1-1-2022

A review on security issues and solutions of the internet of drones

Wencheng Yang
Edith Cowan University

Song Wang

Xuefei Yin

Xu Wang

Jiankun Hu

10.1109/OJCS.2022.3183003
Yang, W., Wang, S., Yin, X., Wang, X., & Hu, J. (2022). A review on security issues and solutions of the internet of drones. IEEE Open Journal of the Computer Society, 3, 96-110. https://doi.org/10.1109/OJCS.2022.3183003

IEEE Open Journal of the Computer Society

Received 13 May 2022; accepted 8 June 2022. Date of publication 14 June 2022;
date of current version 4 July 2022. The review of this paper was arranged by Associate Editor Deze Zeng.

Digital Object Identifier 10.1109/OJCS.2022.3183003

A Review on Security Issues and Solutions of the Internet of Drones

WENCHENG YANG [1], SONG WANG [2], XUEFEI YIN [3], XU WANG [4] (Member, IEEE), AND JIANKUN HU [5,6] (Senior Member, IEEE)

[1]Security Research Institute, School of Science, Edith Cowan University, Cyber Security Cooperative Research Centre, Joondalup, WA 6027, Australia
[2]School of Computing, Engineering and Mathematical Sciences, La Trobe University, Melbourne, VIC 3086, Australia
[3]School of Engineering and Information Technology, University of New South Wales, Canberra, ACT 2600, Australia
[4]School of Electrical and Data Engineering, University of Technology Sydney, Sydney, NSW 2007, Australia
[5]School of Engineering and Information Technology, University of New South Wales, Canberra, ACT 2600, Australia
[6]Australian Defence Force Academy, University of New South Wales, Canberra, ACT 2600, Australia

CORRESPONDING AUTHOR: JIANKUN HU (e-mail: j.hu@adfa.edu.au)

This work was supported in part by Cyber Security Research Centre Ltd., through the Australian Government Cooperative Research Centres (CRC) Program, in part by ARC Discovery under Grants DP190103660 and DP200103207, and in part by ARC Linkage under Grant LP180100663.

ABSTRACT The Internet of Drones (IoD) has attracted increasing attention in recent years because of its portability and automation, and is being deployed in a wide range of fields (e.g., military, rescue and entertainment). Nevertheless, as a result of the inherently open nature of radio transmission paths in the IoD, data collected, generated or handled by drones is plagued by many security concerns. Since security and privacy are among the foremost challenges for the IoD, in this paper we conduct a comprehensive review on security issues and solutions for IoD security, discussing IoD-related security requirements and identifying the latest advancement in IoD security research. This review analyzes a host of important security technologies with emphases on authentication techniques and blockchain-powered schemes. Based on a detailed analysis, we present the challenges faced by current methodologies and recommend future IoD security research directions. This review shows that appropriate security measures are needed to address IoD security issues, and that newly designed security solutions should particularly consider the balance between the level of security and cost efficiency.

INDEX TERMS Authentication, blockchain, internet of drones (IoD), privacy, security.

I. INTRODUCTION

Drones, also called Unmanned Aerial Vehicles (UAVs), have unique features – mobile, easy to maintain and deploy, and capable of measuring numerous quantities at any location anytime. It is a cost-effective solution for gathering and transferring data (e.g., images or videos) and performing required data analysis [1]. With the modernization of the Internet of Things (IoT), the network of drones has been given a new term, called the Internet of Drones (IoD). The IoD possesses similar properties to the IoT and supports the coordination of drones in the air [2]. The IoD can be widely described as a layered network control architecture, aimed at coordinating drones' access to controlled airspace and offering navigation services [3]. In the IoD, numerous drones join and create a network, simultaneously transmitting data to each other and receiving data from each other. Provisions are made for the IoD to be operated distantly, or via the Internet with an Internet Protocol (IP) address. An example of a typical IoD architecture is demonstrated in Fig. 1.

In recent years, the IoD has become a popular research topic in both industry and academia because of its obvious advantages (e.g., mobility, portability and automation). Drones have been applied in many fields, such as military, air traffic control and agriculture. In the IoT environment, drones are utilized in flight domains where they interact with each other to exchange important information [4]. However, the rising popularity of drones has increased the frequency of cyber attacks against IoD systems. For example, adversaries can target the radio connection of drones in an effort to impede the system's

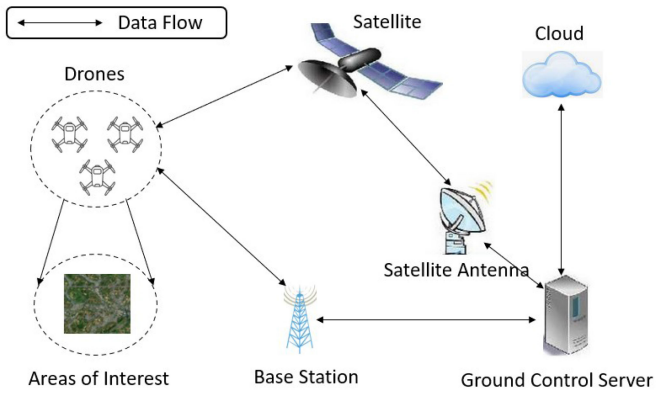

FIGURE 1. An example of IoD architecture (adapted from [6]).

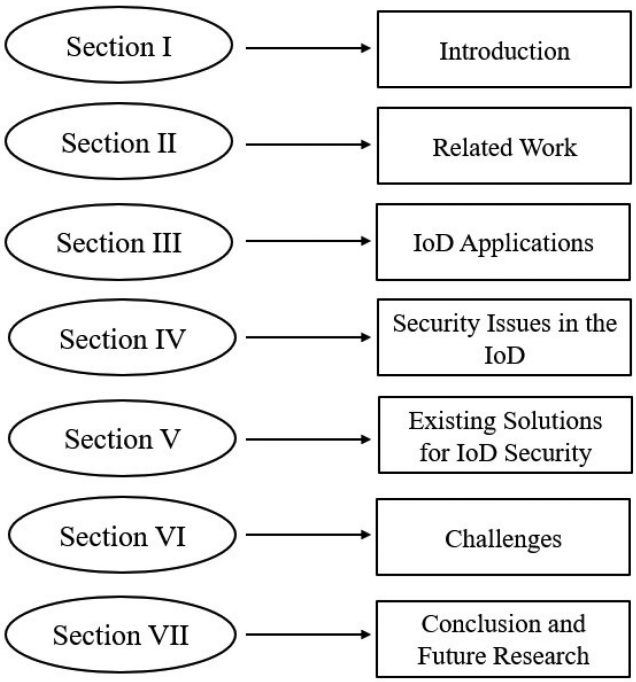

FIGURE 2. Organization of this paper.

communication with users' devices. This intercepted communication information enables the adversary to steal data (e.g., the command/control signals) requested and transmitted by drones. The adversary can manipulate the acquired data to directly control the drone. In addition, by exploiting vulnerabilities in the drone software, adversaries can remotely hijack drones. Global Positioning System (GPS) signals, affected by malicious software programs on drones [5], can be controlled by adversaries for malicious purposes.

Regardless of the advances in drone communications and the vast array of possible solutions, security remains a primary concern for the IoD, as transmissions entail sensitive and critical data. Drones are typically operated remotely and receive control signals and commands from sites on the ground. These signals are coordinated in the IoD. In situations of autonomous drones, these command and control signals are transmitted through various channels with different transmission ratios, thus requiring a significant effort in management and control. Therefore, how to secure wireless communication channels as well as transmitted data is crucial for IoD systems, and IoD security is one of the most important requisites for IoD applications [2].

A. CONTRIBUTIONS OF THIS WORK

This paper provides a comprehensive review of key issues in the IoD, such as security and privacy, IoD security solutions and challenges, and potential research topics on IoD security (e.g., the integration of the IoD with emerging technologies). This IoD-oriented study will benefit future research and development of the IoD by providing valuable insights on IoD security. The main contributions of this work are summarized as follows.

- This review paper focuses on IoD security issues and solutions, analyzing a host of important technologies for securing the IoD. Most of the existing surveys (e.g., [1], [4], [7]–[9]) only discussed general issues of the IoD, such as applications, architectures, types of drones, communications. The security issues of the IoD have only been studied so far in a small number of papers (e.g., [10]–[12]), and these studies did not adequately discuss state-of-the-art security mechanisms applicable to the IoD. In particular, security solutions such as authentication techniques and emerging blockchain-powered schemes have not been analyzed in so much detail as in this paper.
- Based on a detailed analysis, challenges facing authentication and blockchain-powered schemes are demonstrated and discussed.
- Promising research directions are presented, which shed light on how to strengthen the protection of the IoD.

B. ORGANIZATION OF THIS WORK

This paper is organized as follows. Section II presents related work. Section III summarises IoD applications and corresponding categories. Section IV focuses on the security and privacy issues of the IoD, while security solutions are provided in Section V. Section VI discusses challenges regarding IoD security and privacy. Section VII concludes the paper and identifies future research directions. The organization or roadmap of this paper is illustrated in Fig. 2.

II. RELATED WORK

In this section, we review IoD-related survey papers. These survey papers provide an overview of the IoD in terms of applications, communications, architectures, frameworks and security. A summary of the existing IoD-related surveys and this work is provided in Table 1.

Altawy and Youssef [10] surveyed the key security, privacy and safety issues relating to civilian drones. The authors

TABLE 1. A Summary of IoD-Related Surveys

Survey Papers	Year	Highlights	Focus on Security
Altawy and Youssef [10]	2016	The main research directions proposed in this survey paper are forensic investigation, intrusion detection, drone fleets communication and the effect of security implementation on system functionality.	Yes
Alsamhi et al. [1]	2019	This survey paper discusses how cooperative drones and the IoT can enhance smart cities in terms of data gathering, public security, hazard management, energy conservation and living quality.	No
Fotouhi et al. [9]	2019	This survey reviews topics like types of consumer-grade currently available drones, challenges and opportunities of cellular communications for drones, and the cyber-physical security of drone-aided cellular communications.	No
Ilgi and Ever [13]	2020	In this survey, communication, security, and confidentiality issues of the IoD and the existing solutions are analyzed through case studies.	No
Zhi et al. [8]	2020	This survey paper investigates the threats to the IoD from three aspects, namely sensors, communications, and multi-UAVs' security and privacy.	No
Ayamga et al. [7]	2021	This survey paper presents the current development of drones in agricultural, medical and military applications, and analyzes the strengths, weaknesses, opportunities and threats of drone deployment in these applications.	No
Abdelmaboud [5]	2021	This survey paper covers multi-facets of the IoD, such as requirements (e.g., communication and security), taxonomy (e.g., architecture, middleware, data fusion and sharing, and security), applications, and recent advances.	No
Abualigah et al. [4]	2021	This survey gives a comprehensive review of IoD applications (e.g., smart city surveillance) as well as integration of the IoD with privacy protection and security authentication.	No
Boccadoro et al. [6]	2021	This survey classifies and reviews IoD-related topics along two directions: applications and structure of the IP stack.	No
Chamola et al. [11]	2021	This survey paper conducts a review on the attacks to the IoD and the corresponding prevention techniques.	Yes
Labib et al. [14]	2021	This survey paper studies the latest IoD technologies for low-altitude traffic management. It also discusses the status of technology standardization and the synergy between scientific research and standardization efforts in achieving safe drone operations.	No
Nguyen and Nguyen [12]	2021	This survey overviews cyber security weaknesses and cyber attacks by means of a meta-analysis of the literature on drones. This study also discusses how to detect and defend cyber attacks.	Yes
This work	2022	This review paper focuses on IoD security issues and solutions, analyzing a host of important technologies for securing the IoD, especially authentication techniques and emerging blockchain-powered schemes, which have not been adequately considered and analyzed in the existing IoD surveys.	Yes

pinpointed both physical and cyber threats to IoD systems, and predicted that security would be a core enabling technique for upcoming civilian drone development. Ayamga *et al.* [7] conducted an analysis on the strengths, weaknesses and opportunities of agricultural, medical, and military drones in their respective fields. The authors noted that research and development of drone technologies can assist in reducing vulnerabilities and mitigating threats to drones in those fields. In addition, the authors indicated that regulations are needed globally to harness the full potential of drones. Alsamhi *et al.* [1] surveyed potential technologies and applications of recently proposed cooperative drones and the IoT that aim to improve the intelligence of smart cities. This survey highlights the existing and upcoming research in cooperative drones and the IoT and their real-time applications to smart cities. The survey seeks to illustrate how cooperative drones and the IoT can enhance smart cities in terms of data gathering, public security, hazard management, energy conservation and living quality in smart cities. Abdelmaboud [5] presented a taxonomy of the IoD, including key prospects of the IoD, such as security, communication, recent advances and solutions. The authors also discussed commonly used business case studies, the latest technologies for the IoT, challenges and future research of the IoD.

Abualigah *et al.* [4] surveyed the IoD and its applications, deployment and integration. The survey focused on two areas, IoD applications and IoD integration. IoD applications include networking, mobile computing and smart city surveillance, while IoD integration is concerned with neural networks, blockchains, privacy protection and so on. Boccadoro *et al.* [6] classified the multifaceted nature of the IoD along two directions. One direction is potential applications and operating scenarios of the IoD. The other direction is about the issues and challenges of each layer of the IP stack structure. The authors also discussed IoD-related research priorities and future studies, with a focus on the most prospective technologies that merit further development of the IoD. Ilgi and Ever [13] critically analyzed the security and privacy challenges of the IoD and the existing solutions through case studies. The authors suggested that future IoD research should

focus on developing secure and efficient solutions for access control.

Zhi *et al.* [8] investigated three important aspects of threats to drones, namely sensors, communication and multi-drone security and privacy. Spoofing and attacking sensors can have a deadly effect, as misinformation from sensors can result in misjudgments by drones, while damaged sensors may lead to unavailability of information to drones, and in severe cases, drone crashing. In addition, insecure communication links between drones are vulnerable to attacks. Furthermore, privacy breaches are likely caused by aerial photographs. Chamola *et al.* [11] reviewed main attacks to the IoD and the use of anti-IoD-attack technologies to prevent attacks to the IoD. The authors began by discussing different types of the IoD, regulatory laws for IoD activities, the use cases of the IoD, and entertainment and military IoD incidents. After showing how they operate, the authors described various techniques for IoD attack preparation and detection in the context of case studies. Fotouhi *et al.* [9] gave a comprehensive survey on UAV developments that facilitate the seamless incorporation of drones into cellular networks. The authors reviewed the types of consumer-grade drones currently available, the challenges and opportunities of cellular communications for drones, new regulations under development to govern the commercial use of drones, and the cyber-physical security of drone-aided cellular communications.

The use of the IoD brings new research challenges in terms of privacy, security, and most obviously, the safe management of drone operations in high traffic demand. Labib *et al.* [14] studied the latest IoD technologies for low-altitude traffic management. The authors discussed the status of technology standardization and emphasized the synergy between scientific research and standardization efforts in achieving safe drone operations, while taking into account challenges inherent to the IoD, such as security and data protection. In order to raise users' cyber consciousness and boost future IoD research, Nguyen and Nguyen [12] overviewed cyber security weaknesses and cyber attacks by means of a meta-analysis of the literature on drones. The authors also elucidated some of the countermeasures (e.g., attack detection and defensive schemes).

III. IoD APPLICATIONS

The IoD offers tremendous advantages and opportunities in a wide range of disciplines and applications. The IoD can serve as an interface for airspace allocation and can also provide exceptional reliability, navigational performance and precision for drones in a variety of applications, supporting missions and activities in agriculture, military, undersea operations and delivery, healthcare and medical services [7]. In this section, we present main IoD applications, as illustrated in Fig. 3.

A. AGRICULTURE

In agriculture, drones equipped with advanced cameras can deliver real-time data from farms. They help farmers obtain accurate information about soil humidity, evaporation, soil texture, crop fertility, etc. anytime and anywhere, thus allowing farmers to make well-informed decisions about the use of agricultural inputs accordingly to enable higher crop yields [5]. In addition, crop yields are susceptible to various threats (e.g., wildlife and fire). With the IoD, farmers can receive early warnings about threats so that they can be detected and even defused at the earliest point in time.

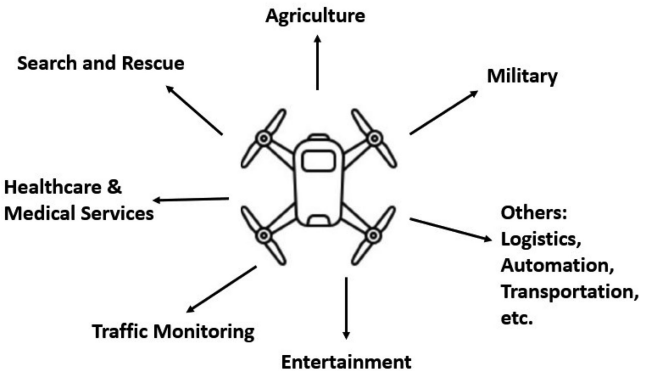

FIGURE 3. Categories of IoD Applications.

Puri *et al.* [15] analyzed the importance of implementing and using drones in agriculture and additional benefits farmers can have on crop yields through the use of drones. These benefits include agricultural farm analysis, improving agricultural yields and imaging crop health. Mogili and Deepak [16] briefly described the use of drones in agricultural crop monitoring and spraying of pesticides. The authors reported that the World Health Organization (WHO) has estimated about one million cases of illness caused by manual pesticide spraying. If drones are used, the drones' cameras can take photos and perform analysis through geographic indicators. Based on the analysis results, drones can easily locate the area where pesticide needs to be sprayed. The drone spraying system automatically navigates through the GPS coordinates and sprays pesticides to infected areas. As a result, drones help spraying efforts safer and faster than humans.

B. MILITARY

Military use of drones has emerged as a major IoD application. Drones have become part of military forces around the world and are used in circumstances where piloted flying is deemed too dangerous or too challenging. Military drones can aid combat tasks, monitor enemy actions and assist in selecting targets for military attacks [17]. They offer troops an eye in the sky 24 hours a day.

Kreps and Wallace [18] investigated the employment of drones for counter-terrorism purposes, a highly controversial topic. This work answers the question about whether legal criticism at the international level affects public support for drone strikes and the centerpiece of U.S. counter-terrorism policies. The authors also discussed if individuals are convincingly persuaded by arguments based on the effectiveness

of drones. Chand *et al.* [19] developed a drone-based high-speed wireless mesh network for regions with no network infrastructure, like in disaster scenarios or military disputes. The study shows that upon arriving in the destination area, the drone can utilize the wireless mesh network to deliver Wi-Fi and disclose local situation with an inbuilt camera. The transmitted video can be displayed at the control center or on mobile phones for real-time monitoring. The proposed network offers up to 160 Mbps wireless communication in a range of about 200 meters.

C. SEARCH AND RESCUE

As climate change gets worse, natural disasters are becoming more common, resulting in search and rescue playing an increasingly important role in our society. The availability of different types of sensors (e.g., thermal sensors) and cameras makes drones a powerful tool for search and rescue missions. Drones are capable of spotting the location of lost or injured people, particularly in adverse conditions or in difficult terrain. Apart from locating unfortunate victims, drones can deliver supplies to inaccessible places in war- or disaster-torn areas [17].

Cui *et al.* [20] addressed the issues presented in the International Micro Air Vehicle Competition in 2014, dealing with the use of drones in urban post-disaster search and rescue tasks. This study documents the solutions to all key task components in the Competition. The proposed schemes were well showcased, making the authors win the Competition. Tilburg [21] reported two case studies to demonstrate the capabilities of drones in search and rescue missions. In Case 1, a rescue team discovered a dead person through the drone's camera and then dispatched rescuers into a narrow valley at night. In Case 2, the drone augmented the ground search, obtaining images of difficult or unsearchable areas (e.g., creek floors and cliffs) and helping accomplish the rescue mission.

Mayer *et al.* [22] illustrated the likely search and rescue scenarios for the deployment of drones. The authors also outlined the challenges and opportunities of human-machine interaction. Using a simulation model, Karaca *et al.* [23] explored the potential use of drones in locating and searching for victims as well as the mobile transportation of search and rescue personnel in mountainous environments. The authors compared two techniques used to search and rescue victims unconscious on snow.

D. ENTERTAINMENT

Versatile and entertaining drones are in demand. Quiroz and Kim [24] produced an initial abstract design of a confetti drone for "drone entertainment" – a robotic drone system dispensing debris particles. The concept was realized with a micro-controller and a 3D printed jar. The confetti jar was presented to test the feasibility of the drone for dispensing confetti pellets. Kim *et al.* [25] explored how drones are used in the entertainment and Augmented and Virtual Reality (AVR) fields, as they become increasingly useful in science, business and entertainment sectors. Industries and individuals are beginning to see the potential of drone technologies, which are expanding into the realm of creating mixed reality. This work provides an overview of drones and the features of their applications in entertainment and AVR.

E. HEALTHCARE AND MEDICAL SERVICES

Drones can be utilized to transport medical supplies, such as blood samples, vaccines and medicines, to remote areas in the developing world during health emergencies.

E. Scott and H. Scott [26] examined the state of innovative drone delivery with a special emphasis on healthcare. The authors discussed the latest decision models that contribute to management decisions on drone fleet operations. It is worth noting that the new models in this study relevant to the design of drone-based medical delivery networks can facilitate more prompt, effective and economical drone medical deliveries, possibly leading to saving lives. Drones are highly promising aerial transport devices for medical products, and have a great potential to transport medical supplies in healthcare systems to overcome limitations in maternal health services, especially in the case of obstetric emergencies. Zailani *et al.* [27] performed a systematic review to investigate the scientific proof about potential positive effects of drone transport on maternal health. The authors identified significant gaps in studies that analyze medical transport models and the adaptation of drones in maternal healthcare.

F. TRAFFIC MONITORING

Barmpounakis and Geroliminis [28] built a comprehensive urban dataset to investigate the congestion issue. This dataset includes multi-day traffic flow records of the central business district of Athens gathered by a fleet of 10 drones. The establishment of this dataset facilitates an in-depth study of key traffic phenomena and greatly benefits researchers to develop and test their models. Christodoulou and Kolios [29] designed optimal trip plans that a fleet of drones could comply with to perform fast traffic surveillance in specific areas of traffic networks. The authors first determined the monitoring sites that drones should overfly, and then calculated travel plans with minimum travel times depending on realistic resource limitations. The proposed method was evaluated on a realistic road network topology to prove its suitability. Exploiting drones' advantages, such as superior mobility, timely manipulation, information richness and cost-effectiveness, Mac *et al.* [30] designed an intelligent IoD system to apply drones to traffic speed monitoring. The proposed system was validated using a laboratory-scale system.

G. OTHERS

In addition to the aforementioned IoD applications, there are other ares where the IoD is applicable, such as logistics, infrastructure inspection, automation and smart transportation.

Menouar *et al.* [31] examined the utilization, optimal deployment and security concerns of drones in intelligent transportation system scenarios. The study found that while drones are likely to become a major part of future smart

cities, there are a number of challenges in the research and implementation of drones, from limitations on batteries to flight legislation of drones. Besada *et al.* [32] designed a multipurpose drone-oriented mission definition system. The system is designed to ease definitions of missions through visual tools for the automatic operation of different types of infrastructure checks. It overcomes the constraints of basic tools provided by drone producers and fosters a shared view of operations between users and pilots. Jasim *et al.* [33] studied the factors that affect consumers' intention to use drones for food delivery in Malaysia, namely drone food delivery (DFD) services. The authors formulated a total of 11 scenarios to study consumers' intention and use of DFD services. The data for this study were obtained from 209 Malaysian participants who frequently ordered food delivery online. The findings reveal that 88.6% of the participants had experienced food delivery services online, and 40.7% of them had heard of DFD services.

IV. SECURITY ISSUES IN THE IoD

When in operation, drones are often outfitted with sensors to gather all sorts of information, such as images, videos and position data. The way personal information is collected, processed, utilized, deposited and disclosed is of public concern. Private or sensitive information of individuals and businesses must be safeguarded from misuse. However, the IoD is a target of many hostile security and privacy attackers. If a drone carrying valuable data is hijacked, the loss can be significant. More damage is likely to be caused to a military drone when it is compromised. The consequence is not only the damage to the data or physical components of the drone, but the attacked drone can be used as a weapon by adversaries [34]. In this section, we consider and discuss some essential security requirements of the IoD as well as cyber security attacks to the IoD.

A. SECURITY REQUIREMENTS OF THE IoD

As data transmitted by the IoD may involve sensitive and critical information, security is a major concern in the use of the IoD. Drones are typically operated remotely and receive control and command signals from ground sites. These command and control signals are transmitted through various sources at different transmission rates, which require significant effort to manage and control [2]. In the IoD environment, since the information exchange between entities is critical, it should not be leaked or compromised under any circumstances. IoD security is vitally important for drone utilization. Robust protection mechanisms are needed to prevent any kind of information leakage [35]. However, drones may not be able to incorporate complex security functions due to limited resources.

Confidentiality, integrity, availability, authenticity and privacy preservation are essential security and privacy requirements of the IoD. These requirements reflect the capabilities and functions of the IoD in tackling threats and security breaches [34], [35].

- *Confidentiality:* The confidentiality of wireless communication channels prevents information leakage in the IoD.
- *Integrity:* It ensures that the information handled by the IoD is intact.
- *Availability:* Relevant IoD services should be available to authorized users even in the event of certain attacks.
- *Authenticity:* It is regarding the authentication of drones, users and gateway points before granting access or disclosing critical information.
- *Privacy:* Protecting privacy is imperative for the IoD. Geolocation or personally identifiable data generated by drones can be used to profile individuals [3]. Leakage of these data raises serious privacy concerns and puts location- and identity-related information at risk.

B. CYBER SECURITY ATTACKS TO THE IoD

Ensuring IoD security is by no means an easy task due to varying communication standards and the scope of applications. Drones are subject to a variety of attacks. According to [34], [36], below are some common attacks targeting the IoD.

1) JAMMING ATTACKS

Attackers interfere with radio signals to cause problems to the connectivity of the IoD, preventing it from operating effectively as well as affecting energy consumption. The initial purpose of jamming is to deliberately disturb the communication streams of the IoD, which can result in a crash or unavailability of IoD services [2].

2) TAMPERING ATTACKS

Attackers intentionally destroy, manipulate or edit data via unauthorized IoD channels. Data in transit or at rest may be intercepted and tampered with. For instance, given a data packet transmitted without protection over an IoD channel, the attacker could intercept the packet, alter its contents and modify its intended destination address [36].

3) COLLISION ATTACKS

When two or more drones operate at the same frequency, it will cause information collision and make network operation unstable. Collisions usually happen because of the poor communication ability and restricted computing resources of the IoD network [37].

4) SELECTIVE FORWARDING ATTACKS

A malicious drone node acts most of the time like a normal drone node, but can selectively discard sensitive or important packets. Selective forwarding attacks are usually most efficient when the malicious node is included explicitly in the path of data streams [38]. This attack can cause all types of packets to be interrupted or dropped, making the entire IoD network unreliable.

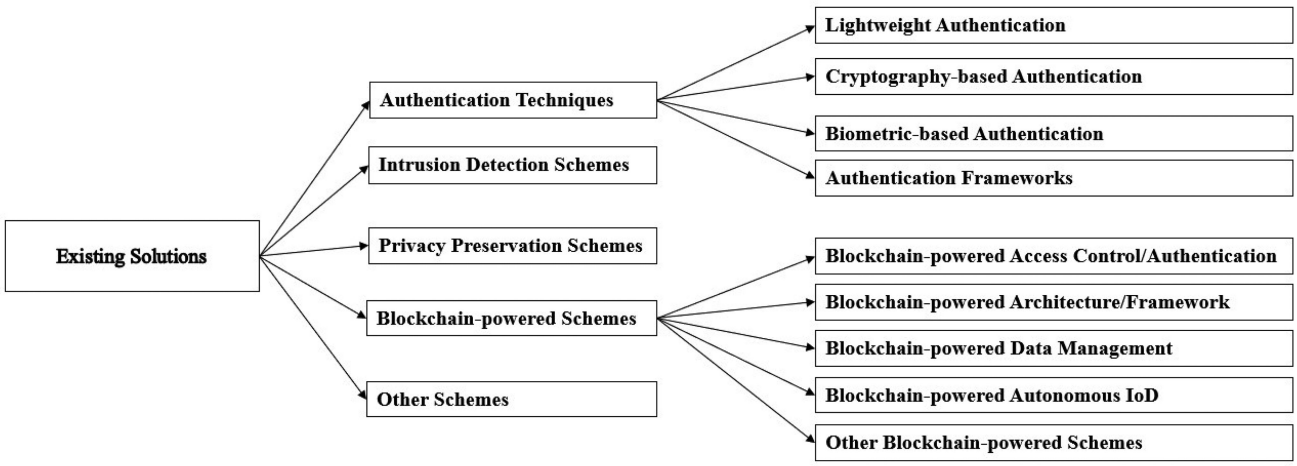

FIGURE 4. Categories of existing solutions for IoD security.

5) FLOODING ATTACKS

A main objective of malicious drones is to flood legitimate drones with large amounts of raw or copied packets. This type of attack can use up limited drone resources (e.g., communication bandwidth and storage space of drones), resulting in extremely large traffic and congestion throughout the IoD network [39].

6) HIJACKING ATTACKS

This type of attack makes some drones inoperable, causing network outages. Several techniques can be used to hijack a drone, such as de-authentication or Wi-Fi Aircrack [40].

7) MAN-IN-THE-MIDDLE ATTACKS

Attackers can deploy malicious drones between operating networks, causing information leaks, outages and other security problems. In addition, attackers can eavesdrop on traffic between a drone and the ground control station, or masquerade as the ground control station, giving false instructions to abort an active mission or even gain control of the drone [41].

8) DENIAL-OF-SERVICE (DOS) ATTACKS

DoS attackers attempt to block legitimate service users from the required resources. The attacker can send large amounts of requests to the server to cause network congestion. Consequently, legitimate users are unable to access services [9].

9) OTHER ATTACKS

These include replay attacks, impersonation attacks, tracing and side channel attacks [42].

V. EXISTING SOLUTIONS FOR IoD SECURITY

Due to the absence of security measures on communication channels and communicating entities of the IoD, security issues arise and various adversarial attacks to the IoD may happen. Therefore, to withstand the detrimental impacts of a wide range of known and unknown security threats [34], it is necessary to establish protection mechanisms for IoD security, including real-time strategies, anti-attack mechanisms and easy-to-update security solutions. In this section, we analyze state-of-the-art security solutions, such as authentication techniques, blockchain-powered schemes, intrusion detection methods and privacy preservation approaches. Note that the focus of this study is authentication techniques and blockchain-powered schemes. The categories of existing solutions for IoD security are demonstrated in Fig. 4.

A. AUTHENTICATION TECHNIQUES

The majority of IoD applications is real-time-based, and IoD customers generally expect to receive real-time data from drones that are part of a specific flight area. However, this could lead to a serious security vulnerability if users are permitted to have direct access to real-time data from flying drones without user authentication [43] in the IoD environment. Data collected in different applications requires protection to meet the authenticity requirement of the IoD. If not, any corrupted unit could render the whole IoD susceptible. For the sake of IoD security, unauthenticated individuals should not be given access to data transmitted by drones [1].

1) LIGHTWEIGHT AUTHENTICATION

Traditional authentication protocols (e.g., signature and public-key cryptosystems) are unsuitable for the IoD, because drones usually have resource constraints, requiring lightweight authentication techniques [44].

Srinivas *et al.* [45] utilized mobile devices, passwords and biometrics to develop an anonymous lightweight user authentication method for IoD environments based on temporal credentials. The proposed method can be efficiently implemented for all participants. In a flight area, some drones communicate with each other and with the ground station server, which is the only trusted entity in IoD settings. External users with their own mobile devices are able to monitor

and gain access to a number of designated drones in the flight area, as long as they are authorized users. The security components of the proposed method were rigorously tested. Nyangaresi and Petrovic [42] developed a lightweight physical unclonable function-based authentication protocol for the resource-constrained IoD. The protocol is computationally efficient using only lightweight exclusive OR (i.e., XOR), concatenation and hashing operations. In the proposed solution, session keys and transient security parameters are updated dynamically to improve security, making it computationally impracticable for adversaries to obtain session keys and ephemeral parameters. The security analysis shows that the proposed method is resistant to IoD attacks such as packet replay and impersonation attacks.

2) CRYPTOGRAPHY-BASED AUTHENTICATION

Authentication is an important function of the IoD to verify the true identity of all communication entities in the IoD prior to the exchange of any sensitive data. Many cryptography-based authentication schemes have been proposed for the IoD in the literature.

Using elliptic curve cryptography (ECC) and symmetric key primitives, Hussain *et al.* [46] designed an authentication scheme for the IoD to protect the communication between users and drones. The design is based on three elements, cryptography, biometrics and mobile devices. The proposed scheme's security is evaluated formally using a random oracle model (ROM). Nikooghadam *et al.* [47] proposed an effective and safe ECC-based authentication solution for the IoD to enable secure and intelligent monitoring and mobility for smart city residents. This work takes into account users, drones and the control server. Users and drones are registered to the control server so as to obtain the required credentials. They further authenticate each other with the help of the server and create a session key to correspond directly without the involvement of the server. The security analysis shows that the proposed solution can defuse the well-known latent attacks.

Authentication and key agreement (AKA) protocols as a subset of cryptography-based authentication produce shared session keys between drones and users to encrypt the transmitted information. For example, Zhang *et al.* [48] developed an efficient AKA IoD protocol based on FourQ curves and Boyko-Peinado-Venkatesan (BPV) precomputing. This protocol is robust to a variety of known attacks and possesses multiple security properties, in particular perfect forward secrecy. Compared to conventional elliptic curve-based methods, the efficiency of the proposed protocol is greatly improved by incorporating FourQ curves and BPV precomputing. The results of practical experiments conducted on Raspberry Pi show that the improved FourQ curve primes are four to five times faster than traditional elliptic curve primes. Zhang *et al.* [49] proposed an AKA scheme in which drones and users authenticate each other with only a secure one-way hash function and a bitwise XOR operation. The security mechanism of this scheme is realized using the ROM and is shown to be able to defeat various known attacks.

3) BIOMETRIC-BASED AUTHENTICATION

Biometrics [50] are biological measurements related to physiological and behavioral characteristics (e.g., face [51], fingerprint [52] and iris [53]), which can be used in access control and identity management. Singandhup *et al.* [54] presented an electroencephalogram (EEG)-based biometric system, which can encrypt the communication between drones and the control base station by producing a key from the user's EEG. First, the coefficients from the EEG data using Legendre polynomials are extracted. Then the coefficients are encoded using Bose-Chaudhuri-Hocquenghem (BCH) encoding and the key is produced from a hash function. Wazid *et al.* [43] combined cryptography and users' biometric data to achieve authentication in the IoD. The proposed method allows authorized users to directly access drones' data in an IoD environment. Formal security analysis shows that the proposed scheme can resist some well-known attacks. The performance comparison shows the effectiveness of the proposed approach and its security improvement over the existing methods.

4) AUTHENTICATION FRAMEWORKS

Tian *et al.* [55] proposed an effective privacy-preserving authentication framework for the IoD. By leveraging a lightweight signature design, the proposed framework guarantees authentication efficiency when deployed on resource-constrained drones. Considering the high mobility of drones, the authors explored a predictive authentication method to further reduce the cost of prospective authentication activities. Also, the authors made a buffered pseudonym and public key update policy so that the proposed framework achieves privacy protection in terms of drone identity, location and flight path. Ever [56] designed a secure authentication framework utilizing an elliptic curve cryptosystem and a layered structure. The purpose of the layered structure is to provide one-time user authentication for the entities in the IoD. Security of the proposed framework, such as data confidentiality and password guessing, is assessed against well-known attacks.

B. BLOCKCHAIN-POWERED SCHEMES

Blockchains offer decentralized data storing services and the ability to log and secure transactions or transaction events with the use of cryptography [58]. Blockchains are composed of blocks of data that are interconnected using cryptographic hash functions. All participating nodes in the blockchain are well aware of each and every transaction that takes place in the blockchain. The principles of blockchains are beneficial to the design of security mechanisms for tackling the challenges faced by the IoD [59].

1) BLOCKCHAIN-POWERED ACCESS CONTROL OR AUTHENTICATION

Bera *et al.* [60] proposed a blockchain-based access control solution in an IoD environment that permits secure communications between drones and between drones and ground station servers (GSS). Secure data collected by GSS forms the transactions which are made into blocks. These blocks are eventually added to the blockchain by the cloud servers that are connected to GSS through the Ripple Protocol Consensus Algorithm (RPCA) in the network of peer-to-peer cloud servers. Transactions contained in blocks cannot be changed, modified or deleted as soon as the block is added to the blockchain.

Since a single point of failure can affect centralized authentication methods, Feng *et al.* [61] came up with a cross-domain blockchain-based authentication solution for 5G-enabled IoD. The proposed solution uses multi-signatures with threshold-based sharing to establish an identity union for cooperative domains. This enables domain joining and exit support. Robust communication between devices across domains is achieved through smart contracts for authentication. Session keys are guaranteed by negotiation for follow-up communication between devices.

2) BLOCKCHAIN-POWERED ARCHITECTURE/FRAMEWORK

Bera *et al.* [62] introduced a new blockchain-based security framework for data management between IoD communicating entities to address the security and privacy issues of blokchains in 5G-based IoD environments. It is shown that this framework provides better security and reduces communication and computational overhead compared to other related work.

One disadvantage of blockchains is that point-to-point network updates are required every few seconds, resulting in heavy traffic in the network. This depletes network resources and may eventually lead to congestion and prolonged latency. To resolve the problem, Singh *et al.* [63] presented a lightweight blockchain architecture based on One Drone One Block for IoD development. This architecture allows each drone to only access its own block, thus making it simple, trusted and lightweight.

In the majority of drone-based applications, authentication schemes suffer from real-time latency and are vulnerable to attacks. To address both issues, Yazdinejad *et al.* [64] explored a low-latency, blockchain-based secure authentication model for drones applied to smart cities. The authors established a zone-based architecture in the drone network and employed a custom decentralized consensus, called Drone-based Delegated Proof of Stake for drones in each zone without the need of re-authentication.

Wazid *et al.* [65] proposed a powerful security protocol, aimed at defending various attacks (e.g., man-in-the-middle and replay attacks) in an IoD computing environment. When compared with the existing schemes, the proposed blockchain-based secure communication framework for the IoD demonstrated strong security, favorable performance and low computational and communication cost.

3) BLOCKCHAIN-POWERED DATA MANAGEMENT

Building on 5G communication networks and artificial intelligence (AI), Gupta *et al.* [66] developed a blockchain-based smart and secure drone communication framework. The proposed architecture utilizes the Interplanetary File System (IPFS) as the platform for data storage, ensuring increased network capacity, communication safety and privacy as well as reducing the cost of transaction storage. Yu *et al.* [67] proposed a blockchain-based IoD system, which is compliant to attribute-based encryption, enables fine-grained data access management by incorporating Chameleon hash algorithms in the blockchain, and empowers attribute updating. The authors devised and executed a verification solution on a multi-layer blockchain architecture so that rogue and misused tampering can be resisted. The proposed system delivers an update-oriented data access management in which historical data on the chain can only be accessed by new members, while revoked members are inaccessible to those data.

Singh *et al.* [59] designed a blockchain-based security mechanism for cyber-physical systems to guarantee the secure transmission of information between drones. The proposed mechanism consists of three phases: registration, verification and transaction. In this mechanism, the miner nodes are chosen using a deep learning-based approach, called deep Boltzmann machine, according to feature data, such as available battery power, computational resources and flight time of drones.

If the flight path exchange between drones and control stations is not protected, it could lead to a catastrophic situation. To mitigate such security risks, Allouch *et al.* [68] studied the security of unmanned traffic management (UTM) in the IoD. The proposed UTM-Chain is a lightweight blockchain-based security solution that uses hyperledger fabric for UTM in low-altitude drones, suitable for drones with limited computational and storage resources. In addition, UTM-Chain provides secure and unalterable traffic data between drones and the control station on the ground.

4) BLOCKCHAIN-POWERED AUTONOMOUS IoD

Muram and Javed [69] analyzed hazards and threats in the design and development of the IoD for drone-based autonomous systems. Assume-guarantee contracts are derived for uncertain sources and are incorporated into blockchain-based smart contracts. To ensure security and safety in the operating phase, contracts for uncertain sources are checked. In case of disagreement, drones offer assistance; otherwise, based on serious risk factors, system controls are adopted to prevent mishaps.

Dawaliby *et al.* [70] presented a blockchain-based drone management platform where drones are controlled to displace faulty devices. The authors gave an overview of the global blockchain-based IoD platform and smart contracts that are

programmed for the control of drone flight and repair tasks. The performance of the blockchain-based decentralized platform is compared with traditional centralized architectures, and the effectiveness of the proposed solution is evidenced by the decrease in overall operational time and the percentage of successful maintenance operations. Kumar *et al.* [71] built an energy-intensive blockchain-based platform to control the operation of drones, while taking care of the confidence and security of all parties engaged. In this work, an Ethernet blockchain was deployed to mitigate spoofing attacks. When an intruder gains access to the data of a single block in the blockchain network, there is no impact on the entire network due to data integrity offered by the encrypted distribution ledger. The blockchain network verifies geolocation data intermittently so that any outrageous data can be detected and quickly removed.

5) OTHER BLOCKCHAIN-POWERED SCHEMES

Establishing a paradigm for trusted collaboration among drone controllers is essential for the IoD. Liao *et al.* [72] utilized smart contracts and blockchains to enable trustful cooperation among controllers for the software-defined IoD (SD-IoD). First, the authors proposed a SD-IoD architecture to strengthen the support for heterogeneity of environmental monitoring and flexibility of the IoD. Next, a controller consortium blockchain was designed for the safe and effective collaboration and interoperability of drone controllers. Then, an incentive scheme was developed to encourage controllers to protect security and offer more secure services to other controllers. Singh and Venkatesan [73] proposed a notional method for blockchain and IoD cooperation that offers advantages to drones with blockchain features. In the proposed method, an Advanced Byzantine Fault-Tolerant (ABFT) consensus was suggested for drone-based applications, providing scalability with minimal cost and resources.

6) SUMMARY

The integration of blockchains with different techniques in the IoD, e.g., authentication, data management and autonomous IoD, can bring some obvious advantages, such as decentralized data storage services, tamper-evident data, improved trust and transparency, and the traceability of data transmitted across the IoD network. However, there are also challenges that should be considered, such as increased computing costs, latency, potential attacks, which will be discussed in detail in Section VI-B.

C. INTRUSION DETECTION SCHEMES

An intrusion is a malicious act of unauthorized access to a network to obtain sensitive information. An Intrusion Detection System (IDS) is a device or a software application that watches for any privacy invasion or unauthorized access to the target network [35].

Perumalla *et al.* [74] designed an intrusion detection method for the IoD based on a deep neuro-fuzzy network. With the proposed deep neuro-fuzzy network, intrusions in the IoD can be detected with minimum delay and good detection accuracy. Ramadan *et al.* [75] studied IoD intrusion threats and introduced a deep learning-based framework for real-time data analysis. Based on Recurrent Neural Networks (RNN), the proposed framework collects data from the RNN and uses Big Data analytics for anomaly detection. This framework contains a stream processing module that captures communication from drones, including information related to intrusion detection. Such information is then sent to two RNN modules for data analysis and training for intrusion detection purposes.

D. PRIVACY PRESERVATION SCHEMES

Nowadays, camera-equipped drones can be used for surveillance and on-air photography in various applications. In contrast to video devices, personal drones with high mobility can track and trail a person, raising identity and location privacy concerns [76].

1) POLICY-BASED PRIVACY PRESERVATION SCHEMES

Yao *et al.* [77] reported findings from two rounds of online survey of 169 drone controllers and 717 bystanders in the United States on how drone controllers and bystanders viewed technology- or policy-based mechanisms to alleviate privacy concerns. It is revealed that owner registration and automatic face blurring to preserve user privacy received the most favorable responses from controllers and bystanders. The study recommended to use a combination of privacy protection approaches in the context of drone use, highlighting contextual preferences. Beck *et al.* [78] proposed a framework for implementing privacy policies on commercial shipping drones, such as those that might be used by Amazon Prime Air. This type of drones will access different host airspaces, each with potentially different privacy requirements. The proposed framework enforces the policies of these host airspaces with mandatory access controls for guest drones. The authors also described the designation and realization of the framework's policy enforcement mechanism and how policies are specified.

2) TECHNIQUE-BASED PRIVACY PRESERVATION SCHEMES

Chen and Wang [76] initiated an improved security pseudonym to protect the privacy of cloud data in the IoD. The two-level network encoding is designed to allow the stored IoD cloud data to be decoupled from its owner's pseudonym. This method can defeat both external and internal attackers and be implemented on untrusted cloud databases. Experimental results show that the proposed method decreased the processing time by more than 90% and the energy consumption by 10% compared to the hash-based pseudonym.

Lee *et al.* [79] developed a privacy-preserving IoD system based on the state-of-the-art generative adversarial network architecture and deep learning techniques. Delicate modifications are made to only the face of individuals captured by drones such that they still look like human in the revised

TABLE 2. The Comparison of Different Types of Authentication Techniques

Type of Technique	Description	Pros	Cons (or Challenges)
Lightweight Authentication	This authentication technique tends to be cost-efficient in terms of computation and communication.	Low computing and communication costs.	(1) The reduction in cost often results in a reduction in security or operations [57]. (2) A trade-off between security and efficiency is needed [34].
Cryptography-based Authentication	This authentication technique allows users to have real-time access to the collected information protected by the cryptographical key.	Mature techniques (e.g., elliptic curve cryptography) with many formal performance analysis tools and models [46].	(1) Issues of high computational complexity regarding public-key cryptosystems [47]. (2) It is challenging to make cryptography-based authentication systems robust to diverse attacks, especially with public insecure channels in the IoD environment [58].
Biometric-based Authentication	Biometric data can be used to generate keys or act as one of the multiple factors in access control and identity management of the IoD.	(1) Unique to any individual users based on "who you are". (2) Can add an extra layer of security to the IoD [54].	(1) Biometric data collection and processing are needed. (2) Issues of real-time latency and extra costs [54].
Authentication Framework	Such frameworks formulate skeletal structures for authentication in the IoD.	A platform upon which authentication solutions can be built according to the needs [55].	(1) A particular framework cannot meet the demands of different scenarios with different environmental factors, security and privacy requirements. (2) Issues may arise when it is hard to keep standard operating procedures in a specific application scenario [27].

video, but are made anonymous. In this way, the semantic information of the videos is retained even after anonymization. Svaigen *et al.* [80] proposed a method called MixDrones to alter drones' trajectory in addition to their pseudonym, thus protecting drones' location information. The experimental results show that MixDrones delivers better location privacy protection than the existing methods, anonymizes a significant number of drones, and is resistant to de-anonymization attacks.

E. OTHER SCHEMES

Federated learning (FL) can be used to train data locally in drones with only training model parameters shared instead of raw drone data to fog nodes, thus preventing the leakage of network data and protecting drone data privacy during the transmission. Yao and Ansari [80] studied the power control of drones in order to optimize the FL system's security rate under the constraints of drone battery capacity and quality of service (QoS) requirements. The authors formulated the issue to be a nonlinear programming problem and obtained an optimized solution without a high degree of computational intensity. Khan *et al.* [81] proposed an identity-based proxy signature encryption method to address security and privacy risks during data transmission from drones to cloud servers. The proposed method provides support to outsourced decryption and member revocation. Evaluated with formal security analysis techniques, it is shown that the proposed method outperforms its counterparts in terms of computational and communication costs.

VI. CHALLENGES

The goal of IoD security is to improve attack resistance and achieve high efficiency or low costs. Some of the critical challenges facing IoD security-related research are discussed below.

A. CHALLENGES FACING AUTHENTICATION SCHEMES

Based on the comparison and analysis of different authentication techniques in Table 2, we now summarize the challenges that need to be overcome by authentication solutions in the IoD environment. Although lightweight authentication schemes have low computation and communication costs, they are likely to have security shortages or reduced operation functions [57]. Also, a good trade-off between security and efficiency is required in the design of lightweight authentication methods [34]. While cryptography-based authentication techniques show strong security, they are usually of high computational complexity, which is a critical challenge for implementing public-key cryptosystems in certain applications [47]. Despite the advantages of using biometrics (e.g., offering an additional layer of protection to the IoD), biometric-based authentication brings extra operational costs and may cause real-time latency [54]. Authentication frameworks provide a platform for finding authentication solutions based on application scenarios, but a specific framework cannot meet all the requirements of different scenarios in the IoD, as each scenario may have different environmental factors requiring different operating procedures for performing tasks [27].

B. CHALLENGES FACING BLOCKCHAIN-POWERED SCHEMES

1) COMPUTING COSTS OF BLOCKCHAINS

Leveraging blockchains in drone networks provides a promising solution to security and privacy threats to the IoD. However, applying advanced learning technologies like blockchains demands significant computing resources. Since drones typically have finite resources and perform varying tasks, the main challenge is how to engage them in the blockchain process and get access to computing resources. Edge computing is an emerging technology where powerful

edge computing servers can be utilized to alleviate the computational burden, but optimization techniques are required to improve data rates or reduce latency to prevent signal drop during transmission between drones and edge computing servers. Hence, how to integrate edge computing into the IoD is an open research question [82].

2) LATENCY OF BLOCKCHAINS

Writing and reading data on blockchains using smart contracts introduce latency. Although the latency of blockchains is used to ensure the consistency of decentralized blockchain networks, for many IoD applications (e.g., real-time monitoring), the high latency of blockchains is unacceptable, as it leads to limited blockchain capabilities in the IoD. Hence, this limitation should be overcome in future IoD-related extensions [58].

3) INCREASE IN THE SCALE OF BLOCKCHAINS

The scale of a blockchain is concerned with its throughput (e.g, the number of processed transactions per second) and system size (e.g., the number of peers in blockchains). If the scale of a blockchain keeps growing with the IoD, and data keeps increasing, the storage and computational load of the blockchain will become burdensome, thus taking more time for the blockchain to synchronize data and making its operation in the IoD problematic [83].

4) ATTACKS TARGETING BLOCKCHAINS

Due to their highly anti-tampering property, applying blockchains to the IoD has attracted great attention in recent years. However, blockchains themselves are facing vulnerabilities and attack threats [58], such as

- *Majority attacks:* If attackers manage to own a significant portion of IoD networks' computing power, then the consensus protocol can be breached. For example, if attackers possess more than half of the hashing power, they can let blockchains accept illegal blocks [83].
- *DOS attacks:* Blockchain resources (e.g., IoD networks' processing capacity) can be depleted by adversaries through the initiation of collaborative attacks [58], [84].
- *Compromising private keys:* User accounts are compromised if attackers steal the private key of the account [58].

C. BALANCES BETWEEN SECURITY AND LIGHTWEIGHT FEATURES

With the IoD, a large number of drones collect data in a collaborative manner and bring large amounts of unstructured data to cloud servers. Big data clustering and mining techniques are needed to process these data in real time [5]. Without security measures, sensitive data collected by the IoD would be at risk. However, it could be costly to implement security mechanisms in the IoD, such as authentication and blockchain-powered schemes, since they create substantial computational and communication overheads. Smart drones can be used to gather data, but they usually have limited computing capacity, thus causing problems such as weak cryptography and data insecurity [1]. High security levels would mean design complexity and demand more computational load and power consumption, so it is challenging to strike a good balance between sound IoD security and lightweight features [85].

D. PRIVACY-RELATED REGULATION ISSUES

The deployment of drones may pose privacy threats to both individuals and organizations. Drones can collect data from individuals and objects as long as they are within drones' view range. In cases where drones are used for monitoring, privacy breaches are likely to occur [9]. Also, drones used in search scenarios can gather large amounts of personal data. In most cases, targeted individuals have no opportunities to consent to data collection [22]. This weakens privacy control policies. Therefore, authorities should be wary of IoD technologies and make privacy-related regulations/policies in alignment with IoD development.

VII. CONCLUSION AND FUTURE RESEARCH

Due to changing communication criteria and the broad scope of IoD applications, it is nontrivial to secure the IoD. Drones are susceptible to a variety of attacks. In this survey, security issues in the IoD are reviewed, followed by discussions about existing solutions and analysis on challenges facing IoD security. Although many countermeasures and solutions are available, this study focuses on two major techniques, namely authentication and blockchain-powered schemes. Some potential research topics are provided below.

- To mitigate negative impacts on the IoD (e.g., high latency and communicational costs) brought by the increasing scale and size of blockchains, blockchain technologies aiming for high throughput and low latency, such as Directed Acyclic Graph (DAG) [86] and Sharding [87], are promising solutions. To overcome heavy computations and meet IoD network requirements, building blockchains into drones is also an appealing research topic.
- The extra costs due to biometric sensors, biometric feature extraction and matching have hindered the work on applying biometrics authentication to the IoD. However, it is widely acknowledged by research communities that the use of biometrics benefits IoT security [88]; we believe that it is equally effective for IoD security. With cost-effective and advanced biometric sensors integrated into drones plus the lightweight design of feature extraction and matching algorithms for drones, biometric authentication applicable to the IoD will attract more and more attention from researchers and industry professionals.
- It is desirable for new IoD methodologies to offer high security while being cost-efficient. Although it is hard to achieve both at the same time, balancing security

and design complexity (e.g., using lightweight features) is worth attempting. Moreover, mobile edge computing [34] is useful to mitigate the issue. In the IoD, edge devices can be placed between flight zones of drones so that some heavy tasks can be shifted to powerful edge computing servers to reduce the computational load of drones.

REFERENCES

[1] S. H. Alsamhi, O. Ma, M. S. Ansari, and F. A. Almalki, "Survey on collaborative smart drones and Internet of Things for improving smartness of smart cities," *IEEE Access*, vol. 7, pp. 128125–128152, 2019.

[2] G. Choudhary, V. Sharma, T. Gupta, J. Kim, and I. You, "Internet of drones (IOD): Threats, vulnerability, and security perspectives," in *Proc. 3rd Int. Symp. Mobile Internet Secur.*, 2018, pp. 1–13.

[3] C. Lin, D. He, N. Kumar, K.-K. R. Choo, A. Vinel, and X. Huang, "Security and privacy for the internet of drones: Challenges and solutions," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 64–69, Jan. 2018.

[4] L. Abualigah, A. Diabat, P. Sumari, and A. H. Gandomi, "Applications, deployments, and integration of internet of drones (iod): A review," *IEEE Sensors J.*, vol. 21, no. 22, pp. 25532–25546, Nov. 2021.

[5] A. Abdelmaboud, "The internet of drones: Requirements, taxonomy, recent advances, and challenges of research trends," *Sensors*, vol. 21, no. 17, 2021, Art. no. 5718.

[6] P. Boccadoro, D. Striccoli, and L. A. Grieco, "An extensive survey on the internet of drones," *Ad Hoc Netw.*, vol. 122, 2021, Art. no. 102600.

[7] M. Ayamga, S. Akaba, and A. A. Nyaaba, "Multifaceted applicability of drones: A review," *Technological Forecasting Social Change*, vol. 167, 2021, Art. no. 120677.

[8] Y. Zhi, Z. Fu, X. Sun, and J. Yu, "Security and privacy issues of UAV: A survey," *Mobile Netw. Appl.*, vol. 25, no. 1, pp. 95–101, 2020.

[9] A. Fotouhi *et al.*, "Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," *IEEE Commun. Surv. Tuts.*, vol. 21, no. 4, pp. 3417–3442, Oct.–Dec. 2019.

[10] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," *ACM Trans. Cyber- Phys. Syst.*, vol. 1, no. 2, pp. 1–25, 2016.

[11] V. Chamola, P. Kotesh, A. Agarwal, N. Gupta, and M. Guizani, "A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques," *Ad Hoc Netw.*, vol. 111, 2021, Art. no. 102324.

[12] H. P. D. Nguyen and D. D. Nguyen, "Drone application in smart cities: The general overview of security vulnerabilities and countermeasures for data communication," *Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead*, Cham, Switzerland: Springer, pp. 185–210, 2021.

[13] G. S. Ilgi and Y. K. Ever, *Critical Analysis of Security and Privacy Challenges for the Internet of Drones: A Survey*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 207–214.

[14] N. S. Labib, M. R. Brust, G. Danoy, and P. Bouvry, "The rise of drones in Internet of Things: A survey on the evolution, prospects and challenges of unmanned aerial vehicles," *IEEE Access*, vol. 9, pp. 115466–115487, 2021.

[15] V. Puri, A. Nayyar, and L. Raja, "Agriculture drones: A modern breakthrough in precision agriculture," *J. Statist. Manage. Syst.*, vol. 20, no. 4, pp. 507–518, 2017.

[16] U. R. Mogili and B. Deepak, "Review on application of drone systems in precision agriculture," *Procedia Comput. Sci.*, vol. 133, pp. 502–509, 2018.

[17] S. Ahirwar, R. Swarnkar, S. Bhukya, and G. Namwade, "Application of drone in agriculture," *Int. J. Curr. Microbiol. Appl. Sci.*, vol. 8, no. 1, pp. 2500–2505, 2019.

[18] S. E. Kreps and G. P. Wallace, "International law, military effectiveness, and public support for drone strikes," *J. Peace Res.*, vol. 53, no. 6, pp. 830–844, 2016.

[19] G. S. L. K. Chand, M. Lee, and S. Y. Shin, "Drone based wireless mesh network for disaster/military environment," *J. Comput. Commun.*, vol. 6, no. 4, 2018, Art. no. 44.

[20] J. Q. Cui *et al.*, "Drones for cooperative search and rescue in post-disaster situation," in *Proc. IEEE 7th Int. Conf. Cybern. Intell. Syst., IEEE Conf. Robot., Automat. Mechatronics*, 2015, pp. 167–174.

[21] C. V. Tilburg, "First report of using portable unmanned aircraft systems (drones) for search and rescue," *Wilderness Environ. Med.*, vol. 28, no. 2, pp. 116–118, 2017.

[22] S. Mayer, L. Lischke, and P. W. Woźniak, "Drones for search and rescue," in *Proc. 1st Int. Workshop Hum.-Drone Interact.*, 2019.

[23] Y. Karaca *et al.*, "The potential use of unmanned aircraft systems (drones) in mountain search and rescue operations," *Amer. J. Emerg. Med.*, vol. 36, no. 4, pp. 583–588, 2018.

[24] G. Quiroz and S. J. Kim, "A confetti drone: Exploring drone entertainment," in *Proc. IEEE Int. Conf. Consum. Electron.*, 2017, pp. 378–381.

[25] S. J. Kim, Y. Jeong, S. Park, K. Ryu, and G. Oh, *A Survey of Drone Use for Entertainment and AVR (Augmented and Virtual Reality)*. Berlin, Germany: Springer, 2018, pp. 339–352.

[26] J. Scott and C. Scott, "Drone delivery models for healthcare," in *Proc. 50th Hawaii Int. Conf. Syst. Sci.*, 2017, pp. 3297–3304.

[27] M. A. H. Zailani, R. Z. A. R. Sabudin, R. A. Rahman, I. M. Saiboon, A. Ismail, and Z. A. Mahdy, "Drone for medical products transportation in maternal healthcare: A systematic review and framework for future research," *Medicine*, vol. 99, no. 36, 2020, Art. no. e21967.

[28] E. Barmpounakis and N. Geroliminis, "On the new era of urban traffic monitoring with massive drone data: The pneuma large-scale field experiment," *Transp. Res. Part C: Emerg. Technol.*, vol. 111, pp. 50–71, 2020.

[29] C. Christodoulou and P. Kolios, "Optimized tour planning for drone-based urban traffic monitoring," in *Proc. IEEE 91st Veh. Technol. Conf.*, 2020, pp. 1–5.

[30] T. T. Mac, C. Copot, C.-Y. Lin, H. H. Hai, and C. M. Ionescu, "Towards the development of a smart drone police: Illustration in traffic speed monitoring," *J. Phys.: Conf. Ser.*, vol. 1487, no. 1, 2020, Art. no. 012029.

[31] H. Menouar, I. Guvenc, K. Akkaya, A. S. Uluagac, A. Kadri, and A. Tuncer, "UAV-enabled intelligent transportation systems for the smart city: Applications and challenges," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 22–28, Mar. 2017.

[32] J. A. Besada *et al.*, "Drone mission definition and implementation for automated infrastructure inspection using airborne sensors," *Sensors*, vol. 18, no. 4, 2018, Art. no. 1170.

[33] N. I. Jasim, H. Kasim, and M. A. Mahmoud, "Towards the development of smart and sustainable transportation system for foodservice industry: Modelling factors influencing customer's intention to adopt drone food delivery (DFD) services," *Sustainability*, vol. 14, no. 5, 2022, Art. no. 2852.

[34] M. Yahuza *et al.*, "Internet of drones security and privacy issues: Taxonomy and open challenges," *IEEE Access*, vol. 9, pp. 57243–57270, 2021.

[35] M. Wazid, A. K. Das, and J.-H. Lee, "Authentication protocols for the internet of drones: Taxonomy, analysis and future directions," *J. Ambient Intell. Humanized Comput.*, pp. 1–10, 2018. [Online]. Available: https://doi.org/10.1007/s12652-018-1006-x

[36] A. Nayyar, B.-L. Nguyen, and N. G. Nguyen, "The internet of drone things (IoDT): Future envision of smart drones," in *Proc. 1st Int. Conf. Sustain. Technol. Comput. Intell.*, 2020, pp. 563–580.

[37] A. Kumar, R. Krishnamurthi, A. Nayyar, A. K. Luhach, M. S. Khan, and A. Singh, "A novel software-defined drone network (SDDN)-based collision avoidance strategies for on-road traffic monitoring and management," *Veh. Commun.*, vol. 28, 2021, Art. no. 100313.

[38] B. Yu and B. Xiao, "Detecting selective forwarding attacks in wireless sensor networks," in *Proc. 20th IEEE Int. Parallel Distrib. Process. Symp.*, 2006, p. 8.

[39] C. Pu and P. Zhu, "Defending against flooding attacks in the internet of drones environment," in *Proc. IEEE Glob. Commun. Conf.*, 2021, pp. 1–6.

[40] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet Things*, vol. 11, 2020, Art. no. 100218.

[41] Y. Li and C. Pu, "Lightweight digital signature solution to defend micro aerial vehicles against man-in-the-middle attack," in *Proc. IEEE 23rd Int. Conf. Comput. Sci. Eng.*, 2020, pp. 92–97.

[42] V. O. Nyangaresi and N. Petrovic, "Efficient puf based authentication protocol for internet of drones," in *Proc. Int. Telecommun. Conf.*, 2021, pp. 1–4.

[43] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. Rodrigues, "Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3572–3584, Apr. 2019.

[44] V. O. Nyangaresi and M. Morsy, "Towards privacy preservation in internet of drones," in *Proc. IEEE 6th Int. Forum Res. Technol. Soc. Ind.*, 2021, pp. 306–311.

[45] J. Srinivas, A. K. Das, N. Kumar, and J. J. Rodrigues, "Tcalas: Temporal credential-based anonymous lightweight authentication scheme for internet of drones environment," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6903–6916, Jul. 2019.

[46] S. Hussain, S. A. Chaudhry, O. A. Alomari, M. H. Alsharif, M. K. Khan, and N. Kumar, "Amassing the security: An ECC-based authentication scheme for internet of drones," *IEEE Syst. J.*, vol. 15, no. 3, pp. 4431–4438, Sep. 2021.

[47] M. Nikooghadam, H. Amintoosi, S. H. Islam, and M. F. Moghadam, "A provably secure and lightweight authentication scheme for internet of drones for smart city surveillance," *J. Syst. Architecture*, vol. 115, 2021, Art. no. 101955.

[48] N. Zhang, Q. Jiang, L. Li, X. Ma, and J. Ma, "An efficient three-factor remote user authentication protocol based on BPV-FOURQ for internet of drones," *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, pp. 3319–3332, 2021.

[49] Y. Zhang, D. He, L. Li, and B. Chen, "A lightweight authentication and key agreement scheme for internet of drones," *Comput. Commun.*, vol. 154, pp. 455–464, 2020.

[50] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and accuracy of fingerprint-based biometrics: A review," *Symmetry*, vol. 11, no. 2, 2019, Art. no. 141.

[51] G. Mai, K. Cao, X. Lan, and P. C. Yuen, "Secureface: Face template protection," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 262–277, 2020.

[52] W. Yang, S. Wang, G. Zheng, J. Chaudhry, and C. Valli, "ECB4CI: An enhanced cancelable biometric system for securing critical infrastructures," *J. Supercomputing*, vol. 74, no. 10, pp. 4893–4909, 2018.

[53] W. Yang *et al.*, "A cancelable IRIS- and steganography-based user authentication system for the Internet of Things," *Sensors*, vol. 19, no. 13, 2019, Art. no. 2985.

[54] A. Singandhupe, H. M. La, and D. Feil-Seifer, "Reliable security algorithm for drones using individual characteristics from an EEG signal," *IEEE Access*, vol. 6, pp. 22976–22986, 2018.

[55] Y. Tian, J. Yuan, and H. Song, "Efficient privacy-preserving authentication framework for edge-assisted internet of drones," *J. Inf. Secur. Appl.*, vol. 48, 2019, Art. no. 102354.

[56] Y. K. Ever, "A secure authentication scheme framework for mobile-sinks used in the internet of drones applications," *Comput. Commun.*, vol. 155, pp. 143–149, 2020.

[57] M. S. Faughnan *et al.*, "Risk analysis of unmanned aerial vehicle hijacking and methods of its detection," in *Proc. IEEE Syst. Inf. Eng. Des. Symp.*, 2013, pp. 145–150.

[58] X. Wang *et al.*, "Survey on blockchain for Internet of Things," *Comput. Commun.*, vol. 136, pp. 10–29, 2019.

[59] M. Singh, G. S. Aujla, and R. S. Bali, "A deep learning-based blockchain mechanism for secure internet of drones environment," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4404–4413, Jul. 2021.

[60] B. Bera, D. Chattaraj, and A. K. Das, "Designing secure blockchain-based access control scheme in IoT-enabled internet of drones deployment," *Comput. Commun.*, vol. 153, pp. 229–249, 2020.

[61] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K.-K. R. Choo, "Blockchain-based cross-domain authentication for intelligent 5G-enabled internet of drones," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 6224–6238, Apr. 2022.

[62] B. Bera, S. Saha, A. K. Das, N. Kumar, P. Lorenz, and M. Alazab, "Blockchain-envisioned secure data delivery and collection scheme for 5G-based IoT-enabled internet of drones environment," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 9097–9111, Aug. 2020.

[63] M. Singh, G. S. Aujla, and R. S. Bali, "ODOB: One drone one block-based lightweight blockchain architecture for internet of drones," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops*, 2020, pp. 249–254.

[64] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava, and M. Aledhari, "Enabling drones in the Internet of Things with decentralized blockchain-based security," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6406–6415, Apr. 2021.

[65] M. Wazid, B. Bera, A. K. Das, S. Garg, D. Niyato, and M. S. Hossain, "Secure communication framework for blockchain-based internet of drones-enabled aerial computing deployment," *IEEE Internet Things Mag.*, vol. 4, no. 3, pp. 120–126, Sep. 2021.

[66] R. Gupta, A. Kumari, and S. Tanwar, "Fusion of blockchain and artificial intelligence for secure drone networking underlying 5G communications," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 1, 2021, Art. no. e4176.

[67] G. Yu *et al.*, "Enabling attribute revocation for fine-grained access control in blockchain-IoT systems," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1213–1230, Nov. 2020.

[68] A. Allouch, O. Cheikhrouhou, A. Koubâa, K. Toumi, M. Khalgui, and T. Nguyen Gia, "Utm-chain: Blockchain-based secure unmanned traffic management for internet of drones," *Sensors*, vol. 21, no. 9, 2021, Art. no. 3049.

[69] F. U. Muram and M. A. Javed, "Drone-based risk management of autonomous systems using contracts and blockchain," in *Proc. IEEE Int. Conf. Softw. Analysis, Evol. Reengineering*, 2021, pp. 679–688.

[70] S. Dawaliby, A. Aberkane, and A. Bradai, "Blockchain-based IoT platform for autonomous drone operations management," in *Proc. 2nd ACM MobiCom Workshop Drone Assist. Wireless Commun. 5G Beyond*, 2020, pp. 31–36.

[71] M. S. Kumar, S. Vimal, N. Jhanjhi, S. S. Dhanabalan, and H. A. Alhumyani, "Blockchain based peer to peer communication in autonomous drone operation," *Energy Rep.*, vol. 7, pp. 7925–7939, 2021.

[72] S. Liao, J. Wu, J. Li, A. K. Bashir, and W. Yang, "Securing collaborative environment monitoring in smart cities using blockchain enabled software-defined internet of drones," *IEEE Internet Things Mag.*, vol. 4, no. 1, pp. 12–18, Mar. 2021.

[73] J. Singh and S. Venkatesan, "Blockchain mechanism with byzantine fault tolerance consensus for internet of drones services," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 4, 2021, Art. no. e4235.

[74] S. Perumalla, S. Chatterjee, and A. S. Kumar, "Block chain-based access control and intrusion detection system in IoD," in *Proc. 6th Int. Conf. Commun. Electron. Syst.*, 2021, pp. 511–518.

[75] R. A. Ramadan, A.-H. Emara, M. Al-Sarem, and M. Elhamahmy, "Internet of drones intrusion detection using deep learning," *Electronics*, vol. 10, no. 21, 2021, Art. no. 2633.

[76] Y.-J. Chen and L.-C. Wang, "Privacy protection for internet of drones: A network coding approach," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1719–1730, Apr. 2019.

[77] Y. Yao, H. Xia, Y. Huang, and Y. Wang, "Privacy mechanisms for drones: Perceptions of drone controllers and bystanders," in *Proc. CHI Conf. Hum. Factors Comput. Syst.*, 2017, pp. 6777–6788.

[78] R. R. Beck, A. Vijeev, and V. Ganapathy, "Privaros: A framework for privacy-compliant delivery drones," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2020, pp. 181–194.

[79] H. Lee, M. U. Kim, Y. Kim, H. Lyu, and H. J. Yang, "Development of a privacy-preserving UAV system with deep learning-based face anonymization," *IEEE Access*, vol. 9, pp. 132652–132662, 2021.

[80] A. R. Svaigen, A. Boukerche, L. B. Ruiz, and A. A. Loureiro, "Mix-drones: A mix zones-based location privacy protection mechanism for the internet of drones," in *Proc. 24th Int. ACM Conf. Model., Anal. Simul. Wireless Mobile Syst.*, 2021, pp. 181–188.

[81] M. A. Khan *et al.*, "Securing internet of drones with identity-based proxy signcryption," *IEEE Access*, vol. 9, pp. 89133–89142, 2021.

[82] Z. Chang *et al.*, "Blockchain-empowered drone networks: Architecture, features, and future," *IEEE Netw.*, vol. 35, no. 1, pp. 86–93, Jan./Feb. 2021.

[83] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, 2017.

[84] M. Vasek, M. Thornton, and T. Moore, "Empirical analysis of denial-of-service attacks in the bitcoin ecosystem," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2014, pp. 57–71.

[85] W. Yang, S. Wang, J. Hu, and N. M. Karie, "Multimedia security and privacy protection in the Internet of Things: Research developments and challenges," *Int. J. Multimedia Intell. Secur.*, vol. 4, no. 1, pp. 20–46, 2022.

[86] H. Pervez, M. Muneeb, M. U. Irfan, and I. U. Haq, "A comparative analysis of dag-based blockchain architectures," in *Proc. 12th Int. Conf. Open Source Syst. Technol.*, 2018, pp. 27–34.

[87] G. Yu, X. Wang, K. Yu, W. Ni, J. A. Zhang, and R. P. Liu, "Survey: Sharding in blockchains," *IEEE Access*, vol. 8, pp. 14155–14181, 2020.

[88] W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed, and C. Valli, "Biometrics for internet-of-things security: A review," *Sensors*, vol. 21, no. 18, 2021, Art. no. 6163. [Online]. Available: https://www.mdpi.com/1424-8220/21/18/6163

WENCHENG YANG is currently a Research Fellow with the Security Research Institute, School of Science, Edith Cowan University, Joondalup, WA, Australia. His main research interests include biometric security, biometric recognition, and network security. He has authored a number of papers published in high-ranking journals, e.g., IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, and *Pattern Recognition*.

SONG WANG received the Ph.D. degree from the Department of Electrical and Electronic Engineering, University of Melbourne, Melbourne, VIC, Australia. She is currently a Senior Lecturer with the Department of Engineering, La Trobe University, Melbourne, VIC, Australia. She has authored or coauthored nearly 50 journal papers, many of which appeared in high-ranking journals, such as *IEEE Communications Magazine*, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON INFORMATION FORENSICS, and *Security and Pattern Recognition*. Her research interests include biometric security, blind system identification, and wireless communications.

XUEFEI YIN received the B.S. degree from Liaoning University, Liaoning, China, the M.E. degree from Tianjin University, Tianjin, China, and the Ph.D. degree from the University of New South Wales, Canberra, NSW, Australia. He is currently a Research Associate with the University of New South Wales. His research interests include biometrics, pattern recognition, privacy-preserving, and intrusion detection. He has authored or coauthored articles in top journals, including IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, *ACM Computing Surveys*, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, and IEEE INTERNET OF THINGS JOURNAL.

XU WANG (Member, IEEE) received the B.E. degree in computer science from Beijing Information Science and Technology University, Beijing, China, in 2010, and the dual Ph.D. degree from the University of Technology Sydney, Ultimo, NSW, Australia, in 2020, and the Beijing University of Posts and Telecommunications, Beijing, China, in 2019. He is currently a Lecturer with School of Electrical and Data Engineering, University of Technology Sydney. His main research interests include blockchain, cybersecurity, privacy, and network dynamics.

JIANKUN HU (Senior Member, IEEE) received the Ph.D. degree in engineering from the Harbin Institute of Technology, Harbin, China, in 1993. He is currently a Full Professor with the School of Engineering and IT, University of New South Wales, Canberra, NSW, Australia. He has authored many papers in high-quality conferences and journals, including IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE in his areas of research, which include cyber security, including image processing/forensics and machine learning. He was the recipient of ten ARC (Australian Research Council) Grants. He was with the prestigious Panel of Mathematics, Information and Computing Sciences (MIC), ARC ERA (The Excellence in Research for Australia) Evaluation Committee. He was the Senior Area Editor of IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY.