947. [CrossRef]
207. Niu, W.; Xiao, J.; Zhang, X.; Zhang, X.; Du, X.; Huang, X.; Guizani, M. Malware on Internet of UAVs Detection Combining String Matching and Fourier Transformation. *IEEE Internet Things J.* **2021**, *8*, 9905–9919. [CrossRef]
208. Zhou, D.; Sheng, M.; Wu, J.; Li, J.; Han, Z. Gateway Placement in Integrated Satellite-Terrestrial Networks: Supporting Communications and Internet of Remote Things. *IEEE Internet Things J.* **2021**, *9*, 4421–4434. [CrossRef]
209. Kak, A.; Akyildiz, I.F. Towards Automatic Network Slicing for the Internet of Space Things. *IEEE Trans. Netw. Serv. Manag.* **2021**, *19*, 392–412. [CrossRef]
210. Han, C.; Huo, L.; Tong, X.; Wang, H.; Liu, X. Spatial Anti-Jamming Scheme for Internet of Satellites Based on the Deep Reinforcement Learning and Stackelberg Game. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5331–5342. [CrossRef]
211. Lim, W.Y.B.; Huang, J.; Xiong, Z.; Kang, J.; Niyato, D.; Hua, X.S.; Leung, C.; Miao, C. Towards Federated Learning in UAV-Enabled Internet of Vehicles: A Multi-Dimensional Contract-Matching Approach. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 5140–5154. [CrossRef]
212. Ning, Z.; Zhang, K.; Wang, X.; Obaidat, M.S.; Guo, L.; Hu, X.; Hu, B.; Guo, Y.; Sadoun, B.; Kwok, R.Y.K. Joint Computing and Caching in 5G-Envisioned Internet of Vehicles: A Deep Reinforcement Learning-Based Traffic Control System. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 5201–5212. [CrossRef]
213. Song, Y.; Fu, Y.; Yu, F.R.; Zhou, L. Blockchain-Enabled Internet of Vehicles with Cooperative Positioning: A Deep Neural Network Approach. *IEEE Internet Things J.* **2020**, *7*, 3485–3498. [CrossRef]
214. Kong, X.; Wang, K.; Hou, M.; Hao, X.; Shen, G.; Chen, X.; Xia, F. A Federated Learning-Based License Plate Recognition Scheme for 5G-Enabled Internet of Vehicles. *IEEE Trans. Ind. Inform.* **2021**, *17*, 8523–8530. [CrossRef]
215. Kumbhar, F.H.; Shin, S.Y. Novel Vehicular Compatibility-Based Ad Hoc Message Routing Scheme in the Internet of Vehicles Using Machine Learning. *IEEE Internet Things J.* **2022**, *9*, 2817–2828. [CrossRef]
216. Nie, L.; Ning, Z.; Wang, X.; Hu, X.; Cheng, J.; Li, Y. Data-Driven Intrusion Detection for Intelligent Internet of Vehicles: A Deep Convolutional Neural Network-Based Method. *IEEE Trans. Netw. Sci. Eng.* **2020**, *7*, 2219–2230. [CrossRef]
217. Lin, K.; Li, Y.; Deng, J.; Pace, P.; Fortino, G. Clustering-Learning-Based Long-Term Predictive Localization in 5G-Envisioned Internet of Connected Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 5232–5246. [CrossRef]
218. Zhang, Q.; Yu, K.; Guo, Z.; Garg, S.; Rodrigues, J.; Hassan, M.M.; Guizani, M. Graph Neural Networks-driven Traffic Forecasting for Connected Internet of Vehicles. *IEEE Trans. Netw. Sci. Eng.* **2021**, *9*, 3015–3027. [CrossRef]
219. Wang, W.; Liu, F.; Zhi, X.; Zhang, T.; Huang, C. An Integrated Deep Learning Algorithm for Detecting Lung Nodules with Low-Dose CT and Its Application in 6G-Enabled Internet of Medical Things. *IEEE Internet Things J.* **2021**, *8*, 5274–5284. [CrossRef]
220. Su, Y.S.; Ding, T.J.; Chen, M.Y. Deep Learning Methods in Internet of Medical Things for Valvular Heart Disease Screening System. *IEEE Internet Things J.* **2021**, *8*, 16921–16932. [CrossRef]
221. Jin, H.; Dai, X.; Xiao, J.; Li, B.; Li, H.; Zhang, Y. Cross-Cluster Federated Learning and Blockchain for Internet of Medical Things. *IEEE Internet Things J.* **2021**, *8*, 15776–15784. [CrossRef]
222. Zhou, X.; Liang, W.; Wang, K.I.K.; Wang, H.; Yang, L.T.; Jin, Q. Deep-Learning-Enhanced Human Activity Recognition for Internet of Healthcare Things. *IEEE Internet Things J.* **2020**, *7*, 6429–6438. [CrossRef]
223. Lin, L.; Guan, X.; Peng, Y.; Wang, N.; Maharjan, S.; Ohtsuki, T. Deep Reinforcement Learning for Economic Dispatch of Virtual Power Plant in Internet of Energy. *IEEE Internet Things J.* **2020**, *7*, 6288–6301. [CrossRef]
224. Fang, D.; Guan, X.; Peng, Y.; Chen, H.; Ohtsuki, T.; Han, Z. Distributed Deep Reinforcement Learning for Renewable Energy Accommodation Assessment with Communication Uncertainty in Internet of Energy. *IEEE Internet Things J.* **2021**, *8*, 8557–8569. [CrossRef]
225. Zhou, X.; Guan, X.; Sun, D.; Jiang, H.; Peng, J.; Jin, Y.; Zhang, Y. Transient Stability Assessment Based on Gated Graph Neural Network with Imbalanced Data in Internet of Energy. *IEEE Internet Things J.* **2021**, *9*, 9320–9331. [CrossRef]
226. Hu, J.; Zhang, H.; Song, L.; Schober, R.; Poor, H.V. Cooperative Internet of UAVs: Distributed Trajectory Design by Multi-Agent Deep Reinforcement Learning. *IEEE Trans. Commun.* **2020**, *68*, 6807–6821. [CrossRef]
227. Yang, B.; Cao, X.; Yuen, C.; Qian, L. Offloading Optimization in Edge Computing for Deep-Learning-Enabled Target Tracking by Internet of UAVs. *IEEE Internet Things J.* **2021**, *8*, 9878–9893. [CrossRef]
228. Zhou, D.; Sheng, M.; Wang, Y.; Li, J.; Han, Z. Machine Learning-Based Resource Allocation in Satellite Networks Supporting Internet of Remote Things. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 6606–6621. [CrossRef]

229. Yan, J.; Gong, Y.; Chen, C.; Luo, X.; Guan, X. AUV-Aided Localization for Internet of Underwater Things: A Reinforcement-Learning-Based Method. *IEEE Internet Things J.* **2020**, *7*, 9728–9746. [CrossRef]
230. Trichili, A.; Issaid, C.B.; Ooi, B.S.; Alouini, M.S. A CNN-Based Structured Light Communication Scheme for Internet of Underwater Things Applications. *IEEE Internet Things J.* **2020**, *7*, 10038–10047. [CrossRef]
231. Gu, B.; Zhang, X.; Lin, Z.; Alazab, M. Deep Multiagent Reinforcement-Learning-Based Resource Allocation for Internet of Controllable Things. *IEEE Internet Things J.* **2021**, *8*, 3066–3074. [CrossRef]
232. Lin, B.; Wang, X.; Yuan, W.; Wu, N. A Novel OFDM Autoencoder Featuring CNN-Based Channel Estimation for Internet of Vessels. *IEEE Internet Things J.* **2020**, *7*, 7601–7611. [CrossRef]
233. Dai, C.; Liu, X.; Xu, H.; Yang, L.T.; Deen, J. Hybrid Deep Model for Human Behavior Understanding on Industrial Internet of Video Things. *IEEE Trans. Ind. Inform.* **2021**, *18*, 7000–7008. [CrossRef]
234. Wang, T.; Cao, Z.; Wang, S.; Wang, J.; Qi, L.; Liu, A.; Xie, M.; Li, X. Privacy-Enhanced Data Collection Based on Deep Learning for Internet of Vehicles. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6663–6672. [CrossRef]
235. Alladi, T.; Kohli, V.; Chamola, V.; Yu, F.R. Securing the Internet of Vehicles: A Deep Learning-Based Classification Framework. *IEEE Netw. Lett.* **2021**, *3*, 94–97. [CrossRef]
236. Grover, H.; Alladi, T.; Chamola, V.; Singh, D.; Choo, K.K.R. Edge Computing and Deep Learning Enabled Secure Multitier Network for Internet of Vehicles. *IEEE Internet Things J.* **2021**, *8*, 14787–14796. [CrossRef]
237. Sharma, P.; Liu, H. A Machine-Learning-Based Data-Centric Misbehavior Detection Model for Internet of Vehicles. *IEEE Internet Things J.* **2021**, *8*, 4991–4999. [CrossRef]
238. Lu, Y.; Huang, X.; Zhang, K.; Maharjan, S.; Zhang, Y. Blockchain Empowered Asynchronous Federated Learning for Secure Data Sharing in Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2020**, *69*, 4298–4311. [CrossRef]
239. Wang, J.; Wu, L.; Wang, H.; Choo, K.K.R.; He, D. An Efficient and Privacy-Preserving Outsourced Support Vector Machine Training for Internet of Medical Things. *IEEE Internet Things J.* **2021**, *8*, 458–473. [CrossRef]
240. Awan, K.A.; Din, I.U.; Almogren, A.; Almajed, H.; Mohiuddin, I.; Guizani, M. NeuroTrust—Artificial-Neural-Network-Based Intelligent Trust Management Mechanism for Large-Scale Internet of Medical Things. *IEEE Internet Things J.* **2021**, *8*, 15672–15682. [CrossRef]
241. Gope, P.; Millwood, O.; Sikdar, B. A Scalable Protocol Level Approach to Prevent Machine Learning Attacks on Physically Unclonable Function Based Authentication Mechanisms for Internet of Medical Things. *IEEE Trans. Ind. Inform.* **2022**, *18*, 1971–1980. [CrossRef]
242. Ding, Y.; Wu, G.; Chen, D.; Zhang, N.; Gong, L.; Cao, M.; Qin, Z. DeepEDN: A Deep-Learning-Based Image Encryption and Decryption Network for Internet of Medical Things. *IEEE Internet Things J.* **2021**, *8*, 1504–1518. [CrossRef]
243. Singh, M.; Aujla, G.S.; Bali, R.S. A Deep Learning-Based Blockchain Mechanism for Secure Internet of Drones Environment. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 4404–4413. [CrossRef]
244. Yao, J.; Ansari, N. Secure Federated Learning by Power Control for Internet of Drones. *IEEE Trans. Cogn. Commun. Netw.* **2021**, *7*, 1021–1031. [CrossRef]
245. Nawaz, S.J.; Sharma, S.K.; Wyne, S.; Patwary, M.N.; Asaduzzaman, M. Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future. *IEEE Access* **2019**, *7*, 46317–46350. [CrossRef]
246. Dunjko, V.; Briegel, H.J. Machine learning & artificial intelligence in the quantum domain: A review of recent progress. *Rep. Prog. Phys.* **2018**, *81*, 074001.
247. Li, Y.; Aghvami, A.H.; Dong, D. Intelligent Trajectory Planning in UAV-Mounted Wireless Networks: A Quantum-Inspired Reinforcement Learning Perspective. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 1994–1998. [CrossRef]
248. Wei, Q.; Ma, H.; Chen, C.; Dong, D. Deep Reinforcement Learning with Quantum-Inspired Experience Replay. *IEEE Trans. Cybern.* **2021**, *52*, 9326–9338. [CrossRef] [PubMed]
249. Masuyama, N.; Loo, C.K.; Seera, M.; Kubota, N. Quantum-Inspired Multidirectional Associative Memory with a Self-Convergent Iterative Learning. *IEEE Trans. Neural Netw. Learn. Syst.* **2018**, *29*, 1058–1068. [CrossRef] [PubMed]
250. Dong, D.; Chen, C.; Chu, J.; Tarn, T.J. Robust Quantum-Inspired Reinforcement Learning for Robot Navigation. *IEEE/ASME Trans. Mechatronics* **2012**, *17*, 86–97. [CrossRef]
251. Patel, O.P.; Bharill, N.; Tiwari, A.; Prasad, M. A Novel Quantum-Inspired Fuzzy Based Neural Network for Data Classification. *IEEE Trans. Emerg. Top. Comput.* **2021**, *9*, 1031–1044. [CrossRef]

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