Privacy Protection for Blockchain-Based Healthcare IoT Systems: A Survey

Minfeng Qi, Ziyuan Wang, Qing-Long Han, *Fellow, IEEE*, Jun Zhang, *Senior Member, IEEE*,
Shiping Chen, *Senior Member, IEEE*, and Yang Xiang, *Fellow, IEEE*

***Abstract*—To enable precision medicine and remote patient monitoring, internet of healthcare things (IoHT) has gained significant interest as a promising technique. With the widespread use of IoHT, nonetheless, privacy infringements such as IoHT data leakage have raised serious public concerns. On the other side, blockchain and distributed ledger technologies have demonstrated great potential for enhancing trustworthiness and privacy protection for IoHT systems. In this survey, a holistic review of existing blockchain-based IoHT systems is conducted to indicate the feasibility of combining blockchain and IoHT in privacy protection. In addition, various types of privacy challenges in IoHT are identified by examining general data protection regulation (GDPR). More importantly, an associated study of cutting-edge privacy-preserving techniques for the identified IoHT privacy challenges is presented. Finally, several challenges in four promising research areas for blockchain-based IoHT systems are pointed out, with the intent of motivating researchers working in these fields to develop possible solutions.**

***Index Terms*—Blockchain, internet of healthcare things (IoHT), privacy-preserving techniques (PPTs).**

I. Introduction

THE rapid population growth has brought enormous pressure on healthcare resources and services. internet of healthcare things (IoHT), a set of inexpensive IoT devices that can be attached to patients' body, is expected to alleviate the stress of the existing healthcare system with higher efficiency and lower cost. It enables precision medicine, continuous remote patient monitoring, real-time alerts, and remote medical assistance [1].

Nevertheless, IoHT currently confronts several obstacles. Primarily, privacy concerns impede the widespread use of IoHT. Users of IoHT often cannot handle their generated data securely. For instance, without patients' agreement, IoHT data can be illegally shared, exploited, and retained, leading to the revelation of sensitive information. Secondly, it is difficult to ensure the integrity of IoHT data end-to-end. During transmission, IoHT data might get contaminated, leading to erroneous or even deadly medical judgments. Due to the centralized system architecture, IoHT systems suffer from the problem of single point of failure (SPoF). If attackers were to target the centralized server, all linked IoHT devices would be at risk of being compromised, and patients wearing IoHT devices would be in grave danger.

Urgently required is a workable solution for ensuring privacy and trustworthiness in a vast array of IoHT applications. Blockchain (a distributed ledger technology) demonstrates the ability to become a crucial component in an intelligent data-driven IoHT system, as depicted in Fig. 1 . The reasons for combining blockchain with IoHT are outlined below.

1) Privacy Enhancement: Using several encryption techniques, such as hash function and asymmetric encryption, blockchain enables robust data encryption to improve privacy. In addition, it offers reliable peer-to-peer communication and additional privacy protection by anonymizing participants' identities.

2) Trustworthiness Support: With the characteristics of immutability and traceability, blockchain ensures that data stored on blockchain cannot be altered by any participants. In addition, as a trusted third party, blockchain provides a consensus mechanism for nodes to perform certificate issuance, authorization, signature verification, etc., thus boosting the trustworthiness of IoHT.

3) Architecture Suitability: The decentralized architecture of blockchain has a natural fit for the distributed IoHT devices. It can mitigate the risk of SPoF and reduce network delays and congestion.

This article attempts to fill in the gaps on three aspects that are inadequately covered in previous studies: i) privacy challenges in IoHT are not well identified; ii) there is a lack of a complete study of blockchain-based IoHT systems; and iii) privacy-preserving solutions based on blockchain for IoHT are not properly explored.

There are a variety of works that discuss different aspects of blockchain, IoHT, and privacy with varing degrees of scope and depth. Blockchain-based IoT solutions are assessed from privacy, security, trustless architectures, and identity management in [2]. The privacy challenges of blockchain in IoT are discussed in [3]−[5]. Besides, various privacy preservation strategies for blockchain-based IoT applications are explored in [6] and [7]. Compared to prior studies, in addition to the review of privacy-preserving techniques suitable for IoHT, a holistic analysis of blockchain-based IoHT systems is per-

Recommended by Associate Editor MengChu Zhou. *(Corresponding author: Qing-Long Han.)*

Citation: M. F. Qi, Z. Y. Wang, Q.-L. Han, J. Zhang, S. P. Chen, and Y. Xiang, "Privacy protection for blockchain-based healthcare iot systems: A survey," *IEEE/CAA J. Autom. Sinica*, 2022, DOI: 10.1109/JAS.2022.106058

M. F. Qi, Z. Y. Wang, Q.-L. Han, J. Zhang, and Y. Xiang are with School of Science, Computing and Engineering Technologies, Swinburne University of Technology, Hawthorn, 3122, Victoria, Australia (e-mail: minfengqi@swin.edu.au; ziyuanwang@swin.edu.au; qhan@swin.edu.au; junzhang@swin.edu.au; yxiang@swin.edu.au).

S. P. Chen is with CSIRO Data61, Sydney, New South Wales, Australia (e-mail: shiping.chen@data61.csiro.au).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JAS.2022.106058

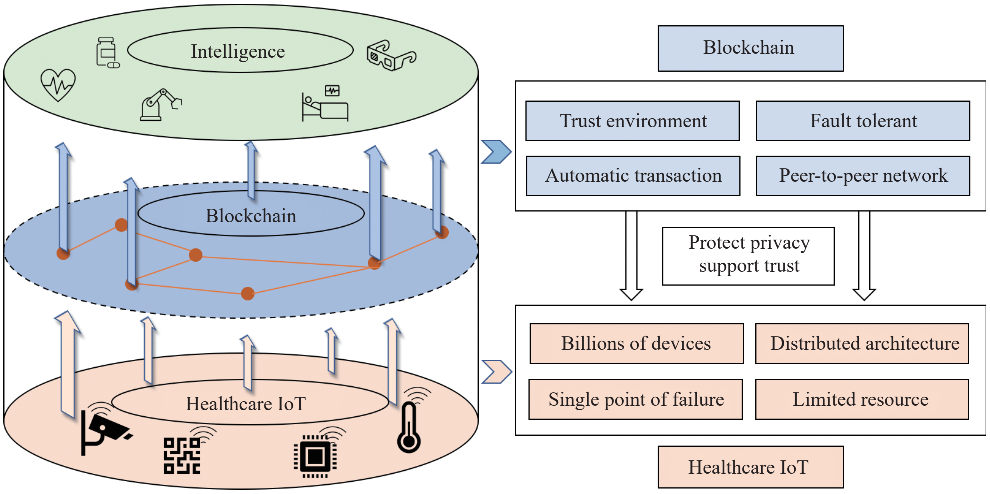

Fig. 1. Motivations for integrating blockchain into IoHT.

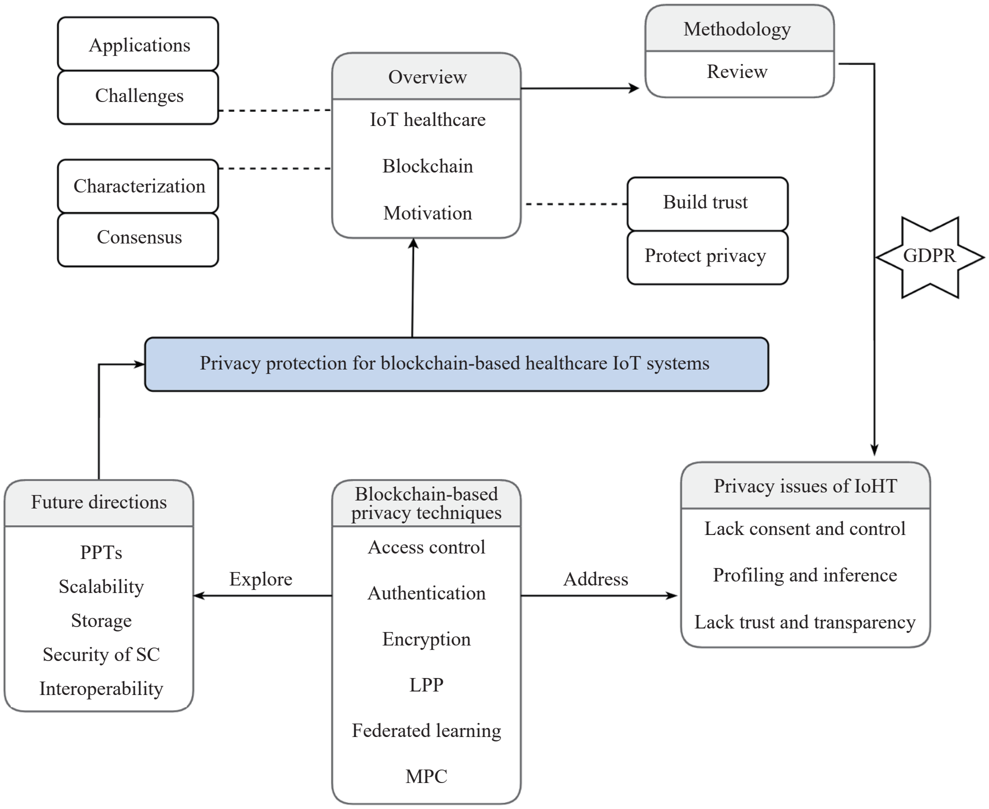

Fig. 2. A roadmap for survey designs.

formed in this article. Moreover, blockchain applications in different IoT scenarios are investigated in [8] and [9]. An assessment is undertaken in [10] of blockchain-based healthcare systems for health information sharing, remote care with IoT, and supply chain. Various applications of blockchain and IoT in healthcare, such as drug traceability and electronic health records, are evaluated in [11]. The advantages of using blockchain in IoT applications are summarized in three categories, including new architecture, data management, and resource management [12]. In contrast to the extent of the studies above, this article only focuses on a distinct area — IoHT. Apart from an in-depth investigation of IoHT privacy problems, this article also reviews the most recent privacy-preserving techniques implemented in blockchain-based IoHT systems in relevant research.

Fig. 2 depicts the survey framework. The following contributions are made in this study:

1) A thorough review of the state-of-the-art blockchain-based IoHT systems is conducted.

2) Existing blockchain-based privacy-preserving techniques adopted in IoHT systems are classified and assessed.

3) The open research challenges of blockchain-based IoHT systems are pointed out, and future directions and potential solutions are discussed accordingly.

The remainder of this survey is structured as follows. In Section II, an overview of IoHT, privacy challenges, and

TABLE I
CLASSIFICATIONS OF PRIVACY ISSUES OF IOHT ACCORDING TO GDPR

Number	Primary privacy issues	GDPR privacy principles
1	Lack of the right to meaningful consent	- Conditions for Consent (Recital 32) - Burden of Proof and Requirements for Consent (Recital 42) - Freely Given Consent (Recital 43) - Right of Rectification and Erasure (Recital 65)
2	Lack of the right to control of data	- Right of Access (Recital 63) - Right to be Forgotten (Recital 66) - Right of Data Portability (Recital 68)
3	Data profiling	- Profiling (Recital 71)
4	Data inference	- Right to Object to Direct Marketing (Recital 70)
5	Lack of trustworthiness	- Identify Verification (Recital 64) - Additional Data for Identification Purposes (Recital 57)
6	Lack of data transparency	- The Principle of Transparency (Recital 58)

blockchain is presented. The state-of-the-art blockchain-based IoHT systems are reviewed in Section III. Blockchain-based privacy-preserving techniques for IoHT are categorized in Section IV. Research directions and challenges are presented in Section V. Finally, the survey is concluded in Section VI.

II. AN UNDERSTANDING OF IOHT, PRIVACY CHALLENGES, AND BLOCKCHAIN

This section introduces readers an overall understanding of IoHT applications, privacy challenges, and blockchain.

A. IoHT Applications Categories

Diverse medical devices and diagnostic sensors can be regarded as smart objects that constitute the core components of IoHT systems [13]. IoHT applications can automatically monitor, track, and report IoHT data, which assists health providers in providing an efficient and accurate diagnosis service. From surveyed papers, the mainstream IoHT applications can be divided into three categories according to different target groups, patients, disabled elderly, and fitness enthusiasts.

1) IoHT Applications for Patients: Patients are the most widely targeted group for IoHT applications. There are four practical types of IoHT applications for patients. *i) Electrocardiogram Monitoring:* Electrocardiogram (ECG) monitoring measures heart rate and basic rhythm, as well as multifaceted arrhythmia and myocardial ischemia [14]. An ECG monitoring system which integrates ECG into a wearable T-shirt is designed in [15], which comprises wireless transmitter and receiver. *ii) Blood Glucose Level Monitoring:* In [16], a blood glucose monitoring system consisting of a blood glucose collector, IoT-based medical acquisition detector, and smartphone is proposed. *iii) Blood Pressure Monitoring:* It contains the blood pressure KIT and the smartphone-enabled KIT [17]. *iv) Oxygen Saturation Monitoring:* Pulse oximetry can monitor the patient's oxygen saturation level in real-time. A wearable pulse oximetry that uses Bluetooth to transmit data from the IoT optimized sensor with low power / low-cost pulse is proposed in [18] and [19].

2) IoHT Applications for the Disabled and Elderly: Considering the complexity of life scenarios, IoHT applications for the disabled and elderly usually embed a variety of IoHT sensors, such as sensors, temperature sensors, and gyroscope sensors. Through real-time monitoring and comprehensive analysis of IoHT data, those applications can realize timely warning and accurate judgment of danger. There are two types of IoHT applications for this target group. *i) WheelChair Management:* A wheelchair management and health monitoring system [20] and a family mobile medical system [21] are designed to monitor the activities and environment of wheelchair users. *ii) Rehabilitation System:* It can help users formulate rehabilitation strategies by automatically analyzing IoHT data [22]. In [23], a stroke rehabilitation system is proposed to facilitate the hand function recovery.

3) IoHT Applications for Fitness Enthusiasts: For fitness enthusiasts, IoHT application is more like a personal trainer, which can help record, analyze, and track changes in physiological indicators during exercise and rest. *i) Wearable Sports Bracelet:* In addition to monitoring heart rate, the wearable sports bracelet can also monitor sleep quality and calorie consumption. *ii) Obesity System:* To help people better manage their weight, an obesity system is designed in [24] to encourage users to actively change their lifestyles by visualizing their IoHT data.

B. Privacy Challenges in IoHT

Despite the fact that IoHT services can increase diagnosis efficiency and accuracy, cut costs, and enhance the user experience, they are facing a difficult development phase due to the confidence crisis. GDPR[1], the most authoritative data protection regulation in the world, reveals a range of privacy problems that are insufficiently resolved in IoHT. One of the contributions made in this article is to map the primary privacy concerns of IoHT with the GDPR privacy principles, and categorize them into six areas (as presented in Table I), including consent and control, profiling and inference, and transparency and trustworthiness.

[1] https://gdpr-info.eu/

1) Consent and Control: Lacking the right to meaningful data consent (Recital 32) is the primary public concern when using IoHT. The issue can be dissected in three aspects. First, an explicit explanation about the purpose of collecting, using, and storing IoHT data is always failed to data owners. Second, consent must be a genuine choice rather than a choice with prerequisites [25]. In some cases, users are not allowed to use IoHT service unless they accept additional conditions. Third, consent cannot be assumed as long-term validity. The one-off "I agree" consent mechanism used in the traditional web service is not suitable for IoHT. Instead, consent requests should be triggered each time the service provider uses IoHT data.

On the other hand, data owners should have the right to control data, as required by Recital 63. Indeed, the lack of control over personal data, as evidenced by the lack of ability to manipulate the data, is a key reason behind the privacy concerns [26]. Most IoHT devices, such as ECGs, cannot provide users with an interactive interface due to resource constraints, making it impossible for users to set privacy preferences for data sharing. In some popular cloud-based IoT applications, while patients can view IoT data from their smartphones, they still have no real control over it because the data stored in a third-party cloud cannot be manipulated by themselves.

2) Profiling and Inference: Profiling (Recital 71) is another privacy issue prevalent in IoHT. It denotes the process of piecing user data together from different dataset sources to recognize users' profile about who they are and what they like. The privacy violation frequently happens to patients who share a portion of their IoHT data with different third parties. Profiling can, therefore, depict patients' complete profiles by combining all data they shared. Some people believe that profiling in some IoHT scenarios is benign [27] since patients can receive better-personalized experience and more accurate diagnoses when caregivers have complete patient profiles. For example, doctors can link various physiological indicators shared by patients to diagnose more accurately. However, for those patients who do not wish to disclose other health information to doctors, profiling brings serious privacy concerns.

Inference (Recital 70) refers to compiling current information about individuals and inferring their interests. The difference between inference and profiling lies in whether there are consequent activities after compiling user IoHT information. For instance, advertisements for heart medications pop up while browsing online due to the leakage of heart rate data.

3) Trustworthiness and Transparency: The valid identity verification of devices and users is considered the prerequisite to establish trustworthiness [28]. Required by Recital 64, it is necessary to perform identity verification before any data manipulation, which is regarded as one of the approaches to protect user privacy. Especially for sensitive health data, building trustworthiness is indispensable. However, due to the resource constraints, it is unrealistic for many IoHT devices to perform classical identity verification operations, resulting in the crash of trustworthiness between patients and devices. In real-world scenarios, patients use a "rogue" IoHT device or share their IoHT data without establishing trustworthiness, which could cause privacy leakage.

The transparency of data is emphasized in Recital 58. The challenge of transparency in IoHT lies in three aspects. First, it is difficult for patients to realize that their data is being silently collected by IoHT devices that are not easily detectable [29]. Some IoHT devices do not provide patients with options to opt out of data collection. Second, for most IoHT devices, due to the lack of hardware such as screens and keyboards for user interaction, they cannot provide patients with clear privacy policies regarding data collecting or sharing. Third, it is difficult for patients to access or erase personal data collected by IoHT devices while ensuring that privacy is not compromised. For example, many patients share an IoHT device where all patients information is recorded. Since the device lacks authorization functions, patients can easily obtain personal information about other patients from the device.

C. Blockchain Technology

Blockchain technology, first proposed in 2009, has become one of the hottest cutting-edge technologies in academia and industry. Encryption, decentralized peer-to-peer (P2P) networks, and consensus protocols are a few examples of the technologies that comprise blockchain technology. This section summarizes blockchain characteristics and compares several consensus mechanisms for IoHT.

1) Features of Blockchain:

i) Decentralization and transparency: Blockchain is a distributed ledger that is jointly maintained (e.g., validate and record) by decentralized parties in a P2P network. Each participant is able to access data on the local ledger copy, which ensures the transparency of blockchain.

ii) Security and anonymity: Security of blockchain is ensured by the consensus protocol that refers to the process of validating transactions by all or several selected members in the blockchain network. In addition, encryption algorithms add extra security to blockchain, and the anonymous address derived from the user's public key realizes the anonymity of blockchain.

iii) Immutability and traceability: Blockchain is a chain comprising consecutively linked blocks. Each generated block points to the previous block by including the hash value of the previous block. Besides that, the block header includes a Merkle tree root hash of all transactions and a timestamp. In this way, blockchain data achieve immutability and traceability.

2) Suitable Consensus Protocols for IoHT: The process of validating transactions broadcasting on the decentralized network is known as consensus protocols. By pre-establishing a rule recognized by all participants, the consensus protocol contributes to building trustworthiness in an untrusted transaction environment. Known as the most classic consensus protocol, proof of work (PoW) [30], has problems of high energy consumption and low consensus efficiency. In the last decade, a variety of innovative consensus protocols, such as proof of activity (PoA) [31] and Performance-optimized consensus mechanism based on node classification [32], have been constantly proposed. Each protocol has its pros and cons, but ultimately, they all strike a balance between decentralization and efficiency.

IoHT applications require a consensus protocol with high throughput and low computing consumption. This work conducts a comparative analysis of ten mainstream consensus protocols (summarized in Table II), and concludes that PBFT [33], DAG [34], and SCP [35] are good candidatures for IoHT. DAG is liklier to be the best choice because of its high degree of decentralization, scalability and concurrent transaction processing, although it may have some security issues such as uncontrollable confirmation times.

TABLE II
COMPARISON OF CONSENSUS ALGORITHMS FOR IOHT

Algorithms	Advantages	Disadvantages	Examples	Suitabiltiy
PoW	High decentre	Low speed	- Bitcoin - Ethereum 1.0	×
PoS	Energy-saving	Nothing at stake	- Ethereum 2.0 - PeerCoin	×
DPoS	Cost-saving	Low decentre	- BitShares - EOS	×
PBFT	Fast speed	Low scalablitity	- Fabric - Stellar	*
PoA	High scalability	High energy cost	- Decred - Espers	×
PoB	Energy-saving	Low scalability	- Slimcoin - SLM	×
PoC	Cost-saving	Low adoption rate	- Burstcoin - BHD	×
PoET	Low cost	Low decentre	- Sawtooth	×
DAG	High scalability	Security issues	- IoTA - Byteball	√
SCP	Low delay	Security issues	- Stellar	*

× denotes suitable, √ denotes not suitable, and * denotes suggested.

III. BLOCKCHAIN-BASED HEALTHCARE IOT SYSTEMS

Aware of the benefits that blockchain can bring to IoHT, this survey is keen to explore current research utilizing both technologies. Several research questions are proposed below: 1) what are the popular architectures in the cutting-edge blockchain-based IoHT systems; 2) what is the role of blockchain in the IoHT system; and 3) what are the privacy-preserving techniques adopted. To answer the aforementioned questions, 38 peer-reviewed papers on blockchain-based IoHT systems are finally screened from databases such as ACM digital library, IEEE Xplore digital library, ScienceDirect, etc. We evaluated those papers from three perspectives, motivations, design features, and evaluation metrics. Finally, we divided the reviewed papers into three groups based on motivations.

A. Address Resource-Constrained Issues

Both IoHT devices and blockchain confront with resource-constrained issues, so related research can be roughly divided into two groups to solve the problems of both sides.

In the light of the computational power-constrained problems of IoHT devices, a privacy-preserving ring signature scheme and a lightweight double encryption scheme (ARX ciphers and public encryption) are adopted to supplant PoW consensus consuming huge computing resources in [36] and [37], respectively. In addition, lightweight blockchain consensus mechanisms are developed in [38] and [39] to reduce the computing stress of remote patient monitoring systems. Besides, an IoHT system model that using an improved simplified payment verification (ISPV) enables power-constrained IoHT devices to join the network as a full node [40]. A lightweight architecture consisting of two blockchain networks is proposed in [41] to reduce the energy consumption of IoHT devices. Similarly, a local blockchain and a global blockchain using Hyperledger Fabric are developed to achieve better storage handling due to the limited storage capacity of IoHT sensors and gateways [42].

In terms of storage-constrained issues of blockchain, on-chain and off-chain storage is a popular method, especially in the field of IoHT. The off-chain storage strategy can prevent blockchain from being colossal and greatly reduce the expense of data storage. A peer-to-peer distributed file system to store the vast amounts of IoHT data is adopted in [43]. IPFS is used to store the original patient health data, while blockchain is used to store only data hash mapped to IPFS [44]. Moreover, to reduce the size of blockchain and save amount of coins for transaction efficiently, a processing mechanism is proposed in [45] to store the medical device information sparingly in accordance with health situation of patients. To solve the problem of long time confirmation while storing real-time IoHT data on blockchain, a modified proof of authority (PoA) protocol is integrated into the proposed system in [46] due to its high transaction speed.

Overall, current studies on addressing resource-constrained issues of IoHT devices and blockchain demonstrates a variety of research directions. Some work is devoted to reducing the computational consumption of IoHT devices by proposing lightweight mechanisms of encryption, consensus, and transaction. Other work targeting addressing storage-constrained issues of blockchain takes strategies such as adopting on-chain and off-chain storage, reducing the size of IoHT data, and improving storage efficiency. Nonetheless, more effort is required as the majority of studies are still in their infancy and the proposed approaches are not applicable to real world because of more complex medical situations. Table III summarizes the studies introduced above.

B. Facilitate Data Sharing

Blockchain has the inherent advantage of ensuring integrity and trustworthiness in data sharing. Therefore, preventing patients' medical data from being tampered with during transmission is one of the significant motivations for integrating blockchain into IoHT systems. In [47], a tree-based data batching method and a user membership service protocol are used to manage data integrity and user identity, respectively. Blockchain plays the role of an immutable database that stores access control policies and other transaction activities. A service blockchain that can be used as an antitamper for recording the interaction between the s-healthcare provider and the

TABLE III
REVIEW OF BLOCKCHAIN-BASED IoHT SYSTEMS–FOR RESOURCE CONSTRAINED ISSUES

Category	Ref.	Design features	Evaluation metrics
For computational power-constrained issues of IoHT devices	[36]	Privacy-preserving ring signature scheme	Security evaluation
	[37]	A lightweight double encryption scheme	Security and efficiency analysis
	[38]	Three layers: BASN, Fog, and Cloud	Energy consumption and block generation time analysis
	[39]	Three layers architecture and 5G technology	Security evaluation and energy consumption analysis
	[40]	Incorporate the SPV technology into Bitcoin	Confirmation time and SPV response analysis
	[41]	Two blockchain networks, local chain and global chain	System performance and scalability analysis
	[42]	Dual blockchain architecture	Security evaluation
For storage-constrained issues of blockchain	[43]	Adopt IPFS as an off-chain database	System implementation process analysis
	[44]	Combine off-chain and on-chain	Latency and throughput
	[45]	Four smart contracts: PRSC, DRSC, ASC, and MPSC	Parallel comparison in confidentiality and availability
	[46]	Apply Proof of Authority	Security analysis for framework

patient is designed in SmartMedChain [48]. Two blockchains, i.e., medical devices blockchain and consultation blockchain, are designed to record the information of IoHT devices and the history of patient records, respectively [49]. Additionally, the swarm exchange paradigm is used in a private blockchain to transfer patients' EHR data to medical doctors, which ensures the integrity of shared data. The paradigm can also facilitate EHR data transmission by associating security services with EHR blocks [50]. A trusted third party auditor (TTPA) mechanism to validate the integrity of shared EMR is proposed in [51]. To build trustworthiness among data-sharing participants, storing data on blockchain and sharing data in a transparent manner is adopted in [52] and [53]. In addition, dual network architecture and session-based data sharing scheme are proposed to enhance trustworthiness in [54]. Dual network architecture is established by combining the digest chain and structured P2P network, and blockchain is adopted to record the data generation event and the session creation event. Moreover, four data layers architecture and two-type of block structure are presented in [55] to improve the reliability of EMR.

Some studies facilitate IoHT data sharing by improving the communication efficiency of blockchain. Multiple communication protocols such as HTTP(S), MQ telemetry transport (MQTT), and constrained application protocol (CoAP) are implemented in the BlockIoT to support all medical devices [56]. An IoHT-to-blockchain protocol mechanism consisting of five elements is designed in [57]. The API gateway plays a critical role in improving blockchain communication, which acts as a client to invoke smart contracts.

To facilitate the management of IoHT data during transmission, an Ethereum-based RMP system that deploys tiered smart contracts, is proposed in [58]. Each sub-contract can be modularized for each patient while all sub-contracts are inherited from the same initial contract. In addition, PoA is adopted in [59]. Blockchain is divided into several clusters comprising a number of nodes, where one node elected as a cluster head is responsible for maintaining patients and IoHT device lists and participate in blockchain events. In [60], a seamless data flow on the top of blockchain is created to manage data between various entities such as government agencies, e-healthcare providers, and patients.

Overall, as summarized in Table IV, there are a number of articles employing blockchain in IoHT systems to facilitate data sharing. Essentially, some studies are devoted to ensuring the integrity and trustworthiness of IoHT data, while others work on improving communication and data management efficiency during data transmission by leveraging blockchain. In most of the above articles, blockchain is commonly used as a distributed database for storing and querying IoT data, while security issues are barely discussed in data sharing.

C. Enhance Privacy Protection

Leveraging blockchain to protect privacy of IoHT data is another research motivation. Some work utilize blockchain to realize the fine-grained access control. A data fine-grained access control and data usage auditing measures are implemented based on smart contracts in [61]. A decentralized control access mechanism is developed in [62], which ensures that IoHT data can be accessed only by any legitimate person with the consent of the patients. In addition, to preserve the privacy of diabetics who use IoHT to monitor their level of diabetes, a blockchain-based diabetes self-management platform is developed to allow only designated doctors to access IoHT data [63]. Channels are created for the use of smart contracts in [64]. Group privacy is ensured by channels, and only members of that group can see transactions performed on channels. Dual-chain architecture is proposed in [65] to realize the control access over the IoHT data. Data chain stores patients' healthcare data and access control chain stores the patient's defined access policies. The latter ensures that the data owner's access policies will remain unaltered, and access to the patient's data will be controlled as expected. Similarly, multiple blockchains are designed for strengthen access control over data in [66]. Global blockchain (GBC) is used for collaboration of all the hospitals, and other blockchains (RBC) are specific to the regions of the patients for problems that require less interaction of doctors.

Using encryption of blockchain to provide privacy protection is also adopted in many works. A permissioned

TABLE IV
REVIEW OF BLOCKCHAIN-BASED IOHT SYSTEMS–FOR DATA SHARING

Category	Ref.	Design features	Evaluation metrics
For integrity and trustworthiness	[47]	Tree-based data processing and batching	Response time and SPV response analysis
	[48]	Service blockchain and Privacy Agreement Management Scheme	Transaction latency and uploading time
	[49]	Device blockchain and Consultation blockchain	Data processing sequence analysis
	[50]	Swarm exchange paradigm	Swarm loading, exchange, and listening time
	[51]	Design a three data management module	Scalability, interoperability, and cost-effetiveness analysis
	[52]	IoT application service and blockchain networks	System performance analysis
	[53]	Four-layers data preserving architecture	Vulnerability analysis and latency evaluation
	[54]	Session-based data sharing scheme	Communication and storage overhead evaluation
	[55]	Validating the security through algorithms	Storage of block analysis
For communication	[56]	API component and multiple communication protocols	System performance and data communication analysis
	[57]	IoHT-to-blockchain protocol	Data synchronization and write latency testing
For data management	[58]	Two smart contracts: main contract and specific contract	Security analysis compared to traditional systems
	[59]	Adopt PoA in the overlay network	Transaction process analysis
	[60]	Three-subsystem architecture	System performance analysis

blockchain-based IoHT platform named MediBchain [67] is proposed to protect patient privacy. A smart contract is deployed to convert the block number to the hash value, which protects the health data from retrieving by adversaries. Similarly, in [68], EMR is recorded in the form of hash value on blockchain. Any changes to the data are visible to all entities in the network, thus ensuring privacy. Moreover, a large-scale health data privacy-preserving scheme based on blockchain technology is proposed in [69], whereby IoHT data are encrypted to conduct fine-grained access control. Patients can effectively revoke or add authorized doctors for privacy preservation. In addition, a novel encryption protocol applied to the multi-tier blockchain framework [70] is designed to assist patients in anonymously accessing and updating their sensitive health records. Besides the improvement in the encryption protocol, a sound authentication mechanism is implemented to further protect privacy.

Authentication is considered an efficient method to limit unauthorized access. Some studies implement authentication schemes based on blockchain to protect patients' privacy. In [71], a Hyperledger's certificate-based identity solution is proposed to tackle the privacy issue of IoHT. A context and trust-based driven Fuzzy logic is also used to provide an adaptive security mechanisms for IoHT devices. Directed acyclic graphs (DAG) is used in both a public blockchain and a private blockchain to provide authentication for IoHT [72]. Additionally, two types of blockchain ledgers are designed to separately store the hash of patient health data and access policy in [73]. The use of blockchain prevents EMR from exposing to unauthorized miners, thereby avoiding leakage of patient privacy. Similarly, two loosely-coupled blockchains are constructed to manage different types of healthcare data, and on-chain verification is designed to satisfy the privacy requirements for authentication [74].

Overall, encryption, access control, and authentication are the classical approaches adopted in the above studies to protect privacy of IoHT data. In acknowledging the advantage of using smart contracts to control data, it is necessary to discuss security issues in the designed framework. For example, distinct levels of complexity of permissions need to be considered when implementing smart contracts. Table V presents the summary of relevant studies in terms of design features and evaluation metrics.

IV. BLOCKCHAIN-APPLIED PRIVACY PROTECTION TECHNIQUES (PPTS) FOR IOHT

Privacy protection, as one of the classic research topics, has been studied in the past decades. Various privacy-preserving techniques, such as encryption, anonymization, and randomization, have been developed to a fairly mature stage. However, the emergence of IoHT presents new challenges to those traditional techniques due to the distinctive features of IoHT (e.g., distributed and resource-constrained hardware). In this article, 45 papers pertinent to blockchain-based privacy protection approaches are filtered out from existing works through a thorough review and justification. Fig. 3 depicts six categories of privacy enhancement techniques based on blockchain.

A. Blockchain-Based Authentication Techniques

Conventional authentication refers to the process of confirming the identity of objects via a centralized server [75]. It enhances the trustworthiness and transparency of IoHT by preventing unauthenticated devices or users from accessing information. Different from the traditional technique, the blockchain-based authentication technique refers to the method to authenticate users or devices through blockchains, which further enhances privacy by avoiding the risk of SPoF [76]. Table VI presents different types of authentication approaches integrating the blockchain architecture.

Studying the authentication of IoHT devices in different wireless sensor network (WSN) is one of the research directions in privacy preservation. WSN is divided into several sub-networks in the blockchain-based multi-WSN authentica-

TABLE V
REVIEW OF BLOCKCHAIN-BASED IOHT SYSTEMS–FOR PRIVACY PROTECTION

Category	Ref.	Design features	Evaluation metrics
Access control	[61]	GhostDag for fine-grained access control	Security and scalability analysis
	[62]	Public chain and private chain	System performance analysis
	[63]	MQTT Protocol and REST API	Consumption energy and response time analysis
	[64]	Channel created for group privacy	Consumption energy and response time analysis
	[65]	Data chain and access control chain	Security analysis and chains performance
	[66]	Multiple chains: GBC and RBCs	System performance analysis
Encryption	[67]	Deploy a smart contract to hash block numbers	Protocol analysis
	[68]	EMR is recorded in the form of hash value	Product drop ratio and authentication delay evaluation
	[69]	Public chain and consortium chain	Capacity of block, processing time, and computation cost evaluation
	[70]	A PBE-DA encryption protocol	Processing times evaluation
Authentication	[71]	federated learning based authentication protocol	Security and functional analysis
	[72]	EMR-chain and PHD-chain	Fairness and throughput evaluation compared with the other two algorithms
	[73]	Two-types ledgers to protect privacy	Security and privacy analysis
	[74]	Enhanced Proof of Work and deep learning	Data storage ratio and Data transportation comparison

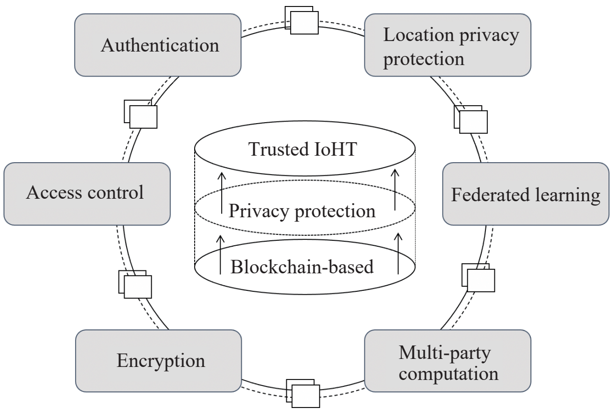

Fig. 3. An overview of blockchain-applied privacy-preserving techniques for IoHT.

tion scheme [77], each of which consists of three types of nodes. The novelty of the scheme lies in the hybrid blockchain model that contains two types of blockchain: public and private blockchain. The former is used to register and authenticate cluster head nodes in different sub-WSNs, and the latter is used to register and authenticate ordinary nodes (IoT devices) in a single sub-WSN. Through this scheme, ordinary nodes can achieve authentication with ordinary nodes in other sub-WSN. Moreover, a migration authentication mechanism based on blockchain is proposed in [78]. A personal area network coordinator (PANC) is designed in each WSN. The authentication logic in their mechanism is as follows. When an IoT device named a1 is authenticated by a PANC A, A sends the transaction to blockchain. If a1 is migrated to a cluster managed by PANC B, then B only needs to send a call function to blockchain to check whether or not a1 is authenticated. In this case, blockchain will return a message to inform B that a1 is authenticated by A. Then, B can use the symmetric keys received from A to communicate with a1.

Mutual authentication between the object device (data owner) and the subject device (data requester) is also studied. A distributed mutual authentication protocol for IoHT devices is presented in [79]. The premise of mutual authentication in the protocol is that IoHT devices must first be registered on the blockchain. The registered device can obtain a unique transaction ID. During the authentication process, Device A sends its ID to Device B, and Device B uses the ID to authenticate Device A through the blockchain, and vice versa. Similarly, in [80], IoHT devices need to be first registered on blockchain where data such as the device's ID and the public key are stored. The difference lies in the authentication process. Device B first searches the public key of Device A in the local blockchain ledger. If it cannot find the public key, it continues to search in the consensus nodes where Device A is registered. The drawback of the mechanism is that it ignores the storage constraints of IoHT devices since each of them needs to synchronize the full blockchain ledger to the local site.

Some authentication mechanisms are built on the blockchain-based edge, where each blockchain edge node plays the role of a middleman connecting IoT devices in different WSN to the blockchain network. The distributed three-layer authentication system proposed in [81], [82] ensures that each IoT device joining the network is authenticated. Blockchain is used to store authentication data and activity logs. In the edge layer, blockchain edge nodes perform the naming solution and provide edge authentication service. Similarly, the single Ethereum smart contract used to register and de-register IoHT devices and fog nodes is the core component of the fog-based authentication mechanism [83]. Through the smart contract, all functions such as registration and authentication can be managed in a manner of decentralization. Moreover, a gateway node-based idea is presented in [84], whereas addressing the resource-constrained issues of IoHT is the main focus.

Blockchain-based authentication mechanisms using tokens or wallets are observed in some other papers. A coin-based distributed mechanism for authenticating IoT devices, and an

TABLE VI
BLOCKCHAIN-BASED AUTHENTICATION TECHNIQUES FOR IOHT

Ref.	Authentication type	Blockchain platform	Evaluation metrics
[77]	Multi-WSN based	Not Mentioned	Security and Effi-ciency Analysis
[78]	Multi-WSN based	Ethereum	Transaction Time and Power Consumption
[79]	Mutual based	Ethereum	Authentication Time Analysis
[80]	Mutual based	Hyperledger Fabric	Security and Per-formance Analysis
[81]	Edge based	Hyperledger Fabric	Communication and storage overhead, and scalability evaluation
[82]	Edge based	Ethereum	Costs, Average De-lay and Hit Ratio Analysis
[83]	Edge based	Ethereum	Security Analysis
[84]	Edge based	Hyperledger Fabric	Security Analysis
[85]	Coin based	Not Mentioned	Scenarios Analysis
[86]	MetaMask based	Ethereum	Security Analysis

TABLE VII
BLOCKCHAIN-BASED ACCESS CONTROL TECHNIQUES FOR IOHT

Ref.	Access control type	Blockchain platform	Evaluation metrics
[89]	Multi-contract based	Ethereum	Gas cost and Time
[90]	Multi-contract based	Ethereum	Cost, Complexity and Security
[91]	Multi-contract based	Hyperledger Fabric	Cost time of con-sensus
[92]	Attribute based	Hyperledger Fabric	Storage and com-putation overhead
[93]	Attribute based	Hyperledger Fabric	Transaction latency
[94]	Organization based	Bitcoin	Functionality pre-defined
[95]	Capability based	Ethereum	Performance and Overhead
[96]	Hub based	Ethereum	Throughput rate and latency
[97]	Hub based	Ethereum	Throughput rate and latency
[98]	Hub based	Ethereum	Conceptual model

authenticated device configuration protocol (ADCP) for establishing connections between IoT devices are designed in [85]. It divides IoT devices into two types. One is a standard device, and another is a hardware authenticator (HA). HA plays a critical role in the system, which is responsible for authenticating standard devices by transferring coins and generating blocks. The novelty of the system lies in the coin-based authentication transaction mechanism, which identifies a standard device that receives a certain amount of coins as an authenticated state. Moreover, an Ethereum-based decentralized authentication protocol used on MetaMask plugin is devised in [86]. It creates an authorization key, access restore key, and recovery seeds to authenticate, manage, and restore accounts separately. However, compared to other works, the downside of the protocol lies in the lack of a detailed authentication process.

B. Blockchain-Based Access Control Techniques

To improve the ability of users to control their data, the access control technique is an indispensable tool that provides fine-grained access permissions to users [88]. The traditional access control techniques such as role-based and attribute-based access control face the risk of SPoF and the challenge of high latency when handling real-time IoHT transactions. As a result, many researchers consider adopting blockchain as a decentralized infrastructure for traditional access control schemes, thus providing a distributed access control system for IoHT. Table VII summarizes the different types of blockchain-based access control approaches.

Implementing access control schemes by employing multiple smart contracts (SC) is a popular approach. A multiple smart contract-based schemes comprising access control contracts (ACCs), a judge contract (JC), and a register contract (RC) is devised in [89]. Each type of smart contract plays a different role in their scheme. ACC provides static and dynamic access rights validation. JC is responsible for judging the misbehavior of the data requester and determining the corresponding penalty. RC manages access control methods by maintaining a lookup table. Moreover, in [90], there are four types of SC, namely IoT Data Access SC, Reputation SC, Aggregator SC, and Oracle SC. Aggregator SC generates access tokens, IoT Data Access SC manages access control and verifies user permissions, and reputation SC calculates the reputation scores of the data requester. A role named Oracle is designed to be registered on Oracle SC and served as gateways to connect IoT devices. Additionally, a multi-contract access control framework is developed in [91]. It consists of three types of SC, policy contract, device contract and access contract. Overall, most SC-based access control schemes in current work specify multiple SCs to perform distinguishable tasks, including device and user registration, policy storage, and access authorization.

TABLE VIII
DECENTRALIZED ENCRYPTION TECHNIQUES FOR IOHT

Ref.	Encryption type	Blockchain platform	Evaluation metrics
[101]	Proxy Re-Encryption based	Ethereum	Impact of proxy re-encryption; Scalability test
[102]	Proxy Re-Encryption based	Private blockchain	Cost of computation and communication
[103]	Proxy Re-Encryption based	Ethereum	Average registration delay
[105]	Attribute based	Public blockchain	Scalability and Key management
[107]	Attribute based	Public blockchain	Security and Data en-cryption time
[108]	Searchable-Attribute based	Consortium blockchain	Storage and Computa-tion
[110]	Searchable-Attribute based	Ethereum	Overhead in execution of smart contract
[111]	Ciphertext-Policy Attribute based	Privarte Ethereum	Security and Computa-tion cost
[112]	Ciphertext-Policy Attribute based	Consortium blockchain	Security performance
[113]	Prefix-Identity based	Hyperledger Fabric	Time cost of committ-ingand fetching data

Applying blockchain into traditional access control techniques such as attributed-based, organization-based, and capability-based techniques is another privacy-preserving approach found in some work. A blockchain-based attribute access control scheme for IoHT is devised in [92]. Attribute authorities are the key entities that are responsible for distributing attributes to IoHT devices. They are selected as nodes to write transactions of attributes into blockchain via Byzantine consensus. Similarly, an attribute-based access control architecture using Hyperledger Fabric is proposed in [93]. The novelty of the access control scheme is that it defines four types of attributes (subject, resource, environment, and action) assigned to different entities by a single smart contract. In addition, a decentralized organization-based access control framework named Fairaccess is proposed in [94]. It uses blockchain as an immutable database to store access policies. The innovation of the scheme lies in the hybrid strategy of choosing different access control methods for the different organizational scenarios. For example, a decentralized approach is used to manage access policies between cooperative organizations, and uses a centralized approach to manage IoHT devices within an organization. Moreover, a decentralized capability-based access control scheme for IoHT is presented in [95]. The domain owner is the core entity responsible for defining access capabilities and creating smart contracts. When an authenticated IoHT device sends an access request, the domain owner will issue a capability token to the requester. The token includes parameters such as virtual ID, delegation right, and access policies.

Hub-based decentralized access control solution to handle the resource-constrained issue of IoHT devices is also studied. A decentralized management-hub model is developed in [96], [97] to perform access control. IoHT devices are grouped into different hubs, and they can only request access via hubs managed by hub managers. The role of managers is to participate in the blockchain network and create a smart contract to define access control operations such as registration, rule addition, and revocation. Based on the work of [97], a dynamic policy generation mechanism is developed in [98] to improve the hub-based access control model by solving the limitation of access control policies and enhancing the data exchange efficiency.

C. Decentralized Encryption Techniques

Cryptographic techniques are considered the most powerful methods to enhance privacy. It can not only ensure the integrity and confidentiality of transaction data, but also protect user identity information from leakage [100]. Concerning the resource-constrained issue of IoHT devices, developing a lightweight encryption scheme is currently a research direction in the field of IoHT privacy preservation. However, most existing encryption techniques are based on the assumption that the centralized authority responsible for managing and issuing secret keys is sufficiently trustable and secure. The consequence could be disastrous if the single authority is compromised. Therefore, many researchers address the issue by combining blockchain with traditional lightweight encryption techniques (shown in Table VIII).

Proxy re-encryption algorithm is adopted in many studies to prevent IoHT data leakage from cloud servers. It can transform the ciphertext encrypted by one public key into the ciphertext encrypted by another public key. A combination of blockchain and a certificate-based proxy re-encryption scheme for IoHT data sharing is proposed in [101]. The scheme consists of seven polynomial-time algorithms. When a request to access data is received, the data owner uses the scheme to generate a re-encrypted cryptographic key and sends the key to the cloud through blockchain. Then, the cloud server uses the key to decrypt and re-encrypt the data. At the same time, it invokes an event on blockchain to notify the requester to use its public key to access the data. During the entire period, the original data is always invisible to the cloud server. Similarly, a blockchain-based proxy re-encryption for EHR sharing is presented in [102]. There are three participants in their scheme, namely the system manager, hospital, and user. The system manager is responsible for generating initial system parameters and computing the conversion key by using the proxy re-encryption algorithm. The private blockchain network where hospitals participate as nodes is in charge of storing EHR. Furthermore, a mechanism that incorporates blockchain and the proxy re-encryption is proposed in [103] to ensure the confidentiality of IoHT data. In the proposed system, the processing node serving as a trusted proxy to execute the re-encryption process is the core entity in the blockchain network. For example, doctor B holding the access policy (H)

TABLE IX
BLOCKCHAIN-BASED LOCATION PRIVACY PROTECTION TECHNIQUES FOR IOHT

Ref.	LPP type	Blockchain platform	Evaluation metrics
[115]	Obfuscation based	Permissioned blockchain	Security and privacy analysis; Average loss of utility
[116]	Obfuscation based	Public and Pri-vate blockchain	Privacy analysis; Task assignment success rate
[117]	Obfuscation based	Public blockchain	Average registration delay
[118]	K-anonymity based	Ethereum	System time evaluation; Average distance and connectivity analysis
[119]	K-anonymity based	Ethereum	Security and privacy analysis; Success Rate and Response Time

requests the share data from doctor A who holds the permitted access policy (H). The critical procedure is that the processing node generates a re-encryption key and transforms the access policy set ($H' \rightarrow H$) for doctor B.

Attribute-based encryption (ABE) allows multiple private keys to be used with a single public key which is constructed from a list of attributes [104]. To achieve fine-grained access control during the verification of IoHT data, a decentralized ABE approach is proposed in [105]. Only blockchain miners who obtain the correct attribute credentials from the attribute authority can decrypt, verify, and re-encrypt transaction data. The advantage of the approach is that it protects the data from leaking by unauthorized miners. Similarly, combining ABE and blockchain to preserve IoHT data privacy is adopted in [106]. The novelty of their scheme lies in a function that enables to judge the source of users' secret keys via attribute authorities, thereby preventing the misuse of secret keys. In addition, in [107], a blockchain-aided searchable attribute-based encryption mechanism is proposed to facilitate data requester to search data on blockchain. Specifically, consensus nodes generate a partial token for each data requester based on their attribute keys, with which the data requester enables to search for data on blockchain. Different from the search method proposed in [107], a searchable encryption scheme that constructs a search EHR index using a complex Boolean expression is devised in [108]. The data requester can search for the index on blockchain through a complex query.

In addition, Ciphertext-policy attribute-based encryption (CP-ABE), a significant branch of ABE, was first proposed in [109]. Due to its one-to-many ciphertext sharing feature, it is considered suitable for access control in a distributed IoHT scenario. In [110], a scheme integrating CP-ABE with a private blockchain to preserve privacy is devised. It strengthens ABE by setting access policies on the encrypted keys encrypted by attributes. Only those requestors whose secret key has met the access policies can decrypt the ciphertext. Similarly, CP-ABE is implemented on the consortium blockchain [111]. The proposed data sharing architecture consists of five layers. The blockchain service layer has two blockchains named record chain and log chain, which are used to store the file storage path of the encrypted file and file access records separately. CP-ABE is used to encrypt the file storage path and the symmetric key when users upload the IoT data file to the system.

Furthermore, combining blockchain with identity-based encryption (IBE) that uses identities instead of public keys to encrypt data [112] is another approach. Prefix encryption is a special flavor of IBE, which is suitable for IoT scenarios since it can use prefix ID instead of full ID for lightweight encryption and sharing data among IoT devices. A decentralized prefix-based encryption scheme that uses the Hyperledger Fabric framework as the back-end for IoHT data sharing is presented in [113]. Blockchain in the scheme is served as a decentralized tamper-proof dataset to store transaction data.

D. Blockchain-Based Location Privacy Protection Techniques

Location-based service (LBS) is one of the most essential functions in IoHT applications, which provides fundamental support for location tracking and navigation. In the recent, the misuse of location data has received increasing attention with the widespread use of IoHT. Protecting location privacy becomes a research hotspot. Traditional location privacy protection (LPP) techniques can be grouped as pseudonyms, location perturbations, and spatial obfuscation [114]. However, those techniques are unable to provide sufficient trustworthiness and security in a dynamical IoHT environment. Meanwhile, they also face the challenge of SPoF. Thus, incorporating blockchain to provide a trusted environment is considered by some researchers as a solution to enhance LPP. Table IX summarizes the current research work.

Combining blockchain with obfuscation methods to establish a decentralized LPP framework is a popular method in IoHT privacy-preserving. A blockchain-based obfuscation mechanism is implemented in [115] to protect the location privacy of IoHT nodes. Blockchain is responsible for the distribution of public and private keys and acts as the trace manager. Besides, the scheme adopts the temporal public key changing technique against colluding attacks between the authority and malicious mobile nodes. An obfuscating path that hides sensitive locations of IoHT nodes is one of the novelties of the design. Moreover, to protect the location privacy of workers in spatial crowdsensing systems, a two-blockchain obfuscation framework that contains a public blockchain and several private blockchains is presented in [116]. The location privacy of workers is protected by uploading their obfuscated working regions instead of exact locations to the public blockchain. Similarly, a longitude and latitude coding method is devised to encode location data by combining the confusion mechanism and blockchain [117], thereby preventing the leakage of nodes' location data in the crowdsensing network.

Other than obfuscation methods, combining K-anonymity and blockchain to protect location privacy is studied. The K-anonymity algorithm is adopted in [118] to perturb attackers, which refers to aggregating multiple locations together to blur the link between the node and its real location. It brings blockchain as a decentralized architecture to store data. In

TABLE X
BLOCKCHAIN-BASED FEDERATED LEARNING TECHNIQUES FOR IOHT

Ref.	FL type	Blockchain platform	Evaluation metrics
[122]	GCN based	Permissioned blockchain	Security analysis; Model ac-curacy and running time evaluation
[123]	CNN based	Consortium blockchain	Security and privacy analy-sis; Test accuracy and train-ning time evaluation
[124]	CNN based	Public blockchain	Convergence and efficiency evaluation; Blockchain eval-uation
[125]	DRL based	Permissioned blockchain and DAG	Accuracy and loss evalua-tion; Cumulative time cost
[126]	CN based	Permissioned blockchain	Over utility analysis; Aver-age loss and learning accu-racy evaluation

GCN denotes Graphic Convolutional Network, CNN denotes Convolutional Neural Networks, DRL denotes Deep Reinforcement Learning, and CN denotes Capsule Network.

addition, a multiple private blockchain-based LPP scheme is proposed in [119]. The K-anonymity principle is adopted to obfuscate the user's real location, thereby enhancing privacy. Blockchain supplants the traditional third-party anonymizing servers to store transactions in a distributed manner.

E. Blockchain-Based Federated Learning Techniques

Federated learning (FL) [120] is an emerging distributed machine learning technique. Each data owner uses a local dataset to train a local model and contributes to a global machine learning model by uploading parameter updates. FL plays a role in privacy protection because it only shares local parameter updates instead of sharing the raw data to a centralized server. FL is regarded as a promising approach for IoHT. On the one hand, it enables sensitive health IoT data to be preserved locally, enhancing the ability of data control. On the other hand, it facilitates data sharing without exposing the original data to others.

However, centralized FL faces several problems that can undermine the security and trustworthiness of the whole system [121]. *1) SPoF:* The FL aggregator (central server) is not always reliable. When the centralized aggregator is breached, the entire FL system will collapse; *2) Malicious Clients and False Data:* It is unrealistic to assume that all clients are trustworthy. The performance of the global model can be significantly impacted by tainted data provided by malicious clients; and *3) The Lack of Proper Incentives:* Due to a lack of proper incentives, the traditional FL model fails to attract or retain a sufficient number of clients to participate in FL training, leading to the failure of FL projects. On the other hand, blockchain demonstrates great potential in resolving the above issues of centralized FL. In a blockchain-based FL system, the model aggregation can be executed by multiple clients, which avoids SPoF. Unreliable clients and data can be filtered out by the verification mechanism of blockchain. Additionally, economic incentives (such as cryptocurrencies) can be used to motivate customers to behave positively. Therefore, as shown in Table X , there are many studies currently exploring the integration of blockchain and FL into IoHT.

A blockchain-based FL data sharing scheme is proposed in [122]. Distributed committee nodes in blockchain replace the role of centralized server in the traditional FL. Another novelty of the paper is that it supplants PoW consensus with a lightweighted federated learning empowered consensus, which minimizes the computational and communication pressure of the committee nodes. Similarly, in [123], blockchain serving as the centralized server is responsible for collecting user-trained models and learning a global FL model for the requester. Considering the limitation of the block size, it uses the off-chain storage technique to store user-trained models on IPFS instead of blockchain. It prevents the risk of user information leakage in FL by employing a differential privacy approach that adds noise to the trained model.

In addition to the integration model of blockchain and FL, a novel hybrid identity mechanism is proposed in [124] to achieve comprehensive identity verification and access control under the decentralized blockchain architecture. Moreover, a double-blockchain based asynchronous FL architecture is devised to solve the problems of low computing efficiency of blockchain and high delay of FL [125]. Permissioned blockchain and local DAG are used to perform synchronous global aggregation and asynchronous local training in FL, respectively. The deep reinforcement learning algorithm (DRL) is adopted to execute asynchronous learning, which considerably improves the efficiency of FL. Furthermore, a hierarchical blockchain-based FL framework that consists of a top-chain (TP) layer and a ground-chain (GC) layer is presented in [126]. It divides the GC layer into several regions, each of which is managed by a GC. The trained-model gradients are firstly aggregated by GCs, and then they are distributed in the TP layer to train a global model. However, the shortcoming of the scheme lies in the high cost of communications between multiple GC blockchains.

Despite the fact that the blockchain-based FL model brings many advantages to IoHT, there are some challenges to its practical adoption that cannot be overlooked. A good blockchain-based FL model in IoHT should consider the trade-offs between high security and privacy, high training efficiency, and low computational cost. For example, since the shared sensitive IoHT data is visible to all nodes across the public blockchain network, there are some risks associated with data security and privacy. In addition, it is challenging to collaborate with millions of IoHT devices to train a model simultaneously. The communication latency, consensus efficiency, and calculated-gradient verification time all need to be considered into training efficiency. Furthermore, due to the limited computational and storage resource of IoHT devices, heavy computational FL tasks can highly affect the number of participated devices, thereby affecting model accuracy.

F. Blockchain-Based Multi-Party Computation Techniques

Secure multi-party computation (MPC) is a key technology

TABLE XI
BLOCKCHAIN-BASED MULTI-PARTY COMPUTING TECHNIQUES FOR IOHT

Ref.	MPC type	Blockchain platform	Evaluation metrics
[128]	Secret sharing based	Public blockchain	Storage and comput-ing efficiency analysis
[129]	Secret sharing based	EOS	Fairness and robust-ness analysis
[130]	Homomorphic based	Public blockchain	Security and privacy analysis
[131]	Homomorphic based	Private Ethereum	Process time and transaction fee eva-luation; Block transactions analysis
[132]	Generic	Private blockchain	Security analysis; Running time

to protect the privacy of multi-party data sharing. A solution is provided to enable multiple distributed participants to compute the desired common result collaboratively while remaining privacy by hiding inputs [127]. However, despite its advantages in protecting privacy, traditional MPC architecture has some limitations such as the risk of SPoF, inefficient computation protocol, and frequent interactions. On the other hand, blockchain regarded as a distributed tamper-proof ledger, provides an incentive mechanism to promote multi-party computing collaboration. Therefore, some studies combine blockchain and MPC to solve the problem of SPoF and provide a more reliable collaborative data-sharing scheme (shown in Table XI).

A decentralized computation platform named Enigma aims to extend the practicability of the public blockchain in privacy-preserving and storage [128]. The secret-sharing based MPC technique is used to keep smart contracts and transactions secret from anyone except transaction-related parties. Moreover, a blockchain and secret-sharing based MPC technique is designed in [129] to enhance fairness and robustness. There are two types of smart contracts used to manage MPC nodes and users, respectively. The reputation of each MPC node recorded in the smart contract is used to assist users in selecting more reliable nodes. Besides, an incentive mechanism designed in the smart contract enables MPC nodes to behave honestly.

A scheme combining homomorphic encryption-based MPC and blockchain to protect privacy in IoHT data sharing is adopted in [130] and [131]. In [130], there are two key entities: aggregator consortium and computing server. The former formed by distributed nodes are used to collect data, perform MPC, and maintain blockchain. The latter is responsible for re-encrypting the ciphertext by using homomorphic encryption before MPC, which ensures the ciphertext not to be disclosed to nodes. In [131], blockchain is served as a medium to transmit homomorphic-encrypted data, queries, and computing results in the form of blockchain transactions. For example, when the leader wants to obtain a computing result from MPC servers, it will send a query to servers via blockchain transactions. In addition, in order to ensure privacy while solving the problem of resource-constraints of IoHT, a lightweight framework (SSP) combing blockchain and MPC is devised in [132]. It uses blockchain to store the transaction data, and uses MPC to distribute access rights and keys to IoHT devices. However, it has not given a detailed discussion about the implementation of MPC in their work.

In summary, MPC and blockchain are technologies with intrinsic support for a decentralized and multi-party environment. MPC provides privacy features absent from some blockchain protocols, while blockchain provides a level playing field where MPC transactions have an immutable representation. As learned from the above works, MPC and blockchain have proved the ability to protect privacy of IoHT data, but its actual potential and widespread usage have yet to be recognized, and exploration of their combination is still in its infancy. There are a number of challenges faced when synergizing, such as the high computing delay and low computing performance with the increase in the number of participants.

V. CHALLENGES AND FUTURE OPPORTUNITIES

While blockchain presents an excellent opportunity to enhance privacy protection and trustworthiness in IoHT, the development of blockchain-based IoHT systems faces several challenges in various aspects. Five potential research areas are depicted in Fig. 4, with the intent of motivating anyone working in these fields to collaborate on possible solutions.

A. Promising PPTs for Blockchain-Based IoHT Systems

In addition to the privacy protection techniques (PPTs) discussed in Section IV, there are some other promising PPTs that can be further explored in blockchain-based IoHT systems. To solve the bottleneck of heavy computational overhead in the asymmetric encryption, Ring signature [133] is considered a potential technique that hides a signer's data in a large collection to confuse the verifier. It only requires low computational power but can provide strong security. Apart from Ring signature, differential privacy [134] is considered another promising approach. The transparent nature of the public blockchain may lead to the privacy leakage of transactions, while differential privacy addresses the problem by adding noise to the transaction data. For example, a differential-privacy based data perturbation mechanism to protect EHR is utilized in [135]. In addition, anonymization can protect patient privacy by hiding the personally identifiable information (PII). For example, bilinear pairing is used in [136] to protect the identity of patients by generating anonymous IDs in the blockchain system. Furthermore, searchable encryption (SE), a cryptographic primitive that enables users to search for keywords in ciphertext, has recently shown great potential in preventing EHR data breaches. Well-designed expressions are utilized to search the index of EHR stored on blockchain, enabling data sharing while preserving privacy of patients' data [137], [138].

While the above PPTs are combined with blockchain in IoHT systems, there are some challenges that need to be

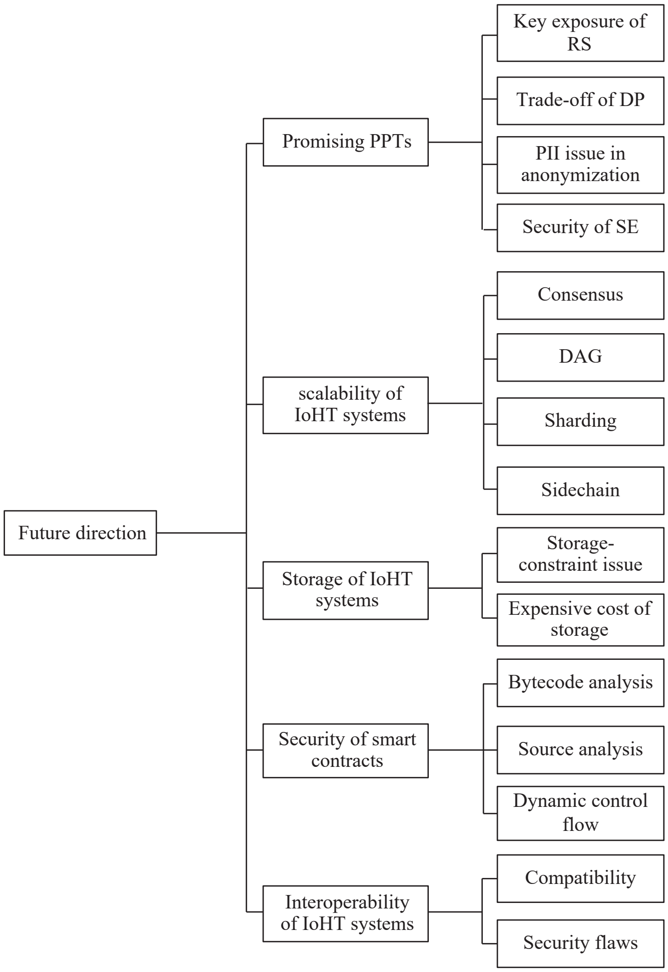

Fig. 4. Research directions for blockchain IoHT systems.

solved accordingly in the future.

- *Key Exposure of Ring Signature:* Ordinary digital signatures have a basic limitation: once a signer's secret key is compromised, all of that signer's signatures become invalid. The problem of key disclosure is particularly severe with a ring signature method. In ring signature methods, if an attacker gains access to a user's secret key, he can not only produce an ordinary digital signature for any document, but also sign any document on behalf of the group. The solutions (such as key security monitoring) to prevent key exposure of ring signature can be a research direction in the future.
- *Trade-Offs Between Privacy and Accuracy in Differential Privacy:* A main challenge of differential privacy lies in the trade-offs between privacy and accuracy (or even other desirable business goals). With more noise added to the original data, the private information is hidden more deeply, but the integrity of the data will be undermined. There will be a need to consider the trade-offs of using differential privacy between enhancing privacy and reducing the loss of data accuracy and integrity.
- *PII Issues in Anonymization:* Firstly, identifying a specific PII is difficult as it varies from case to case. It is impossible to anonymize the whole IoHT dataset in order to prevent disclosure. Secondly, it is inconvenient for data users to extract and process the anonymized data. For future work, defining a general PII and, more importantly, making the original data searchable and securely linked with the anonymized data are both worth exploring.
- *Security of Searchable Encryption:* Although blockchain-based SE avoids index tampering by malicious cloud servers, the security of SE still faces challenges. Inference attacks and file injection attacks are two classical attacks. For the former, hiding the pattern of the returned result is a straightforward solution, but it has a significant impact on the searching performance. In terms of methods to the forward security, efficiency and overhead issues require further trade-offs. On the other hand, while nearly all SE schemes provide provable security, they do not employ a common security model. Developing an uniform security model for SE systems is therefore a direction for future research.

B. Scalability of Blockchain-Based IoHT Systems

Blockchain-based IoHT Systems provide a platform to accurately and timely collect and store critical medical data. However, with the growth of IoHT devices, scalability of blockchain-based IoHT systems become an urgent concern. Scalability determines the maximum number of concurrent transactions that can be processed, which is primarily evaluated by the ratio of transactions per second (TPS) to the number of nodes. In an interactive IoHT real-time scenario, it is unacceptable if the system with a low TPS, as the repercussions might be catastrophic. For instance, the patient can be at risk if the heart-alert message from ECG is not confirmed and recorded on blockchain instantly.

Currently, improving the scalability of blockchain-based IoHT systems is an urgent need in a blockchain-based IoHT system, despite the fact that there are a variety of approaches proposed to tackle this obstacle. Several challenges are pointed out in different research directions.

- Trade-offs between efficiency and decentralization is challenging when developing a consensus protocol for IoHT applications. Existing potential algorithms such as PBFT, SCP, and Casper need to be further tested and verified.
- DAG, as a nonlinear blockchain data structure has great potential for IoHT applications, which can significantly enhance the capability of handling concurrent transactions. However, the security and stability of DAG need to be further studied in the near future.
- Sharding technique can increase the throughput for IoHT applications with parallel processing. Nevertheless, the internal security issues of sharding, as well as the low cross-sharding efficiency caused by cross-shard transactions are worthy of further exploration.
- Side-chain protocols have proven to improve the scalability. Nonetheless, the complexity, fraudulent transfers, and lack of miners are the significant challenges of side-chain protocols.

C. Storage of Blockchain-Based IoHT Systems

With the growing use of EMR, the healthcare industry has struggled to securely store patient, hospital, insurance, and billing records. In a blockchain-based IoHT system, every full node participating in the consensus process is required to host a full copy of blockchain ledger on the local site, resulting in the high requirement for storage capability. Consequently, in the face of a large amount of data, storage-constraint issues and expensive storage costs become significant obstacles.

● *Storage-Constraint Issue:* It is a truth that expanding the storage capacity of IoHT devices is impractical owing to hardware limitations (e.g., size of disk). For IoHT devices, joining the blockchain through a gateway or smartphone with sufficient computational power becomes a feasible alternative. However, gateways or smartphones may not be able to match the storage requirements, since the block size continues to expand at a pace of around 50 gigabytes per year. A potential solution is to use SPV technology, that is, smartphones act as light nodes, and healthcare organizations serve as full nodes in blockchain. Since light nodes only need to store block headers, storage requirements can be greatly reduced. Nonetheless, the way to effectively achieve IoHT data and retrieve data in a tremendous and decentralized database still needs to be explored in the future.

● *Expensive Cost of Storing IoHT Data:* Using Ethereum storage cost as an example. Storing a single non-zero 32-byte word costs 20 gwei (about 0.0000125 ether/byte). In other words, each gigabyte will cost 173 140, far more than the cost of storage in conventional data centers, such as Amazon's S3 (which costs only 75.96 per gigabyte). Adopting an on-chain and off-chain storage approach might be an option for reducing storage costs. The idea of the strategy is to store critical data requiring a high level of integrity on blockchain, while storing medium and low-levels of data off-chain. Choosing a suitable location (such as IPFS) for off-chain data and avoiding centralization are, nevertheless, two challenges associated with the on-chain and off-chain storage methods. Apart from it, designing a data cleaning and detection mechanism used to remove old transactions on blockchain is another promising future direction for IoHT systems to reduce the cost of storage. However, the method conflicts with the intended idea of immutable data on blockchain. The mechanism of reallocating the removed data is also worthy of further study.

D. Security of Smart Contracts in Blockchain-Based IoHT Systems

Smart contract, a critical component in a blockchain-based IoHT system, enables the agreement written in computer programs to be executed automatically, without the intervention of a trusted third party [139]. Smart Contracts in Blockchain-based IoHT Systems can automate most billing and payment procedures, thereby reducing administrative costs and saving time for both patients and medical institutions. Additionally, smart contracts can provide effective basis for later insurance claims and bill management. However, due to the complexity of smart contract modeling, it is difficult to audit the correctness of smart contracts and modify smart contracts after deployment. Several challenges associated with smart contract audits are discussed below.

● *Bytecode Analysis:* Bytecode level analysis requires only the compiled bytecode of the smart contract, which is readily available. How to use these bytecodes to detect security threats has become a research hotspot.

● *Source Code Analysis:* Compared to bytecode level analysis, source code analysis requires the availability of smart contract source code. Although source code analysis contains more information, it also requires high-precision analysis.

● *Dynamic Control Flow:* Although deployed smart contracts are immutable, there is no guarantee that the control flow of smart contracts is immutable. In particular, smart contracts can interact with other contracts (for example, transfer funds to contracts or create new contracts). When developing a contract, the control flow of the smart contract needs to be carefully designed. The interaction of smart contracts leads to an increase in the number of interconnected contracts over time. Therefore, how to predict contract behavior becomes challenging. In addition, most existing methods focus on the detection of potential dynamic control flow problems in programs but ignore the reliability of the execution environment. It is also important to check that the execution environment is reliable in the future.

E. Interoperability of Blockchain-Based IoHT Systems

Blockchain-based IoHT Systems enable large-scale interoperability in medical data exchange, patient tracking, as well as identity verification among healthcare organizations, medical professionals, patients, and insurance institutions. For example, patients typically seek care from multiple physicians and their medical needs may change, medical records can be easily transferable between multiple healthcare facilities while ensuring accuracy. However, the aforementioned situation requires the use of the same blockchain. In fact, different healthcare institutions employ different blockchains, resulting in the transfer of medical data between institutions being extremely challenging.

Blockchain interoperability is highly constrained. Some important aspects of IoHT systems contribute to the difficulty include *a) Data privacy:* It is difficult to determine what information should and should not be transferred based on the level of data privacy offered by various blockchains; *b) Data security:* Because blockchains employ several encryption mechanisms, medical data cannot be transmitted across blockchains in a secure manner; and *c) Lack of standardization:* Because there are no defined blockchain interoperability standards, it can be challenging for developers to determine which standards their blockchains have to conform to.

Despite the fact that constant innovation makes it difficult to categorize blockchain interoperability technologies, the recent research on improving interoperability can be generally divided into three approaches:

● *Public Connectors:* It includes sidechains that connect to the mainchain via a two-way bridge (such as Polygon), notary systems (such as decentralized exchanges), and hash-time locked contracts (such as Bitcoin's Lightning Network). It is important to note that public connectors are the traditional means of enhancing interoperability, notwithstanding their limited capacity to connect to multiple networks.

● *Blockchain Hub:* It includes Layer-0 protocols such as Cosmos and Polkadot. Cosmos creates an interoperable hub of sovereign chains to connect independent blockchains, and Polkadot develops an interchain messaging protocol that relies on using Bridges for communication. Despite of large scalability, blockchain hub needs external infrastructure to communicate with other blockchains.

● *Hybrid Connectors:* It enhances interoperability across public and private blockchains (such as Hyperledger Cactus). However, inadequate backwards compatibility and lack of support for hard forks hinder the development of these solutions.

In general, interoperability technology needs to conform to the system's atomicity, universality, and security requirements. The current interoperability technology has inadequate support for smart contracts of multiple tokens, and the compatibility between multiple chains is still difficult to satisfy. How to better verify the legitimacy and validity of transactions can be one of the future research directions. Additionally, there are security flaws in the interoperability technology, and the trust architecture has significant opportunity for improvement.

VI. Conclusion

With the widespread use of IoHT, privacy has become a serious public concern, while blockchain is regarded as a suitable technique to enhance privacy protection and trustworthiness in IoHT systems. Inspired by the gap in relevant studies, a current view of the state-of-the-art blockchain-based IoHT systems and privacy-preserving techniques suitable for those systems is provided. Specifically, various types of privacy challenges in IoHT by examining the GDPR are firstly identified and summarized. A panoramic view of designed questions is then obtained through extensive comparative analysis. In addition, a thorough review is conducted to identify the cutting-edge privacy-preserving techniques for blockchain-based IoHT systems. Six main categories with respect to those techniques are classified and discussed in depth. Apart from the review of current research, five promising research areas for blockchain-based IoHT systems are pointed out, including PPTs, scalability, storage, security of smart contracts, and interoperability. Challenges and solutions are presented in each area accordingly.

References

[1] M. A. Ferrag, L. Shu, and K. R. Choo, " Fighting COVID-19 and future pandemics with the internet of things: Security and privacy perspectives," *IEEE/CAA J. Autom. Sinica* , vol. 8, no. 9, pp. 1477–1499, 2021.

[2] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, " Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Communications Surveys* & *Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2018.

[3] M. A. Ferrag and L. Shu, "The performance evaluation of blockchain-based security and privacy systems for the internet of things: A tutorial," *IEEE Internet of Things Journal* , vol. 8, no. 24, pp. 17236–17260, 2021.

[4] W. Liang and N. Ji, "Privacy challenges of IoT-based blockchain: A systematic review," *Cluster Computing*, pp. 1–19, 2021.

[5] Z. Iftikhar, Y. Javed, S. Y. A. Zaidi, M. A. Shah, Z. Iqbal Khan, S. Mussadiq, and K. Abbasi, " Privacy preservation in resource-constrained IoT devices using blockchain—A survey," *Electronics*, vol. 10, no. 14, p. 1732, 2021.

[6] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," *Future Generation Computer Systems*, vol. 97, pp. 512–529, 2019.

[7] S. Cha, T. Hsu, Y. Xiang, and K. Yeh, " Privacy enhancing technologies in the internet of things: Perspectives and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2159–2187, 2018.

[8] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, " Blockchain technologies for the internet of things: Research issues and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2188–2204, 2018.

[9] R. Thakore, R. Vaghashiya, C. Patel, and N. Doshi, "Blockchain-based IoT: A survey," *Procedia Computer Science* , vol. 155, pp. 704–709, 2019.

[10] E. J. De Aguiar, B. S. Faiçal, B. Krishnamachari, and J. Ueyama, "A survey of blockchain-based strategies for healthcare," *ACM Computing Surveys* (*CSUR*), vol. 53, no. 2, pp. 1–27, 2020.

[11] Ratta, A. Kaur, S. Sharma, M. Shabaz, and G. Dhiman, "Application of blockchain and internet of things in healthcare and medical sector: Applications, challenges, and future perspectives," *Journal of Food Quality*, vol. 2021, 2021.

[12] H. Hui, X. An, H. Wang, W. Ju, H. Yang, H. Gao, and F. Lin, "Survey on blockchain for internet of things," *Journal of Internet Services and Information Security*, vol. 9, no. 2, pp. 1–30, 2019.

[13] G. Fortino, F. Messina, D. Rosaci, and G. M. Sarnè, "ResIoT: An IoT social framework resilient to malicious activities," *IEEE/CAA J. Autom. Sinica*, vol. 7, no. 5, pp. 1263–1278, 2020.

[14] O. Friha, M. A. Ferrag, L. Shu, L. A. Maglaras, and X. Wang, "Internet of things for the future of smart agriculture: A comprehensive survey of emerging technologies," *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 4, pp. 718–752, 2021.

[15] T. Wu, J. Redouté, and M. Yuce, " A wearable, low-power, real-time ECG monitor for smart T-shirt and IoT healthcare applications," in *Proc. Advances in Body Area Networks I*, 2019, pp. 165–173.

[16] M. M. Ahmadi and G. A. Jullien, " A wireless-implantable microsystem for continuous blood glucose monitoring," *IEEE Trans. Biomedical Circuits and Systems*, vol. 3, no. 3, pp. 169–180, 2009.

[17] L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville, L. M. R. Arbiza, F. Carbone, M. Marotta, and J. J. C. De Santanna, "Internet of things in healthcare: Interoperatibility and security issues," in *Proc. Int. Conf. on Communications*, 2012, pp. 6121–6125.

[18] A. J. Jara, M. A. Zamora-Izquierdo, and A. F. Skarmeta, "Interconnection framework for mhealth and remote monitoring based on the internet of things," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 47–65, 2013.

[19] E. C. Larson, T. Lee, S. Liu, M. Rosenfeld, and S. N. Patel, "Accurate and privacy preserving cough sensing using a low-cost microphone," in *Proc. 13th Int. Conf. Ubiquitous Computing*, 2011, pp. 375–384.

[20] S. S. Nayak, Gupta, A. B. W. Upasana, and A. B. Wani, "Wheel chair with health monitoring system using IoT," *Int. Research Journal of Engineering and Technology* (*IRJET*), vol. 4, no. 5, 2017.

[21] L. Yang, Y. Ge, W. Li, W. Rao, and W. Shen, " A home mobile healthcare system for wheelchair users," in *Proc. 18th Int. Conf. Computer Supported Cooperative Work in Design*, 2014, pp. 609–614.

[22] Y. J. Fan, Y. H. Yin, L. Da Xu, Y. Zeng, and F. Wu, "IoT-based smart rehabilitation system," *IEEE Trans. Industrial Informatics* , vol. 10, no. 2, pp. 1568–1577, 2014.

[23] G. Yang, J. Deng, G. Pang, *et al.*, " An IoT-enabled stroke rehabilitation system based on smart wearable armband and machine learning," *IEEE Journal of Translational Engineering in Health and Medicine*, vol. 6, pp. 1–10, 2018.

[24] C. Dobbins, R. Rawassizadeh, and E. Momeni, " Detecting physical activity within lifelogs towards preventing obesity and aiding ambient assisted living," *Neurocomputing*, vol. 230, pp. 110–132, 2017.

[25] J. Zhang, L. Pan, Q.-L. Han, C. Chen, S. Wen, and Y. Xiang, "Deep learning based attack detection for cyber-physical system cybersecurity: A survey," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 3, pp. 377–391,

2021.

[26] A. D. Kounoudes and G. M. Kapitsaki, "A mapping of IoT user-centric privacy preserving approaches to the gdpr," *Internet of Things*, vol. 11, p. 100179, 2020.

[27] G. Lin, S. Wen, Q.-L. Han, J. Zhang, and Y. Xiang, "Software vulnerability detection using deep neural networks: A survey," *Proc. the IEEE*, vol. 108, no. 10, pp. 1825–1848, 2020.

[28] S. Wachter, "Normative challenges of identification in the internet of things: Privacy, profiling, discrimination, and the gdpr," *Computer Law and Security Review*, vol. 34, no. 3, pp. 436–449, 2018.

[29] Y. Miao, C. Chen, L. Pan, Q.-L. Han, J. Zhang, and Y. Xiang, "Machine learning-based cyber attacks targeting on controlled information: A survey," *ACM Computing Surveys* (*CSUR*) , vol. 54, no. 7, pp. 1–36, 2021.

[30] S. Nakamoto, " Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[31] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake," *ACM SIGMETRICS Performance Evaluation Review*, vol. 42, no. 3, pp. 34–37, 2014.

[32] Zhang, M. Zhou, Q. Zhao, A. Abusorrah, and O. O. Bamasag, "A performance-optimized consensus mechanism for consortium blockchains consisting of trust-varying nodes," *IEEE Trans. Network Science and Engineering*, vol. 8, no. 3, pp. 2147–2159, 2021.

[33] M. Castro, B. Liskov, *et al.*, "Practical byzantine fault tolerance," in *Proc. OsDI*, vol. 99, no. 1999, 1999, pp. 173–186.

[34] F. M. Benčić and I. P. Žarko, " Distributed ledger technology: Blockchain compared to directed acyclic graph," in *Proc. 38th IEEE Int. Conf. Distributed Computing Systems*, 2018, pp. 1569–1570.

[35] D. Mazieres, "The stellar consensus protocol: A federated model for internet-level consensus," *Stellar Development Foundation*, vol. 32, pp. 1–45, 2015.

[36] T. H. Kim and J. Lampkins, "SSP: Self-sovereign privacy for internet of things using blockchain and mpc," in *Proc. IEEE Int. Conf. Blockchain*, 2019, pp. 411–418.

[37] G. Srivastava, J. Crichigno, and S. Dhar, " A light and secure healthcare blockchain for IoT medical devices," in *Proc. Canadian Conf. Electrical and Computer Engineering*, 2019, pp. 1–5.

[38] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A decentralized patient agent controlled blockchain for remote patient monitoring," in *Proc. Int. Conf. Wireless and Mobile Computing, Networking and Communications*, 2019, pp. 1–8.

[39] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Blockchain leveraged decentralized IoT ehealth framework," *Internet of Things*, vol. 9, p. 100159, 2020.

[40] P. Ray, N. Kumar, and D. Dash, " BLWN: Blockchain-based lightweight simplified payment verification in IoT-assisted e-healthcare," *IEEE Systems Journal*, vol. 15, no. 1, pp. 134–145, 2020.

[41] F. P. Oikonomou, G. Mantas, P. Cox, F. Bashashi, F. Gil-Castiñeira, and J. Gonzalez, " A blockchain-based architecture for secure IoT-based health monitoring systems," in *Proc. IEEE 26th Int. Workshop on Computer Aided Modeling and Design of Communication Links and Networks*, 2021, pp. 1–6.

[42] F. P. Oikonomou, J. Ribeiro, G. Mantas, J. M. C. Bastos, and J. Rodriguez, " A hyperledger fabric-based blockchain architecture to secure iot-based health monitoring systems," in*Proc. IEEE Int. Mediterranean Conf. Communications and Networking (MeditCom)*, 2021, pp. 186–190.

[43] K. Azbeg, O. Ouchetto, S. J. Andaloussi, L. Fetjah, and A. Sekkaki, "Blockchain and IoT for security and privacy: A platform for diabetes self-management," in *Proc. 4th IEEE Int. Conf. Cloud Computing Technologies and Applications*, 2018, pp. 1–5.

[44] N. Rifi, E. Rachkidi, N. Agoulmine, and N. C. Taher, "Towards using blockchain technology for ehealth data access management," in *Proc. 4th IEEE Int. Conf. Advances in Biomedical Engineering*, 2017, pp. 1–4.

[45] H. L. Pham, T. H. Tran, and Y. Nakashima, " A secure remote healthcare system for hospital using blockchain smart contract," in *Proc. IEEE Globecom Workshops*, 2018, pp. 1–6.

[46] M. Muofhe, N. Dlodlo, and A. Terzoli, " An internet of things-based system integrated with blockchain to manage patient data in the healthcare sector," in *Proc. Open Innovations*, 2019, pp. 97–103.

[47] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *Proc. 28th IEEE Annu. Int. Symp. Personal, Indoor, and Mobile Radio Communications*, 2017, pp. 1–5.

[48] D. El Majdoubi, H. El Bakkali, and S. Sadki, " Smartmedchain: A blockchain-based privacy-preserving smart healthcare framework," *Journal of Healthcare Engineering*, vol. 2021, 2021.

[49] O. Attia, I. Khoufi, A. Laouiti, and C. Adjih, " An IoT-blockchain architecture based on hyperledger framework for health care monitoring application," in *Proc. 10th IFIP Int. Conf. New Technologies, Mobility and Security*, 2019, pp. 1–5.

[50] P. Ray, B. Chowhan, N. Kumar, and A. Almogren, "BIoTHR: Electronic health record servicing scheme in IoT-blockchain ecosystem," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10857–10872, 2021.

[51] R. Jabbar, N. Fetais, M. Krichen, and K. Barkaoui, "Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity," in *Proc. Int. Conf. Informatics, IoT, and Enabling Technologies*, 2020, pp. 310–317.

[52] S. Jeong, J.-H. Shen, and B. Ahn, " A study on smart healthcare monitoring using IoT based on blockchain," *Wireless Communications and Mobile Computing*, vol. 2021, 2021.

[53] N. Dilawar, M. Rizwan, F. Ahmad, and S. Akram, "Blockchain: Securing internet of medical things (IoMT)," *Int. Journal of Advanced Computer Science and Applications*, vol. 10, no. 1, pp. 82–89, 2019.

[54] P. Ray, B. Chowhan, N. Kumar, and A. Almogren, "BIoTHR: Electronic health record servicing scheme in IoT-blockchain ecosystem," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10857–10872, 2021.

[55] X. Cai, S. Geng, J. Zhang, D. Wu, Z. Cui, W. Zhang, and J. Chen, "A sharding scheme-based many-objective optimization algorithm for enhancing security in blockchain-enabled industrial internet of things," *IEEE Trans. Industrial Informatics*, vol. 17, no. 11, pp. 7650–7658, 2021.

[56] M. Shukla, J. Lin, and O. Seneviratne, "BlockIoT: Blockchain-based health data integration using IoT devices," in *Proc. AMIA Annu. Symp. Proceedings*, vol. 2021, 2021, p. 1119.

[57] A. Bhawiyuga, A. Wardhana, K. Amron, and A. P. Kirana, "Platform for integrating internet of things based smart healthcare system and blockchain network," in *Proc. 6th IEEE NAFOSTED Conf. Information and Computer Science*, 2019, pp. 55–60.

[58] K. N. Griggs, O. Ossipova, C. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *Journal of Medical Systems*, vol. 42, no. 7, pp. 1–7, 2018.

[59] A. D. Dwivedi, L. Malina, P. Dzurenda, and G. Srivastava, "Optimized blockchain model for internet of things based healthcare applications," in *Proc. 42nd IEEE Int. Conf. Telecommunications and Signal Processing*, 2019, pp. 135–139.

[60] P. Ray, D. Dash, K. Salah, and N. Kumar, "Blockchain for IoT-based healthcare: Background, consensus, platforms, and use cases," *IEEE Systems Journal*, vol. 15, no. 1, pp. 85–94, 2020.

[61] G. Srivastava, R. M. Parizi, A. Dehghantanha, and K.-K. R. Choo, "Data sharing and privacy for patient IoT devices using blockchain," in *Proc. Int. Conf. Smart City and Informatization*, 2019, pp. 334–348.

[62] G. Tripathi, M. A. Ahad, and S. Paiva, "S2hs– a blockchain based approach for smart healthcare system," *Healthcare* , vol. 8, no. 1, p. 100391, 2020.

[63] T. Dey, S. Jaiswal, S. Sunderkrishnan, and N. Katre, "Healthsense: A medical use case of internet of things and blockchain," in *Proc. IEEE Int. Conf. Intelligent Sustainable Systems*, 2017, pp. 486–491.

[64] A. Ali Süzen and B. Duman, “ Protecting the privacy of IoT-based health records using blockchain technology,” pp. 35–54, 2021.

[65] K. M. Hossein, M. E. Esmaeili, T. Dargahi, A. Khonsari, and M. Conti, “Bchealth: A novel blockchain-based privacy-preserving architecture for IoT healthcare applications,” *Computer Communications*, vol. 180, pp. 31–47, 2021.

[66] G. Hameed, Y. Singh, S. Haq, and B. Rana, “Blockchain-based model for secure IoT communication in smart healthcare,” pp. 715–730, 2022.

[67] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, “Medibchain: A blockchain based privacy preserving platform for healthcare data,” in *Proc. Int. Conf. Security, Privacy and Anonymity in Computation, Communication and Storage*, 2017, pp. 534–543.

[68] G. Rathee, A. Sharma, H. Saini, R. Kumar, and R. Iqbal, “A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology,” *Multimedia Tools and Applications*, vol. 79, no. 15, pp. 9711–9733, 2020.

[69] J. Xu, K. Xue, S. Li, *et al*., “Healthchain: A blockchain-based privacy preserving scheme for large-scale health data,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8770–8781, 2019.

[70] S. Badr, I. Gomaa, and E. Abd-Elrahman, “Multi-tier blockchain framework for IOT-ehrs systems,” *Procedia Computer Science* , vol. 141, pp. 159–166, 2018.

[71] Z. Zulkifl, F. Khan, S. Tahir, M. Afzal, W. Iqbal, A. Rehman, S. Saeed, and A. M. Almuhaideb, “FBASHI: Fuzzy and blockchain-based adaptive security for healthcare IoTs,” *IEEE Access*, vol. 10, pp. 15 644–15 656, 2022.

[72] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, “ BlocHIE: A blockchain-based platform for healthcare information exchange,” in *Proc. Int. Conf. Smart Computing*, 2018, pp. 49–56.

[73] K. M. Hossein, M. E. Esmaeili, T. Dargahi, *et al*., “Blockchain-based privacy-preserving healthcare architecture,” in *Proc. Canadian Conf. Electrical and Computer Engineering*, 2019, pp. 1–4.

[74] G. Gunanidhi and R. Krishnaveni, “ Improved security blockchain for IoT based healthcare monitoring system,” in *Proc. 2nd Int. Conf. Artificial Intelligence and Smart Energy*, 2022, pp. 1244–1247.

[75] N. Sun, J. Zhang, Rimba, S. Gao, L. Y. Zhang, and Y. Xiang, “Data-driven cybersecurity incident prediction: A survey,” *IEEE Communications Surveys* & *Tutorials*, vol. 21, no. 2, pp. 1744–1772, 2018.

[76] H. Lu, Y. Tang, and Y. Sun, “ DRRS-BC: Decentralized routing registration system based on blockchain,” *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 12, pp. 1868–1876, 2021.

[77] Z. Cui, X. Fei, S. Zhang, X. Cai, Y. Cao, W. Zhang, and J. Chen, “A hybrid blockchain-based identity authentication scheme for multi-WSN,” *IEEE Trans. Services Computing*, vol. 13, no. 2, pp. 241–251, 2020.

[78] M. T. Hammi, P. Bellot, and A. Serhrouchni, “ BCTrust: A decentralized authentication blockchain-based mechanism,” in *Proc. Wireless Communications and Networking Conf.*, 2018, pp. 1–6.

[79] A. Fayad, B. Hammi, R. Khatoun, and A. Serhrouchni, “A blockchain-based lightweight authentication solution for IoT,” in *Proc. 3rd IEEE Cyber Security in Networking Conf.*, 2019, pp. 28–34.

[80] D. Li, W. Peng, W. Deng, and F. Gai, “ A blockchain-based authentication and security mechanism for IoT,” in *Proc. 27th IEEE Int. Conf. Computer Communication and Networks*, 2018, pp. 1–6.

[81] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, “Blockchain meets edge computing: A distributed and trusted authentication system,” *IEEE Trans. Industrial Informatics*, vol. 16, no. 3, pp. 1972–1983, 2019.

[82] K. Albalawi and M. M. A. Azim, “ Cloud-based IoT device authentication scheme using blockchain,” in *Proc. Global Conf. Internet of Things*, 2019, pp. 1–7.

[83] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, and K. Salah, “A user authentication scheme of IoT devices using blockchain-enabled fog nodes,” in *Proc. 15th IEEE Int. Conf. Computer Systems and Applications*, 2018, pp. 1–8.

[84] S. S. Panda, U. Satapathy, B. K. Mohanta, D. Jena, and D. Gountia, “A blockchain based decentralized authentication framework for resource constrained IoT devices,” in *Proc. 10th IEEE Int. Conf. Computing, Communication and Networking Technologies*, 2019, pp. 1–6.

[85] C. H. Lau, K.-H. Y. Alan, and F. Yan, “ Blockchain-based authentication in IoT networks,” in *Proc. Conf. Dependable and Secure Computing*, 2018, pp. 1–8.

[86] B. K. Mohanta, A. Sahoo, S. Patel, S. S. Panda, D. Jena, and D. Gountia, “ Decauth: Decentralized authentication scheme for IoT device using ethereum blockchain,” in *Proc. IEEE Region 10 Conf.*, 2019, pp. 558–563.

[87] I. Riabi, H. K. B. Ayed, and L. A. Saidane, “A survey on blockchain based access control for internet of things,” in *Proc. 15th IEEE Int. Wireless Communications & Mobile Computing Conf.*, 2019, pp. 502–507.

[88] J. Qiu, J. Zhang, W. Luo, L. Pan, S. Nepal, and Y. Xiang, “A survey of android malware detection with deep neural models,” *ACM Computing Surveys* (*CSUR*), vol. 53, no. 6, pp. 1–36, 2020.

[89] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, “Smart contract-based access control for the internet of things,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594–1605, 2018.

[90] H. Al Breiki, L. Al Qassem, K. Salah, M. H. U. Rehman, and D. Sevtinovic, “ Decentralized access control for IoT data using blockchain and trusted oracles,” in *Proc. Int. Conf. Industrial Internet*, 2019, pp. 248–257.

[91] B. S. Egala, A. K. Pradhan, V. Badarla, and S. Mohanty, “Fortified-chain: A blockchain-based framework for security and privacy-assured internet of medical things with effective access control,” *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11717–11731, 2021.

[92] B. Chai, B. Yan, J. Yu, and G. Wang, “BHE-AC: A blockchain-based high-efficiency access control framework for internet of things,” *Personal and Ubiquitous Computing*, pp. 1–12, 2021.

[93] M. A. Islam and S. Madria, “A permissioned blockchain based access control system for IoT,” in *Proc. Int. Conf. Blockchain*, 2019, pp. 469–476.

[94] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, “Fairaccess: A new blockchain-based access control framework for the internet of things,” *Security and Communication Networks*, vol. 9, no. 18, pp. 5943–5964, 2016.

[95] R. Xu, Y. Chen, E. Blasch, and G. Chen, “BlendCAC: A blockchain-enabled decentralized capability-based access control for IoTs,” in *Proc. IEEE Int. Conf. Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data*, 2018, pp. 1027–1034.

[96] O. Novo, “ Scalable access management in IoT using blockchain: A performance evaluation,” *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4694–4701, 2018.

[97] O. Novo, “Blockchain meets IoT: An architecture for scalable access management in IoT,” *IEEE Internet of Things Journal* , vol. 5, no. 2, pp. 1184–1195, 2018.

[98] D. Hwang, J. Choi, and K.-H. Kim, “Dynamic access control scheme for IoT devices using blockchain,” in *Proc. Int. Conf. Information and Communication Technology Convergence*, 2018, pp. 713–715.

[99] S. Singh, K. Sharma, S. Y. Moon, and J. H. Park, “Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions,” *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–18, 2017.

[100] B. B. Gupta, K.-C. Li, V. C. Leung, *et al*., “Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system,” *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 12, pp. 1877–1890, 2021.

[101] A. Manzoor, M. Liyanage, A. Braeke, S. S. Kanhere, and M. Ylianttila, “Blockchain based proxy re-encryption scheme for secure IoT data sharing,” in *Proc. Int. Conf. Blockchain and Cryptocurrency*, 2019, pp. 99–103.

[102] A. Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal, and F. M. Almansour, “ Blockchain-assisted secured data management

framework for health information analysis based on internet of medical things," *Personal and Ubiquitous Computing*, pp. 1–14, 2021.

[103] Z. Zhang, L. Huang, R. Tang, T. Peng, L. Guo, and X. Xiang, "Industrial blockchain of things: A solution for trustless industrial data sharing and beyond," in *Proc. 16th IEEE Int. Conf. Automation Science and Engineering*, 2020, pp. 1187–1192.

[104] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Annu. Int. Conf. Theory and Applications of Cryptographic Techniques*, 2005, pp. 457–473.

[105] Y. Rahulamathavan, R. C.-W. Phan, M. Rajarajan, S. Misra, and A. Kondoz, " Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption," in *Proc. Int. Conf. Advanced Networks and Telecommunications Systems*, 2017, pp. 1–6.

[106] A. Wu, Y. Zhang, X. Zheng, R. Guo, Q. Zhao, and D. Zheng, "Efficient and privacy-preserving traceable attribute-based encryption in blockchain," *Annals of Telecommunications*, vol. 74, no. 7, pp. 401–411, 2019.

[107] S. Liu, J. Yu, Y. Xiao, Z. Wan, S. Wang, and B. Yan, "BC-SABE: Blockchain-aided searchable attribute-based encryption for cloud-IoT," *IEEE Internet of Things Journal* , vol. 7, no. 9, pp. 7851–7867, 2020.

[108] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Future Generation Computer Systems* , vol. 95, pp. 420–429, 2019.

[109] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. Symp. Security and Privacy*, 2007, pp. 321–334.

[110] Y. Zhang, D. He, and K.-K. R. Choo, " BaDS: Blockchain-based architecture for data sharing with ABS and CP-ABE in IoT," *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1–9, 2018.

[111] D. Han, J. Chen, G. Zang, X. Wang, and Y. Gao, " DSSPS: A data sharing security protection scheme based on consortium blockchain and ciphertext-policy attribute-based encryption," in *Proc. 2nd Int. Conf. Blockchain Technology and Applications*, 2019, pp. 14–19.

[112] R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext security from identity-based encryption," in *Proc. Int. Conf. Theory and Applications of Cryptographic Techniques*, 2004, pp. 207–222.

[113] H. T. T. Truong, M. Almeida, G. Karame, and C. Soriente, "Towards secure and decentralized sharing of IoT data," in *Proc. Int. Conf. Blockchain*, 2019, pp. 176–183.

[114] H. Zhao, J. Yan, X. Luo, and X. Gua, "Privacy preserving solution for the asynchronous localization of underwater sensor networks," *IEEE/CAA J. Autom. Sinica*, vol. 7, no. 6, pp. 1511–1527, 2020.

[115] A. R. Shahid, N. Pissinou, L. Njilla, S. Alemany, A. Imteaj, K. Makki, and E. Aguilar, " Quantifying location privacy in permissioned blockchain-based internet of things (IoT)," in *Proc. 16th EAI Int. Conf. Mobile and Ubiquitous Systems: Computing, Networking and Services*, 2019, pp. 116–125.

[116] M. Yang, T. Zhu, K. Liang, W. Zhou, and R. H. Deng, "A blockchain-based location privacy-preserving crowdsensing system," *Future Generation Computer Systems*, vol. 94, pp. 408–418, 2019.

[117] S. Zou, J. Xi, G. Xu, M. Zhang, and Y. Lu, " CrowdHB: A decentralized location privacy-preserving crowdsensing system based on a hybrid blockchain network," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14803–14817, 2022.

[118] H. Li, L. Pei, D. Liao, G. Sun, and D. Xu, "Blockchain meets VANET: An architecture for identity and location privacy protection in VANET," *Peer-to-Peer Networking and Applications* , vol. 12, no. 5, pp. 1178–1193, 2019.

[119] S. Zou, J. Xi, H. Wang, and G. Xu, "CrowdBLPS: A blockchain-based location-privacy-preserving mobile crowdsensing system," *IEEE Trans. Industrial Informatics*, vol. 16, no. 6, pp. 4206–4218, 2019.

[120] S. K. Lo, Q. Lu, C. Wang, H.-Y. Paik, and L. Zhu, " A systematic literature review on federated machine learning: From a software engineering perspective," *ACM Computing Surveys* (*CSUR*) , vol. 54, no. 5, pp. 1–39, 2021.

[121] M. Qi, Z. Wang, F. Wu, R. Hanson, S. Chen, Y. Xiang, and L. Zhu, "A blockchain-enabled federated learning model for privacy preservation: System design," in *Proc. Australasian Conf. Information Security and Privacy*, 2021, pp. 473–489.

[122] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT," *IEEE Trans. Industrial Informatics*, vol. 16, no. 6, pp. 4177–4186, 2019.

[123] Y. Zhao, J. Zhao, L. Jiang, R. Tan, D. Niyato, Z. Li, L. Lyu, and Y. Liu, " Privacy-preserving blockchain-based federated learning for IoT devices," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1817–1829, 2021.

[124] Y. Qu, L. Gao, T. H. Luan, Y. Xiang, S. Yu, B. Li, and G. Zheng, "Decentralized privacy using blockchain-enabled federated learning in fog computing," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5171–5183, 2020.

[125] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles," *IEEE Trans. Vehicular Technology*, vol. 69, no. 4, pp. 4298–4311, 2020.

[126] H. Chai, S. Leng, Y. Chen, and K. Zhang, "A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles," *IEEE Trans. Intelligent Transportation Systems* , vol. 22, no. 7, pp. 3975–3986, 2021.

[127] A. C. Yao, "Protocols for secure computations," in *Proc. 23rd IEEE Annu. Symp. Foundations of Computer Science*, 1982, pp. 160–164.

[128] H. Shrobe, D. L. Shrier, and A. Pentland, " Enigma: Decentralized computation platform with guaranteed privacy," pp. 425–454, 2018.

[129] Z. Guan, X. Zhou, P. Liu, L. Wu, and W. Yang, "A blockchain based dual side privacy preserving multi party computation scheme for edge enabled smart grid," *IEEE Internet of Things Journal*, 2021.

[130] Y. Yang, L. Wei, J. Wu, and C. Long, "Block-SMPC: A blockchain-based secure multi-party computation for privacy-protected data sharing," in *Proc. 2nd Int. Conf. Blockchain Technology*, 2020, pp. 46–51.

[131] B. Jia, X. Zhang, J. Liu, Y. Zhang, K. Huang, and Y. Liang, "Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT," *IEEE Trans. Industrial Informatics* , vol. 18, no. 6, pp. 4049–4058, 2022.

[132] T. H. Kim and J. Lampkins, "SSP: Self-sovereign privacy for internet of things using blockchain and MPC," in *Proc. Int. Conf. Blockchain*, 2019, pp. 411–418.

[133] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Proc. Int. Conf. Theory and Application of Cryptology and Information Security*, 2001, pp. 552–565.

[134] C. Dwork, " Differential privacy: A survey of results," in *Proc. Int. Conf. Theory and Applications of Models of Computation*, 2008, pp. 1–19.

[135] G. G. Dagher, J. Mohler, M. Milojkovic, and B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustainable Cities and Society*, vol. 39, pp. 283–297, 2018.

[136] H. Wu and C. Tsai, " Toward blockchains for health-care systems: Applying the bilinear pairing technology to ensure privacy protection and accuracy in data sharing," *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 65–71, 2018.

[137] S. Jiang, J. Cao, J. A. McCann, Y. Yang, Y. Liu, X. Wang, and Y. Deng, " Privacy-preserving and efficient multi-keyword search over encrypted data on blockchain," in *Proc. IEEE Int. Conf. Blockchain*, 2019, pp. 405–410.

[138] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Future Generation Computer Systems* , vol. 95, pp. 420–429, 2019.

[139] X. Huang, D. Ye, R. Yu, and L. Shu, "Securing parked vehicle assisted fog computing with blockchain and optimal smart contract design," *IEEE/CAA J. Autom. Sinica*, vol. 7, no. 2, pp. 426–441, 2020.

Minfeng Qi received the M.S. degree in information system from Monash University, Australia, in 2019. He is currently pursuing the Ph.D. degree from Swinburne University of Technology, Australia. His research interests include blockchain, privacy-enhancing technologies, and federated learning. He has published papers in *IEEE ICWS*, *IEEE Blockchain*, and *ICBC*.

Ziyuan Wang is a Senior Research Fellow at Swinburne University of Technology in Australia. She received the Ph.D. degree from the University of Melbourne in 2010. Her research interests include blockchain, stream computing, and spatio-temporal data analytics. She has published papers in international journals and conferences, as well as co-authored patents in IoT, AI, and blockchain.

Qing-Long Han (Fellow, IEEE) received the B.Sc. degree in mathematics from Shandong Normal University in 1983, and the M.Sc. and Ph.D. degrees in control engineering from East China University of Science and Technology, in 1992 and 1997, respectively.

Professor Han is Pro Vice-Chancellor (Research Quality) and a Distinguished Professor at Swinburne University of Technology, Australia. He held various academic and management positions at Griffith University and Central Queensland University, Australia. His research interests include networked control systems, multi-agent systems, time-delay systems, smart grids, unmanned surface vehicles, and neural networks.

Professor Han was awarded The 2021 Norbert Wiener Award (the Highest Award in systems science and engineering, and cybernetics) and The 2021 M. A. Sargent Medal (the Highest Award of the Electrical College Board of Engineers Australia). He was the recipient of The 2021 IEEE/CAA Journal of Automatica Sinica Norbert Wiener Review Award, The 2022 IEEE Systems, Man, and Cybernetics (SMC) Society Andrew P. Sage Best Transactions Paper Award, The 2020 IEEE SMC Society Andrew P. Sage Best Transactions Paper Award, The 2020 IEEE Transactions on Industrial Informatics Outstanding Paper Award, and The 2019 IEEE SMC Society Andrew P. Sage Best Transactions Paper Award.

Professor Han is a Member of the Academia Europaea (The Academy of Europe). He is a Fellow of The International Federation of Automatic Control and a Fellow of The Institution of Engineers Australia. He is a Highly Cited Researcher in both Engineering and Computer Science (Clarivate Analytics). He has served as an AdCom Member of IEEE Industrial Electronics Society (IES), a Member of IEEE IES Fellows Committee, and Chair of IEEE IES Technical Committee on Networked Control Systems. He is Co-Editor-in-Chief of *IEEE Transactions on Industrial Informatics*, Deputy Editor-in-Chief of *IEEE/CAA Journal of Automatica Sinica*, Co-Editor of *Australian Journal of Electrical and Electronic Engineering*, an Associate Editor for 12 international journals, including the *IEEE Transactions on Cybernetics*, *IEEE Industrial Electronics Magazine*, *Control Engineering Practice*, and *Information Sciences*, and a Guest Editor for 14 Special Issues.

Jun Zhang (Senior Member, IEEE) received the Ph.D. degree in computer science from the University of Wollongong, Australia, in 2011.

He is the Co-Founder and Director of the Cybersecurity Lab, Swinburne University of Technology, Australia. His research focuses on cybersecurity. He is the Chief Investigator of several projects in cybersecurity, funded by the Australian Research Council (ARC). He has published more than 100 research papers in reputed international journals and conferences, such as the *IEEE CST*, *PIEEE*, *TIFS*, *TDSC*, *CSUR*, *CCS*, *PETS*. Two of his papers were selected as the featured articles in IEEE TDSC and IT Professional. He has been recognised in The Australians Top Researchers special edition publication (09/2020) as the leading researcher in the field of Computer Security & Cryptography. He is leading Swinburne Cybersecurity Lab to deliver value and impact to our community, including significant contribution to Australian P-TECH education program and penetration test service to the industry partners.

Shiping Chen (Senior Member, IEEE) received the Ph.D. degree in computer science from UNSW, Australia, in 2000.

He is a Principal Research Scientist with Data61, CSIRO. He is an Adjunct Associate Professor with the University of Sydney and the University of New South Wales through supervising Ph.D. students. He has been working on distributed systems for over 20 years with focus on performance, security, and trust. He has published 180+ research papers and technical reports in these areas. He has been actively participating in research communities through publishing papers, journal editorships and conference PC/Chair services, including WWW, EDOC, ICSOC, IEEE ICWS/SCC/CLOUD and ICBC. His current research interests include: application security, blockchain and service computing.

Yang Xiang (Fellow, IEEE) received the Ph.D. in computer science from Deakin University, Australia. He is currently a Full Professor and the Dean of Digital Research, Swinburne University of Technology, Australia. His research interests include cyber security, which covers network and system security, data analytics, distributed systems, and networking. He is also leading the Blockchain initiatives at Swinburne. In the past 20 years, he has published more than 300 research papers in many international journals and conferences. He is the Editor-in-Chief of the *SpringerBriefs on Cyber Security Systems and Networks*. He serves as the Associate Editor of *IEEE Transactions on Dependable and Secure Computing*, *IEEE Internet of Things Journal*, and *ACM Computing Surveys*. He served as the Associate Editor of *IEEE Transactions on Computers* and *IEEE Transactions on Parallel and Distributed Systems*. He is the Coordinator, Asia for IEEE Computer Society Technical Committee on Distributed Processing (TCDP). .