Future Generation Computer Systems 97 (2019) 512–529

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions

Muneeb Ul Hassan [a,*], Mubashir Husain Rehmani [b], Jinjun Chen [a]

[a] Swinburne University of Technology, Hawthorn VIC 3122, Australia
[b] Department of Computer Science, Cork Institute of Technology, Rossa Avenue, Bishopstown, Cork, Ireland

HIGHLIGHTS

- We present the importance of privacy preservation in blockchain-based IoT systems.
- We provide analysis of privacy preservation strategies applied in blockchain-based IoT systems.
- We highlight future research directions and challenges of blockchain privacy of IoT systems.

ARTICLE INFO

Article history:
Received 30 October 2018
Received in revised form 6 January 2019
Accepted 22 February 2019
Available online 1 March 2019

Keywords:
Internet of things (IoT)
Blockchain
Decentralized IoT
Privacy issues of blockchain-based IoT
Privacy preservation

ABSTRACT

Modern Internet of Things (IoT) systems are paving their path for a revolutionized world in which majority of our objects of everyday use will be interconnected. These objects will be able to link and communicate with each other and their surroundings in order to automate majority of our tasks. This interconnection of IoT nodes require security, seamless authentication, robustness and easy maintenance services. In order to provide such salient features, blockchain comes out as a viable solution. The decentralized nature of blockchain has resolved many security, maintenance, and authentication issues of IoT systems. Therefore, an immense increase in applications of blockchain-based IoT systems can be seen from the past few years. However, blockchain-based IoT network is public, so transactional details and encrypted keys are open and visible to everybody in that network. Thus, any adversary can infer critical information of users from this public infrastructure. In this paper, we discuss the privacy issues caused due to integration of blockchain in IoT applications by focusing over the applications of our daily use. Furthermore, we discuss implementation of five privacy preservation strategies in blockchain-based IoT systems named as anonymization, encryption, private contract, mixing, and differential privacy. Finally, we discuss challenges, and future directions for research in privacy preservation of blockchain-based IoT systems. This paper can serve as a basis of development of future privacy preservation strategies to address several privacy problems of IoT systems operating over blockchain.

1. Introduction

The exponential growth of devices using Internet of Things (IoT) technology has attracted attention of both academia and industrial sector [1]. IoT technology is playing an active part in advancement of various domains of our everyday life including industrial automation, transportation, energy systems, and healthcare. It is predicted that there will be approximately 18 billion IoT devices by the year 2022 [2]. These IoT devices collect data from surroundings and may exchange information with other IoT devices, and platforms. In traditional IoT systems, collected data is stored in certain centralized server (especially cloud servers) for future use [3]. Therefore, IoT users have to develop trust for the centralized servers that their sensitive and private data is safe in these servers. Despite of the unquestionable advantages offered by these service providers, centralized IoT systems may face certain challenges [4]. For instance, unencrypted server data can be hacked and may cause leakage of sensitive information [5]. Moreover, some IoT devices require management by more than one manager a same time. Keeping in view all these points, researchers are thinking to move towards decentralized architecture for management and storage of IoT devices and data respectively [6]. Blockchain is a new paradigm towards decentralized storage and data management, as it actually works over the concept of a shared, secured, and distributed ledger that stores and keeps records without any centralized authority or trusted third-party [7]. In context of IoT, blockchain permits two devices to communicate and exchange, resources, information, and

* Corresponding author.
E-mail addresses: muneebmh1@gmail.com (M. Ul Hassan), mubashir.rehmani@cit.ie (M.H. Rehmani), jinjun.chen@gmail.com (J. Chen).

https://doi.org/10.1016/j.future.2019.02.060
0167-739X/

data in a decentralized peer-to-peer (P2P) network. Blockchain provides a transparent infrastructure in which chances of any fraudulent entry is minimum because the decision of addition of any data is broadcast to the whole network, and any critical decision is taken with consent of majority of users instead of a single centralized administrator/server. Similarly, blockchain-based IoT systems are secure against certain attackers whom aim is to control the centralized server and get personal information or control the whole system. Certainly, the additional cost over security monitoring of IoT servers can easily be minimized using blockchain [8]. Furthermore, blockchain technology stores IoT devices records in such a way that they are easy to backtrack in case of any contradiction or issue.

One major phenomenon used during data dissemination of IoT devices in blockchain network is encryption. In a P2P network, every node is equipped with two different keys. One is public key; which is used by other nodes to encrypt the message and broadcast it to all nodes. While second one is private key; this key is used by specific receiver to decrypt the received message [9]. Only the node having a unique and specific private key can decrypt the message and can see its' contents. This key encryption ensures the security within a blockchain network, so that any intruder or adversary will not be able to infer the information illegally. However, in a blockchain based IoT network every IoT device is identified using its public key. Which means that privacy is not confirmed, since every transaction or transmission is shared, there is a possibility for a third-party to view and analyse these transactions, and infer the real identities of IoT participants [10]. This scenario becomes more complex, because the privacy requirements of IoT devices varies from one country to another [11].

In order to overcome these privacy issues, researchers have started working over privacy preservation of blockchain based IoT systems. Certain approaches including private contract, anonymization, encryption, mixing, and differential privacy have been introduced by researchers to overcome these privacy issues [12]. The proposed approaches have certain advantages, disadvantages, and limitations. In this research article, we analyse and discuss the importance, application, and protection methods regarding privacy preservation of blockchain-based IoT systems.

1.1. Contribution of this article

While few researchers highlighted and surveyed concept of privacy preservation in blockchain technology, to the best of our knowledge there is no article discussing the importance, application, and protection techniques of blockchain technology from IoT perspective. In this paper, we present state-of-the-art literature on privacy protection in blockchain-based IoT systems. In summary, the key contributions made in this article are as follows:

- We highlight the importance of privacy protection in blockchain-based IoT systems.
- We focus more over presenting the practical issues caused due to privacy leakage in IoT systems operating on blockchain technology.
- We provide an analysis about implementation of privacy protection techniques of blockchain-based IoT systems.
- We focus on integration of privacy preservation technologies in practical applications of IoT systems working over blockchain.
- We outline various open issues, challenges, and certain future direction for research in privacy protection of blockchain-based IoT systems.

1.2. Review of related survey articles

Our current article provides a detailed overview of privacy issues in blockchain-based IoT systems and is distinct from all previous articles and studies, as we significantly cover the specific area of privacy issues in applications of blockchain-based IoT systems. A comprehensive literature of past survey articles focusing over blockchain and its integration with IoT is present, and few of them focused over security and privacy issues of blockchain. However, to the best of our knowledge, there is no past article that profoundly addresses privacy preservation strategies in blockchain-based IoT environment from application perspective. We categorize the previous work of literature over blockchain into 8 major categories named as blockchain applications, blockchain as trust model, blockchain-based security services, blockchain for security and privacy of IoT, security and privacy issues of bitcoin, security issues of blockchain, privacy issues of blockchain systems, and privacy issues in blockchain-based IoT systems. The detailed application scenario, major scientific contributions and certain considered factors about previous survey articles is demonstrated in Table 1.

A profound work on applications of blockchain is presented in [13,14]. Gao et al. in [14] outlined the functioning and implementation of practical framework of blockchain system and provided discussion about the applications of blockchain in a comprehensive and detailed manner. Similarly, in [13], the authors provided a significant overview of direct and smart contract based transactions in blockchain-based banking ledgers. They further discussed two state-of-the-art concepts called as "Internet of money" and "second generation blockchain". Moving further to use cases of blockchain, the authors in [15] used blockchain as a trust model because of its salient properties. The authors provided a systematic survey of practical implementation of blockchain in various smart applications. Another key survey over using blockchain as a security service is conducted by Salman et al. in [16]. This survey focused over using blockchain for different security services such as access control, authentication, privacy control, and confidentiality.

It is important to discuss here that implementation of blockchain in IoT systems is analysed from two different perspectives. One is the use of blockchain in IoT in order to enhance its security and privacy because of immutable, decentralized, and secure nature of blockchain. However, another aspect in the research of blockchain-based IoT systems is the discussion about security and privacy issues that arises with the incorporation of blockchain in IoT systems. Here, we first investigate few survey articles covering the first aspect of blockchain as security and privacy, and afterwards we discuss about security and privacy issues in blockchain-based IoT systems. An extensive literature on the use of blockchain for security and privacy if IoT systems is provided in [17–19]. In [17], a detailed analysis about integration of blockchain for IoT systems is given. To strengthen the provided claims, authors further discussed two case studies of smart homes and food supply chain and concluded that blockchain can be feasible solution to enhance security and transparency of IoT systems. Likewise, the authors in [18] discussed about various functional characteristics of blockchain in IoT systems, furthermore, they worked over highlighting the major challenges, and research problems being faced while developing such systems. The authors focused over decentralized nature and showed its importance in IoT systems using detailed analysis. Moreover, Ferrag et al. in [19] provided a comprehensive literature survey of different blockchain protocols for IoT networks, and discussed various threat models for IoT applications operating over blockchain environment. Similarly, another critical survey discussing recent industrial and research advances of blockchain-based IoT systems is carried out in [20].

Table 1
Summary comparison of previous survey articles over security and privacy aspects of blockchain with its application scenario, year, major contributions, and considered factors. ✔ Indicates that the topic is covered, ✗ indicates that the topic is not covered, and ✻ indicates that the topic is partially covered.

Application Scenario	Ref No.	Year	Major Contribution	Considered Factors	Discussed Privacy in Blockchain IoT
Blockchain Applications	[13]	2016	Overview of blockchain transactions and smart contract based second generation blockchain system is provided	• Internet of money • Transaction security • Banking Ledger	✗
	[14]	2018	Outlined framework of blockchain and along with provided a detailed discussion about its applications	• Practical usage of blockchain • Security vulnerabilities and privacy attacks	✻
Blockchain as Trust Model	[15]	2018	A systematic overview of practical implementation of blockchain as a trust model is presented	• Smart applications using blockchain • Security, privacy, and scalability aspects	✻
Blockchain-based security services	[16]	2018	Use of blockchain as a security service such as access control, authentication, privacy control, and confidentiality is studied in detail	• Cryptographic solutions • Integrity assurance • Challenges, problems and their effect over current applications	✗
Blockchain for Security and Privacy of IoT	[17]	2019	A detailed analysis over integration of blockchain for IoT systems is provided and information is supported with the help of two case studies	• Data storage architecture for blockchain-based IoT systems • Legal issues and optimal design goals for blockchain integration	✻
	[18]	2018	A discussion about characteristics of blockchain in IoT application is carried out along with it highlighted the major problems in development of such systems	• Decentralized features of IoT • Traceability and information exchange in blockchain nodes	✻
	[19]	2018	A comprehensive literature survey of blockchain protocols for various IoT networks is presented from application perspective	• IoT applications over blockchain • Threat models for blockchain-based IoT systems	✻
	[20]	2018	A detailed discussion about the implementation, challenges, and recent advances of applications of blockchain over IoT systems is provided	• Applications of blockchain in IoT • Recent advances in industry and research	✻
Security and privacy issues of Bitcoin	[21]	2016	An investigation about recent challenges of bitcoin transactions is presented by focusing mainly over transactional privacy	• Scalability solutions • Impact of these solutions over user privacy	✗
	[22]	2018	A brief discussion about vulnerabilities, security threats, privacy threats, and their prospective solutions for bitcoin system is presented	• Vulnerabilities in PoW • Crypto user privacy	✗
Security Issues of Blockchain	[23]	2017	An in-depth study about security threats and corresponding real attacks over blockchain systems is carried out	• Risks to blockchain • Attack models • Solution protocols	✗
	[24]	2018	Summary and classification of blockchain data attacks and their defence mechanisms are presented	• Data integrity • Data controllability attacks • Security protection strategies	✗
Privacy Issues of Blockchain Systems	[25]	2018	A comprehensive literature review of privacy aspects of blockchain is provided by focusing over possible solution strategies	• Critical analysis of zero knowledge proofs, cryptography, and signature approaches of blockchain	✗
	[26]	2018	Detailed insights about privacy issues in blockchain network is provided along with analysing various defence mechanisms	• Cryptographic solutions • Anonymization • Privacy services	✗
Privacy Issues in Blockchain-based IoT Systems	This Work	2018	An in-depth survey of privacy preservation techniques of blockchain-based IoT systems from application and implementation perspective	• Privacy preservation strategies • Attacks of blockchain-based IoT • Functioning and implementation of blockchain privacy preserving approaches	✔

Moving towards the second aspect called as security and privacy issues of blockchain, many researchers explored this field and highlighted that blockchain is not 100% secure and is prone to many vulnerabilities and security threats. One pioneering work over privacy and security issues of bitcoin is presented by Conti et al. in [22]. This work briefly studies vulnerabilities, security threats, privacy threats, and their prospective solutions for bitcoin system. The article also analysed PoW based consensus mechanism and highlighted that it is also prone to many vulnerabilities. Another work purely targeting privacy in bitcoin

transactions is presented in [21]. The authors investigated state-of-the-art challenges of transactional privacy and studied the impact of various proposed solutions by focusing over individual user privacy. The domain of security issues of blockchain system is briefly analysed in [23,24]. In [23], Li et al. presented an insightful study about security threats and corresponding real attacks over blockchain system. Furthermore, the authors presented a detailed summary of solution protocols to tackle certain attacks and threats. Similarly, a detailed summary and classification of blockchain data attacks and their defence mechanisms by focusing over data integrity is presented in [24].

A detailed investigation over privacy issues and solutions of blockchain is carried out in [25,26]. The authors in [25] provided a comprehensive literature review of privacy aspects of blockchain and their possible solution strategies. The study presented an in-depth analysis of zero knowledge proofs, cryptography, and signature approaches of blockchain. Feng et al. in [26] presented a detailed insights about privacy issues in blockchain systems. Afterwards, the authors analysed various defence mechanism by providing a brief summary of technical details. However, the survey topics of all presented blockchain surveys do not address the privacy issues and their solutions in blockchain-based IoT systems.

1.3. Article structure

The remainder of paper is organized as follows: Section 2 presents overview of blockchain and IoT technology. Section 3 briefly states the privacy issues during implementation of blockchain in IoT. While, Section 4 provides a detailed information about privacy preservation strategies in blockchain-based IoT system. Section 5 provides a brief overview of challenges and future research directions. Finally, Section 6 concludes the paper.

2. Blockchain and internet of things: An overview

Decentralized storage property of blockchain has paved paths for various other future technologies and IoT is one of them. In this section, we discuss blockchain, IoT, types of IoT and blockchain, and motivation of using blockchain in IoT systems.

2.1. Blockchain

Blockchain technologies emerged after the introduction of an online cryptocurrency named as Bitcoin in 2008 [27]. The reason behind such rapid spread of Bitcoin was its absence of control from any centralized financial entity or authority. Relatively, the currency was securely and collectively held and stored by the help of a decentralized network of nodes that constitute a transparent and auditable network. The popularity of Bitcoin caused researchers to work over the concept of technology managing it, and then researches started exploring blockchain technology in deep detail. The functioning of blockchain is based on a decentralized distributed ledger system that is shared among every blockchain node. The information on ledger is open and transparent, hence every transaction even from the start of system can be audited using this transparent nature. Moreover, the transactions are immutable, which means that one transaction can never be overwritten or removed from the ledger. This immutability develops the trust of users in the network, that their assets or currency is safe and can easily be tracked even in case of any error. After every transaction, the new information containing the type and value of transaction along with the timestamp of transaction is stored in the block using ledger. Each block stores the performed set of transactions, these blocks are further linked with each other with reference of previous block and thus form a chain like structure called as blockchain [12].

Blockchain is a P2P decentralized network, hence the phenomenon of storage, security, routing, and mining cannot be neglected [28]. The transaction and block details are propagated into the network by the use of routing protocol. A ledger storage is responsible for keeping the true copy of transactions in the chain of nodes. Security or wallet services allow blockchain users to perform secure and risk-free transactions with the help of security keys. Finally, the phenomenon of mining is used to create the new set of blocks or to solve the puzzle such as proof-of-work. Few major characteristics of blockchain technology are presented in Fig. 1.

2.1.1. Types of blockchain systems

On the basis of several criterions such as authentication and control mechanism, blockchain systems can further be divided into three sub categories.

2.1.1.1. Public blockchain.

A permissionless or public blockchain is basically an open source decentralized platform in which every individual independent of its organization or background can join, and can perform mining or transaction operations [29]. Every node participating in blockchain has full authority to perform operation of reading, writing, auditing, or reviewing of blockchain at any instance of time for example Bitcoin cryptocurrency [27]. Public blockchain is a P2P transparent network in which every user is able to collect transaction information and start the mining process to earn the reward. *Miner* nodes collect the transaction information in blocks, check validity of them, and afterwards start the consensus to mine and append the reward/block into the existing blockchain [30]. Consensus mechanism is used to ensure the consistency of blocks throughout blockchain, the consistency is maintained so that no node has multiple blocks that contradict each other. In public blockchain, the participants are unknown before mining, and every node is allowed to create a block, which in turn make public blockchain prone to Sybil attacks [31].

One of the most efficient mechanism to overcome such issues in public blockchains is Proof-of-Work (PoW) consensus. In this mechanism, if adversary wants to control the blockchain, then it requires to have 51% of mining power of the blockchain network. In order to secure transaction, public key cryptography is used in blockchain in which address of every user is hash value of the users' public key. A participating node can pass the transaction/asset to another node by simply signing hash of its previous trading transaction along with including the new owners' public key in transaction. Similarly, the new owner has to verify signature in order to confirm the ownership chain [32]. However, because of high computational complexity, PoW and public block chains are not suitable for certain applications such as finance and banking because large volume of data needs to be handled in these applications. Researchers are working to develop efficient and less complex mechanisms for such applications.

2.1.1.2. Private blockchain.

A permissioned or private blockchain system is a decentralized network which is designed to assist private exchange and sharing of volume/data within an organization or specified group of people. Mining phenomenon in a private blockchain is controlled by selected individual or a specific organization, thus any new/unknown user cannot access the blockchain until the new user receive a special invite from the authority controlling it [33]. Hyperledger [34] is one of the most famous example of private blockchain. Deterministic distributed consensus such as PFBT [35] is carried out in private blockchain to ensure the transparency,

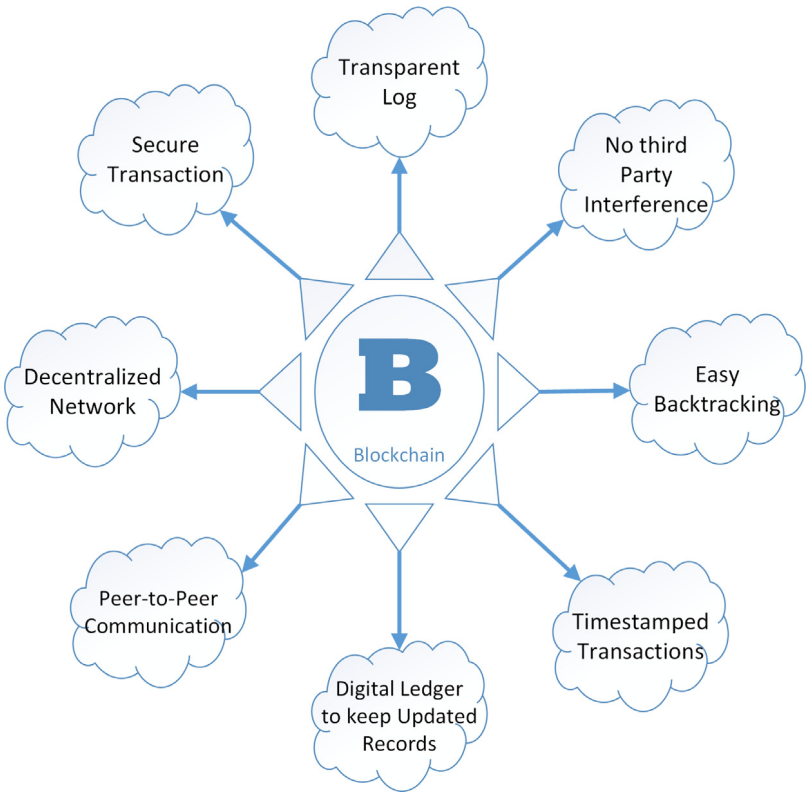

Fig. 1. Advantages of using blockchain technology.

and security. PFBT is a consensus protocol that works over pre-preparation, preparation, and commitment phases. The writes in a private blockchain is restricted, and only the controlling nodes have the permission to write or transact something in the network. This makes the inclination of private blockchain towards a centralized architecture. However, certain other properties of private blockchain such as consensus, distributed ledger, transparent log, and P2P communication, and smart contracts make this type of blockchain suitable for financial organizations and banks [36].

2.1.1.3. Consortium blockchain.

Consortium blockchain system is generally considered as a merger of public and private blockchain. In consortium blockchain, a group of organizations or individuals are responsible to take decisions regarding block validation and consensus [37]. These group of organization decides participating and mining nodes in the network. A multi-signature scheme is used to mine the block in the network, in which the mined block is only considered as a valid block if the controlling nodes approve and sign it up [33]. These controlling nodes can also decide regarding the read or write permission of the network, they can approve or block someone from reading or writing in the blockchain network. However, one major disadvantage of this type of blockchain is its possibility of tampering. As the blockchain is controlled by group of nodes, they can collaborate with each other and may reverse or tamper a transaction. In turn, it destroys the irreversibility and immutability guarantee of blockchain technology.

2.1.2. Working phenomenon of blockchain

Blockchain is an append-only, shared, fault-tolerant, and distributed database which maintains set of records in form of blocks. The blocks are transparent and are accessible by every blockchain node, however they cannot be modified or deleted. Blocks combine with each other and form a chain like structure, each block is linked with its predecessor according its hash value [7]. Similarly, each block has its transactional value along with private key and creation time of that specific block. Since blockchain is a P2P network, communication between peers is carried out using broadcast phenomenon. A new block in the blockchain architecture is created using mining process. The new created block is first validated, and after validation it is linked to blockchain database and after linking it cannot be modified or deleted. The first block in the blockchain is known as *genesis*, which is always hardcoded block into software. For any new block in the blockchain database, it only has one path towards genesis. Another terminology named as *fork* refers to two blocks that are created at the same time or few seconds apart. Once blockchain encounters any such situation, the latest block on the basis of complexity of that chain is chosen, while the other chain is the considered invalid and the blocks of invalid chain are known as *orphan* blocks [6].

2.1.2.1. Consensus and mining in blockchain. Since blockchain do not have any trusted third-party, all nodes in the network follow a consensus mechanism to validate a new transaction. Consensus is carried out to ensure that there is no conflict in future regarding any carried transaction. The consensus in blockchain is carried out using various methods, few are named as proof of work (PoW) [38], proof of space (PoSpace) [39], measure of trust (MoT) [40], proof of stake (PoS) [41], proof of importance (PoI) [42], practical byzantine fault tolerance (PBFT) [35], and minimum block hash [38]. The most famous used consensus approach is PoW which is also used in Bitcoin and other similar blockchain technologies. Mining nodes are required to solve a hard mathematical puzzle in order to win reward. After solving of puzzle, the reward earned in the form of mined block is further submitted to all nodes of network of blockchain who further validate and agree upon submission. Once the legitimacy of block

is confirmed, it is then appended in the blockchain database. Thus, compromising a PoW based blockchain requires adversary to get control over more than 50% of nodes. Similarly, another well-known digital currency named as Ethereum [43] uses both PoW and PoS. Unlike PoW, the mechanism of PoS do not require mining nodes to work over and solve any mathematical problem to get reward. Contrary to this, the miner who is allowed to create new block is chosen randomly on the basis of its wealth. The more wealth a node has, the higher will the chances of that particular node to mine the next block in the blockchain.

2.2. Internet of things

The name IoT was introduced first to address identifiable unique objects that were connected with the help of a wireless medium called as radio-frequency identification (RFID) [44]. However by keeping in view the benefits, this RFID concept shifted towards Internet. In IoT, everyday objects are equipped with sensors, transceivers, and microcontrollers for efficient reporting and communication. The basic concept of IoT is to make Internet more pervasive and immersive by enabling easy interaction and connection of IoT devices with Internet and with each other [45]. Nowadays, IoT is found in approximately every application of our daily lives ranging from home energy systems to transportation systems. In this section, we discuss few important applications of IoT systems that have a huge impact on our everyday life.

2.2.1. Applications of internet of things

2.2.1.1. Healthcare systems.

Healthcare is one of the most essential and fundamental part of human life. Trend of involvement of IoT in healthcare initiated from the concept of remote monitoring of patients [46]. This phenomenon further strengthened and now various healthcare devices are working over the principles of IoT based systems. The connection of healthcare with IoT has great potential and it gave rise to numerous modern healthcare applications such as real-time health data monitoring, electronic health (E-health) record keeping, and wearable health devices. Healthcare devices are being made smart by enhancing their connection with Internet and with each other. Similarly, wearable healthcare devices contains wireless sensors that collect and transmit real-time data [47,48]. This transmitted data contains specific medical parameters of patient, such as blood glucose level, blood pressure, heartbeat, etc. The data from healthcare devices is collected and stored in centralized servers or cloud. This data is further used by various doctors and healthcare survey organizations to conduct surveys regarding various diseases or upcoming threats in near future.

2.2.1.2. Energy systems.

With the involvement of information and communication technologies (ICT) in energy systems, the traditional energy systems are being replaced by *smart grids* that is also known as future of energy systems. Smart grid is considered as next generation energy system because of its various applications such as two-way communication, cost-effectiveness, and un-interrupted power supply [49]. Researchers are working over these systems to make them more advance and efficient by involving IoT technologies in energy systems such as load forecasting, real-time pricing, demand response, and timestamped load monitoring. Another important application of smart grid includes its merger with modern electric vehicles (EVs). EV also known as plug-in electric vehicle is a modern electric vehicle that is capable to get its batteries charged by smart grid power. Smart charging and discharging phenomenon of EVs can help smart grid to balance its load, as EVs can be charged even at low power and can also supply power to smart grid if its required [50].

2.2.1.3. Intelligent transportation systems.

The term intelligent transportation system (ITS) is used to show the advancements in traditional vehicular networks. In ITSs, vehicle-to-vehicle (V2V) communication, device-to-device (D2D) communication, traffic system, mass transits, and similar parameters are addressed to improve congestion, safety, sustainability, and efficiency of traditional transport system [51]. This merger of IoT technology with transportation system is also named as Internet of Vehicles (IoV), in which every travelling vehicle within a certain area will be connected to each other by the help of D2D and V2V communication [52]. By the help of IoT technology, every vehicle can be tracked in case of an emergency, similarly the routes and previous travelling history of vehicles can be used in order to find best travelling routes for future on the basis of time. Real-time vehicular data is usually transmitted and stored via mobile applications such as Google Maps, which is used by certain organizations in future. The integration of IoT in transportation systems are playing an important role in enhancement of ITSs.

2.2.1.4. Finances.

People are experiencing new level of financial services because of vast connections and communications of IoT systems. Financial IoT is the new paradigm in banking sectors and researches have started work over enhancement of certain performance analytics and data processing services using IoT technology [53]. The quality of service of financial and banking system can be enhanced and made efficient by using IoT technologies in finance sector. For example, financial organizations can add up an intelligent gateway over their application and communication layer to track each transaction in the most efficient way. These types of gateways provides intelligent information tracking by the use of RFID, social networks, global positioning system (GPS), telematics and similar mobile devices [54]. Thus, integration of IoT in banking sector can be very beneficial and researches are being carried out to further explore the potential of this field.

2.3. Motivation of using blockchain in internet of things

Blockchain has the potential to efficiently revolutionize functioning of a large number of IoT applications by providing a decentralized, trusted, and secured data sharing service in which information can easily be traced and backtracked. It can enhance various IoT systems such as smart grid, smart cars, food industry, healthcare systems, etc. Keeping in view all the basics of blockchain, it can be claimed that IoT can significantly benefit from blockchain functionalities. We have highlighted only a few (among many) improvements that are the basic causes behind integration of blockchain technology in IoT applications.

- **Decentralized Nature:** The decentralized nature of blockchain-based IoT systems will eradicate certain issues of centralized architecture such as bottleneck and centralized failure point [55]. It will also prevent situations in which few controlling companies have power and they control the storage and processing of a data of large amount of people.
- **Security:** The transactional information of IoT applications will remain secure, because all transactions are protected using cryptographic encryption [56]. In blockchain-based IoT systems, data exchange through devices can be dealt as a transaction, which in turn will secure the data.
- **Immutable and Reliable:** The immutable nature of blockchain-based IoT systems develops the trust of particpants, as they can backtrack and verify any transaction without any risk of tampering [57]. Moreover, this property do also enhances traceability of IoT sensors' data.

- **Identity:** In blockchain-based IoT systems, data from each device can be tracked easily as unique identifiers for every device are used. Similarly, trusted distributed authorization and authentication services can also be provided using blockchain in IoT systems [58].

3. Privacy issues in blockchain-based internet of things: Issues and attacks

Blockchain-based IoT systems are well-known for secure and immutable transactions. Certain encryption and authentication strategies are being used in blockchain-based IoT systems to ensure security of data. These security services of blockchain are implemented using various key encryption schemes, in which all nodes of the network have their private key along with the public key via which they manage transactions in the network. These strategies do only serve the purpose to protect transaction security, but on the other hand, the privacy of blockchain-based IoT systems do also needs considerable protection. In [27], S. Nakamoto discusses that privacy leakage of blockchain users can be a threat as if personal identity gets leaked in any transaction, then this can lead to leakage of all transaction details of same person. In this section, we first present the motivation of privacy preservation in blockchain-based IoT systems and later on we present certain privacy attacks that can be harmful for such systems.

3.1. Motivation of privacy preservation in blockchain-based IoT systems

Generally, blockchain is a public ledger in which everything is easily accessible by every blockchain member. In [27], S. Nakamoto discusses that privacy leakage of blockchain users can be a threat as if personal identity gets leaked in any transaction, then this can lead to leakage of all transaction details of same person. Moreover, the availability of transactional record on public ledger can also lead to leakage of private information such as amount of transactions carried out between two specific users. Thus, the privacy protection parameters of blockchain-based IoT systems can be categorized into two major types named as (*i*) IoT user identity privacy preservation and (*ii*) Transactional privacy preservation among IoT nodes. In this subsection, we will discuss these two in detail.

3.1.1. IoT user identity privacy

In a blockchain-based IoT network, all nodes connected in a decentralized manner, and information is uniformly distributed via ledger. However, the identity of IoT users can easily be cracked using various strategies. E.g., studies using behaviour analysis strategies (such as anti-money launder (AML) [59] or know your customer (KYC) policy [60]) over blockchain have shown that these strategies can be used to easily reveal personal information and identities of blockchain users [26]. That who is using blockchain for what specific purpose, thus modern blockchain-based IoT systems need to be capable of preserving the privacy of its users.

3.1.2. Transactional privacy

Maintaining the uniformity of ledger by updating it after every IoT node transaction is one of the most critical phenomenon of blockchain-based IoT systems, however updating the information without considering the privacy protection can lead to leakage of transactional privacy. Information regarding the transaction, or exchange of information from a specific node to another one can easily be tracked by analysing transactional graphs via some attacking techniques [61]. Therefore, the ledger needs to be updated by keeping in view the minimum privacy requirements that does not allow the leakage of privacy among blockchain-based IoT users.

3.2. Privacy attacks

Privacy protection in blockchain-based IoT networks is a critical issues because privacy can easily be breached using certain attacks, discussion about few attacks are provided in this section:

3.2.1. Address reuse

An important aspect that causes leakage of privacy in blockchain network is address reuse. Public addresses of blockchain users are open to anyone in the network and any adversary can easily get access to these addresses via Internet access. Sometimes the privacy is protected by using pseudonym addresses that do not necessarily have link with actual identities, but still pseudonymity do not provide complete protection as certain methods can be adopted to link blockchain data with original owner [62]. Once adversary successfully links the address with original identity, every transaction or information exchange of that particular user becomes visible to adversary, which is a big loophole in privacy requirement of blockchain-based IoT systems.

3.2.2. Deanonymization analysis using graphs

A complete anonymous transaction in blockchain is not possible without any specific privacy preservation strategy. Generally the digital currencies such as Bitcoin generates multiple addresses of a single user and only stores their mapping information in order to prevent linkability. Researchers identified multiple public addresses can be linked to infer and reveal identity of Bitcoin users using detailed analysis process [61]. One of such process is named as blockchain analysis, in which transaction, address and entity graphs are used to reveal original identities of blockchain users [63]. In this method, flow of transaction, relationship among different outputs and inputs, and grouping of addresses is used to diagnose actual user information respectively.

3.2.3. Wallet privacy leakage

In order to overcome issue of address reuse, some researchers proposed wallets for blockchain-based IoT transactions. In this strategy, temporary addresses are used in every data exchange and the address is disposed after each transaction. A software named as "Wallet" should be used to handle generation, and disposing of addresses that handles the addresses transparently and do not make it hectic for users. However, researches showed that this concept of wallet do also reveal privacy of blockchain-based systems when different outputs and inputs are combined in the wallet to complete single transaction [10].

3.2.4. Sybil attacks

One of the major attack to consider in blockchain-based IoT systems is sybil attack. In this attack, adversaries try to create a large number of fake IoT user nodes and try to gain large influence in blockchain network [31]. As discussed in Section 2.1, more than 50% of majority nodes or mining power is required to control network in case of public blockchain PoW consensus. Therefore, adversary try to create as much fake identities as they can so that they can control the blockchain and intrude into personal data of other users. Researchers are working to overcome sybil attacks by using various modern algorithms such as NetFLow [64]. However, researches still needs to be carried out in order reduce hazards of this attack in blockchain-based IoT systems as this attack may cause strong privacy leakage once the blockchain gets compromised.

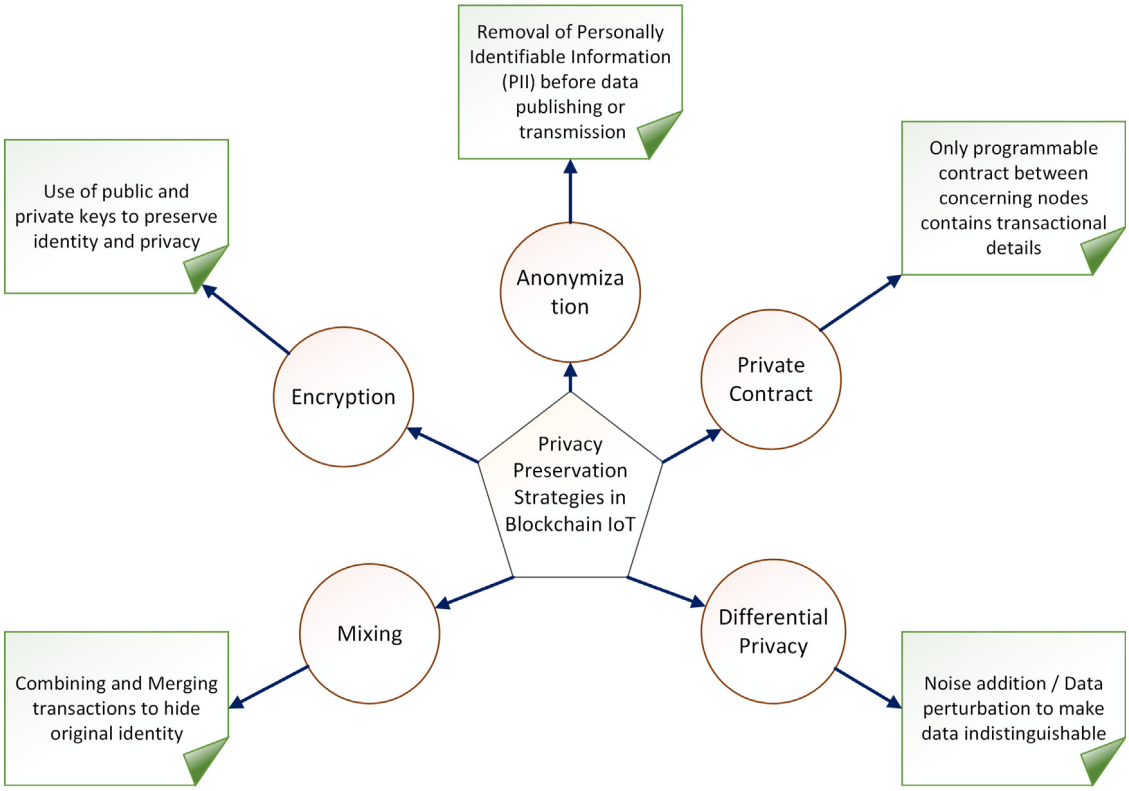

Fig. 2. Privacy preserving strategies of blockchain-based Internet of Things (IoT) systems discussing their working phenomenon according to IoT environment.

3.2.5. Message spoofing

In general terms, message spoofing is linked with forgery of a message in the network in order to disseminate false information in the network [65]. Similarly, in blockchain-based IoT networks, spoofing reference to a phenomenon in which the attacker node tried to disseminate fake message via broadcast in order to reduce the security, safety, efficiency, and privacy of blockchain network [66]. For example, in a vehicular blockchain network, a malicious electric vehicle connected to the network finds out the traffic accident happened over a busy highway, but keeps on broadcast the message to the network that "The highway is clear for traffic!". An important phenomenon over here is the detection of such attacks without breaching the privacy and private information of such vehicles. Thus, timely detection, and prevention of such attacks that can lead to severe circumstances needs to be carried out along with considering their privacy requirement.

3.2.6. Linking attacks

Linking attack is more inclined towards IoT stored data, external data is combined with protected/anonymized data in order to infer personal information [67]. Similarly, in context of distributed blockchain-based IoT networks, linking attacks can be carried out over distributed ledger that contains copy of transactions. For example, an anonymized data collected from two separate blockchain databases having records of same individuals; basic re-identification can be carried out by using various linking algorithmic attacks. Therefore, even anonymized data is not 100% safe, so strong privacy protection needs to be maintained while publicizing blockchain private data.

As we discussed in this section, that information over blockchain-based IoT network is public, similarly, every blockchain IoT user is identified using its hash value or public key, which shows that privacy protection is not guaranteed in blockchain-based IoT systems and any third-party can infer transactions or identities [10,68]. Furthermore, IoT devices do also contain and store different types of private information whose requirements of privacy vary from country to country [11]. Therefore, preserving IoT devices privacy require totally different needs as compared to traditional blockchain applications. Because in online payments of traditional blockchain applications, only transaction amount and identities require privacy. While in IoT applications of blockchain, many parameters needs to be preserved before publicizing any information. Keeping in view all these aspects, it can be concluded that privacy preservation of blockchain-based IoT systems is important, and these systems require certain privacy protection strategies to protect individual and device privacy.

4. Privacy preservation strategies of blockchain-based IoT

As discussed earlier that privacy is not pre-enforced in the design of blockchain-based IoT systems and private user data can be leaked by using certain attacking strategies. In order to overcome similar issues, researchers proposed various privacy preservation strategies for different applications of blockchain-based IoT systems. We divide privacy preserved applications on the basis of five privacy preservation approaches as classified in Fig. 3. Similarly, a brief functioning of these privacy preservation strategies is given in Fig. 2. In this section, we discuss the implementation of five most popular privacy preservation strategies in context of different blockchain-based applications of IoT. In order to evaluate the level of privacy protection from a technical perspective, we used certain metrics and parameters to compare these approaches. The detailed description of these privacy preservation parameters along with their comparison is provided in Table 2.

4.1. Encryption

Encryption strategy is widely used in almost every blockchain network for secure transactions and data transmissions. Every

Table 2
Comparative view of privacy preservation techniques in blockchain-based internet of things applications with their specific technique, optimized parameters, and experimental platform.

Main Category	Sub-Domain	Ref No.	Mechanism Name	Privacy Technique Used	Privacy Enhancement	Key Contribution	Overcome Attacks	Consensus	Platform Used
Encryption	Vehicular Networks	[66]	PKI in vehicles	Discussed usage of public key as identifier	• Vehicle identity	Joint consensus to ensure timeliness	• Message spoofing	Joint PoW & PoS	N/A
	Wearable Body Networks	[69]	Public Key Recovery	Key recovery protection and management algorithm developed	• Real-time privacy • Backup data privacy	Distinguished key encryption	• Statistical	PoW	N/A
Private Contract		[70]	ShadowEth	Only invocation & verification information is publicized	• Execution, specification, and state privacy of smart contracts	Off-chain trusted execution	• Deanonymization	Proof of Elapsed Time	N/A
	Finances	[71]	Hawk	Mint & Pour privacy protection used	• Transactional privacy • Money spending privacy	ZKP encryption for on-chain privacy	• Front running	PoW	N/A
	Electric Vehicles	[72]	BARS	Anonymous certificate authentication is used	• Vehicle identity privacy	Preventing forged messages	• Message spoofing	PoW	N/A
Anonymization	Electric Health Record	[73]	Bilinear pairing	Anonymous IDs & common secret keys are used	• Patients identity • Location of change	Information safety & confidentiality	• Sybil	PoW	N/A
		[74]	BSPP for consortium blockchain	Pseudo identities are used	• Patient's original identity	Searchable data confidentiality	• Sybil	Proof of Conformance	N/A
		[75]	ZeroCoin	Used anonymity to prevent linking data	• User privacy in public log	Transactional graph preservation	• Sybil	PoW	N/A
	Finances	[76]	ZeroCash	Non-iterative knowledge arguments are used	• User identity	Prevent public transaction leakage	• Double spending	PoW	ZK-Snark
		[77]	FICA	Privacy preserving range query is implemented	• Traceability • Auditability	Conditionally anonymous traceability protection	• False reporting	PoS	Miracl
	Vehicular Networks	[78]	CreditCoin	Threshold ring signature and incentive phenomenon	• Vehicular identity	Anonymous announcement in a non-trusted environment	• DoS • Sybil	PoW	Polar SSL
	Energy Systems	[79]	PriWatt	Multi-Signature proof-of-concept phenomenon used	• Identity preserving during bidding, negotiation, and transaction	Anonymous message stream for trading & negotiation	• Double spending • Sybil • DoS	PoC	Python
Mixing		[80]	CoinShuffle	Mixing and shuffling transactions carried out	• Unlinkability • Verifiability	Prevent internal unlinkability	• Double spending • DoS	PoW	N/A
	Finances	[81]	MixCoin	Application of sequential mixing	• Transactional privacy	Signature based accountability	• Data linking	PoW	N/A
Differential Privacy	Healthcare Systems	[82]	Differential perturbation	Discussed perturbation of private data	• Patients' identity	Highlighted use of perturbed differentially private data	• Man in the middle	Contract based	N/A

user in blockchain network do receive different keys, one type of key is public key that is to be used by the other blockchain users in order to send the message to this specific node, and one private key to decrypt and read only the desired messages. This encryption and decryption phenomenon protects individual message and transaction privacy of blockchain transactions. Taking a step further, researchers discussed that advanced encryption strategies can also be used to preserve privacy at certain level.

4.1.1. Vehicular networks

One important application blockchain-based modern ITS are vehicular networks in which every vehicle is connected with each other using wireless medium operating over blockchian, and this communication is generally known as V2V communication. These vehicular networks require privacy protection because of sensitive data of owner or driver. Thus, encryption based strategies can be a possible solution in order to preserve their privacy. Yang et al. in [66] discussed privacy preservation using encryption in vehicular IoT networks based on blockchain technology. The authors suggested that identifying vehicles on the basis of their pubic key value can be a possible solution to protect vehicular privacy, as public keys act as a meaningless string and they can easily be changed after their interaction with road side units in a vehicular network. Thus, once the public key of any electric vehicle gets changes then it is hard for any adversary to track the owner identity even in a public blockchain network. Generally the encryption mechanism increases network overhead and is time consuming, in order to overcome this issue and increase timeliness of blockchain network, the authors used joint consensus mechanism and merged PoW and PoS in a combined consensus. Furthermore, the authors tried to overcome message spoofing attack by using the concept of public key identity property of their designed mechanism. Thus, it can be concluded that the authors can easily overcome issues that can be cause by the mentioned adversaries such as malicious vehicles and compromised roadside units.

4.1.2. Wearable health devices

Encryption based strategies can also be used to protect privacy of wearable devices that are connected with each other via blockchain network. Wearable devices mainly constitute smart watches, real-time heartrate monitors, real-time blood pressure monitors, etc. These devices are attached with patients' body and report real-time values to concerning authorities such as doctors, hospitals, and medical coaches. In order to protect this private information from getting into wrong hands, encryption enable and ensure the correct recipient of information. A work over encryption based protection is done by Zhao et al. in [69] in context of healthcare IoT systems. The basic purpose of proposed strategy was to develop a distinguishable key encryption strategy in wearable body blockchain network. In order to do so, the authors first highlighted that data in a health blockchain is public and any adversary (such as attacking blockchain controller or body sensor node) can get access to private data of patients that can be harmful threat for someone's privacy. Furthermore, the idea of protecting user privacy in body sensor networks is implemented by authors using encryption key management. In proposed approach, body sensor first receives physiological signals from the surrounding, produces a private key that only the user knows and then broadcast the signal to hospital. The privacy preservation acts in such a way that even the hospital cannot decrypt the signal without patients' permission because only patient knows private key and thus the decentralized stored patients' data get protected from various statistical privacy attacks.

Weaknesses of encryption:

Encryption provides a strong privacy and security guarantee, however, the encryption based privacy preservation increases the computation and communication overhead of the blockchain-based IoT networks. As, in case of strong encryption and decryption, nodes require heavy computational power to generate and distribute keys accordingly which in turn will cause an immense increase in overhead. Moreover, encryption strategies can also be compromised by finding loop holes in the mathematical formulation of encryption that may lead the breaking of cipher and can leak the complete data privacy. Solution to this problem can also lead to formation large sized public keys which also turns out to be another obstacle as it increase computational overhead of network [83]. Therefore, the trade-off between privacy and computational overhead needs to be maintained first while applying encryption in blockchain-based IoT systems.

4.2. Smart contract

The name "Smart Contract" can be traced back to the year 1996, in which Szabo proposed a smart contract based upon set of promises and protocol in order to remove third party interference [84]. However, blockchain technology made this concept of smart/private contract possible because of its decentralized nature. In smart contracts based blockchain, the transaction details are not stored over blocks, instead a smart contract is written that contains all data and information related to transaction. Smart contract is like a programmable code operating over blockchain that IoT nodes can write according to the requirement of transaction, and then they can execute the contract into blockchain network [85]. Once the contract gets deployed in the blockchain, it start execution and then no IoT user can stop this execution, not even the creator of code. A graphical demonstration of smart contract based vehicular networks and financial system is given in Fig. 4.

4.2.1. Financial data

Interest in blockchain-based financial IoT systems are increasing rapidly because of their modern features such as transparency and tractability. The transactions carried out in these blockchain-based systems has large amount of private information that requires protection. Smart contract based financial transactions is termed as a considerable solution to overcome certain issues. Thus in literature, researchers worked over integration of smart contract in financial applications of IoT operated over blockchain. The authors in [70] used private smart contract named as "ShadowEth" to protect financial transaction privacy along with enhancement of off-chain trusted execution of smart contract. The proposed smart contract based model runs in such a manner that even after execution of smart contract at every blockchain node, the malicious users will not be able to infer any private or critical information. The authors first deployed the smart contract in public blockchain to enhance privacy, then they presented a hardware enclave system to ensure contract confidentiality. Authors claimed that ShadowEth provided a secure and confidential platform that is protected by using trusted execution environment of blockchain to store and execute smart private contracts. Only the verification of transactions are placed over blockchain instead of complete transaction detail. In this way, the authors protected execution, specification, and state privacy of smart contracts in decentralized financial IoT systems. The authors worked over protection from deanonymization attack, and thus proposed their own consensus mechanism named as "proof of elapsed time", which enhances the timeliness, privacy, and

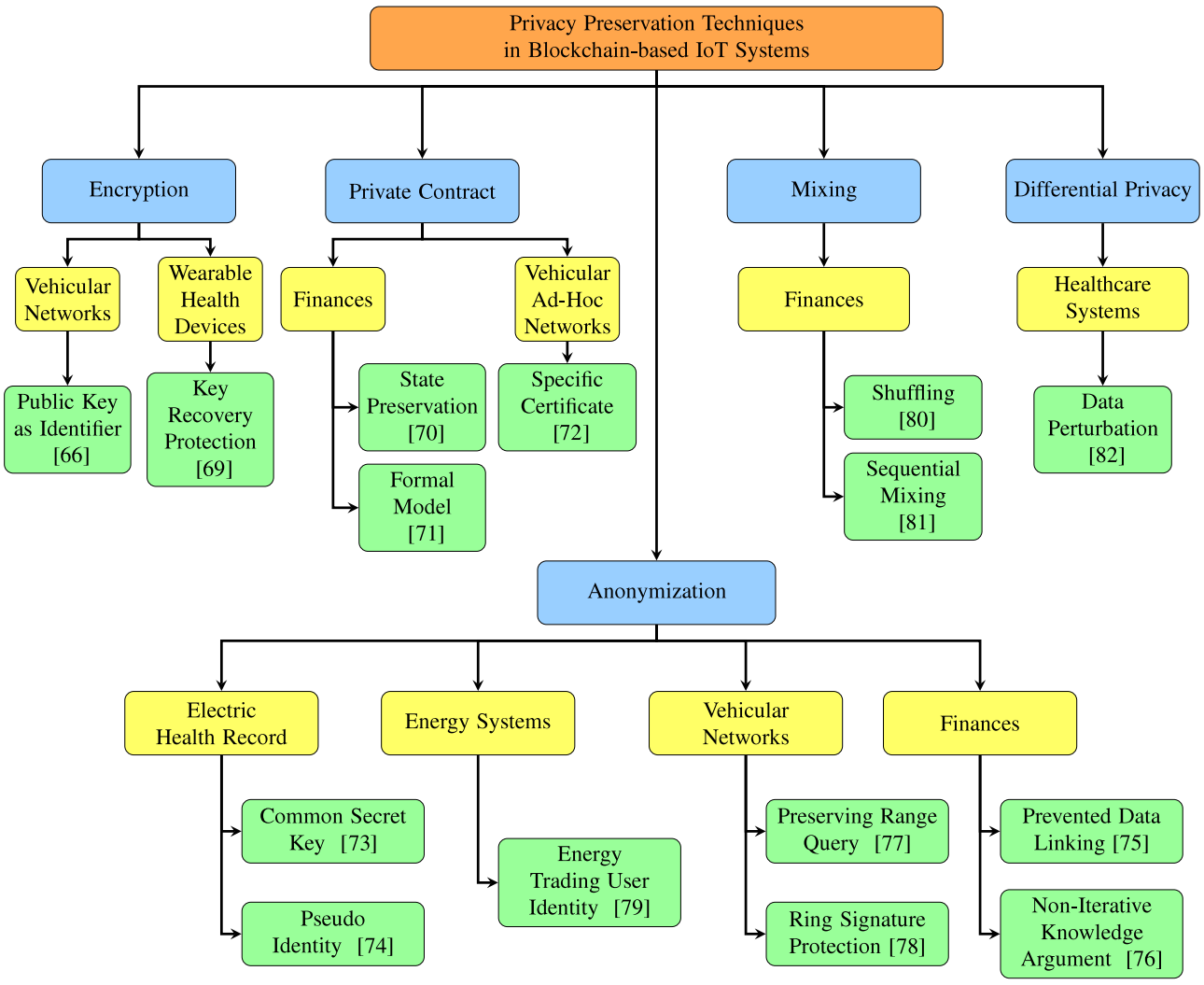

Fig. 3. Privacy Preservation Strategies in Blockchain Technology can mainly be classified into anonymization, encryption, private contract, mixing, and differential privacy.

security of blockchain network. Furthermore, another smart contract based strategy named "Hawk" was presented by Kosba et al. in [71] to protect user transactional privacy in public blockchain environment. Hawk works over a decentralized system of smart contracts that do not store financial transaction details on blocks of blockchain. The proposed mechanism uses the concept of zero knowledge proof for on-chain privacy, which ensures that no front running attack or adversary can access private information of blockchain nodes. Thus, no adversary in the network can infer identities of users who were involved in the transaction, and only the participants have access to complete information that contains details of transactions and money spent.

4.2.2. Vehicular ad-hoc networks

Smart vehicles are future of ITS because they are fully autonomous, intelligent, and environment friendly vehicles. In blockchain-based vehicular ad-hoc networks (VANETs), these vehicles are continuously communicating with each other and are updating their real-time information using distributed ledger technology of blockchain. This data can contain personal information such as location of car that requires certain level of protection. Controlling privacy of information along with its real-time reporting can be done by using modern smart blockchain contracts. Lu et al. in [72] implemented smart contract privacy preservation in blockchain-based VANETs. The proposed strategy named "BARS" protect vehicles against different tracking attacks that try to break location of vehicles using their broadcast messages. The authors used trusted certificates in order to prevent linkability between public keys and actual identities. Furthermore, a trust model on the basis of reputation of VANET user is formulated that efficiently enhances and elaborates trustworthiness of broadcast message. The presented mechanism ensures that no forged broadcast get approved by PoW consensus mechanism, thus protecting the complete blockchain network from network spoofing.

Weaknesses of smart contract:

Although the smart contracts are autonomous, safe, and precise way of transaction in IoT applications, but the involvement of third party cannot be completely eradicated in context of smart contract. As, sometimes the users might need IT experienced people in order to write efficient programs or a fresh user can do some clerical errors that may endanger the whole transaction. Moreover, the implementation, consensus, distribution, and storage cost of smart contracts can also not be neglected, as it is essential for every node to store and broadcast the smart contract after every successful consensus.

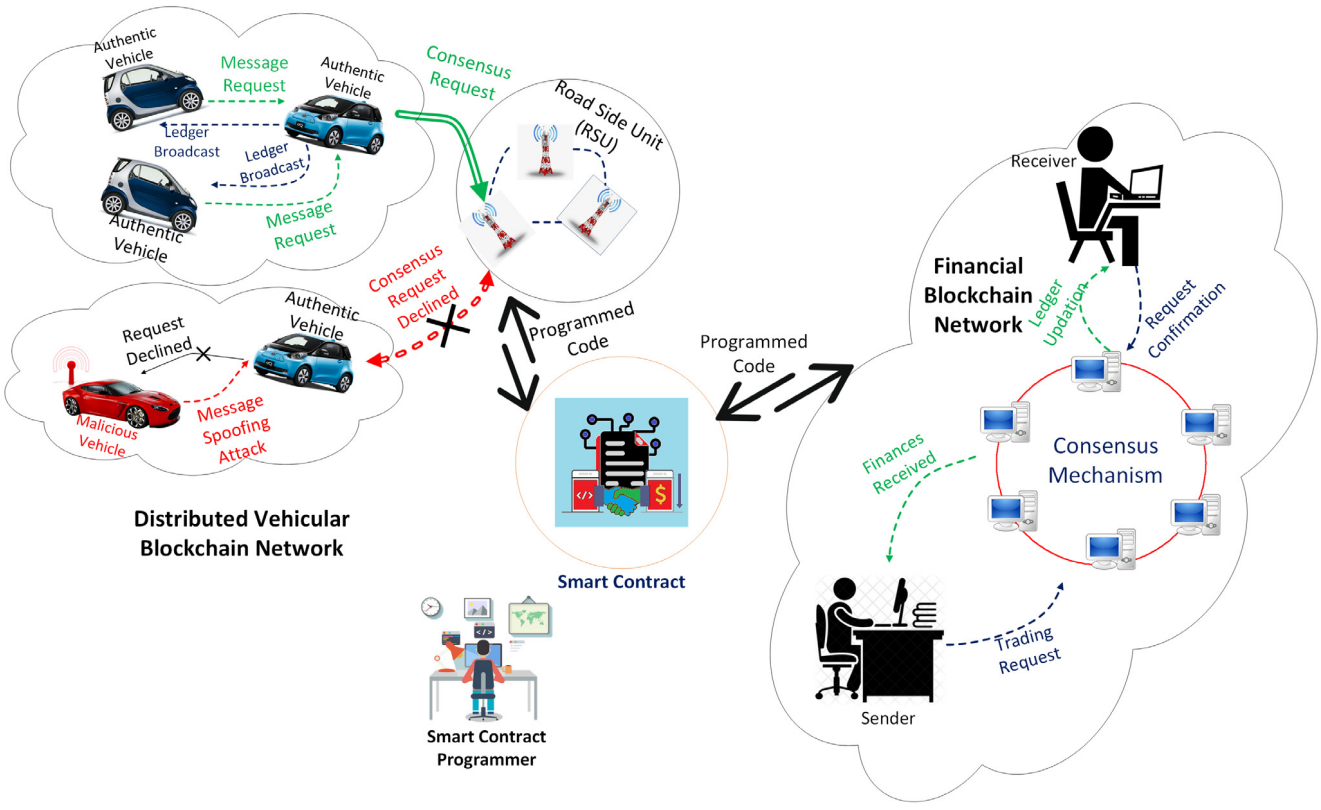

Fig. 4. Smart Contract based privacy preservation in Vehicular Ad-Hoc Networks and Financial Network Operating over Blockchain.

4.3. Anonymization

Anonymization is a famous method to preserve privacy in IoT based systems. Many researchers have applied anonymization techniques to protect privacy of blockchain-based IoT applications. Some common applications include electronic health record, finances, vehicular networks, and energy systems. There are various anonymization strategies such as *k-anonymity* [86], *t-closeness* [87], and *l-diversity* [88] proposed by researchers to make anonymization stronger. The detailed discussion about these strategies of anonymization is out of scope of this article, interested readers can read work presented in [89]. In anonymization, personal identifiable information (PII) is identified in the data and these PIIs are then protected using various anonymization strategies. For example in case of electronic health data, the patients' identity is the most important PII that is preserved first. Similarly in finances, the identity and transaction amount requires protection. So, PII varies according to the scenario of installed application. After identification of PIIs, the next step is to remove these PIIs from dataset in such a way that no adversary will be able to get the information about hidden data. After successful anonymization, the data is further presented or sent to desired destination.

4.3.1. Electronic patient record

In blockchain-based IoT systems, anonymization is applied over various field to protect different PIIs and electronic patient record is one of them. In such records, the complete record of patient is usually stored in order to access and verify any detail about tests or medications at any instant of time. For instance, the record of patient from its first day of admittance in hospital to its discharge, containing all medications and medical test results are stored in such records. Protection of such data is extremely important as it contains private information that can be used for various adversarial purposes such as blackmailing, etc. Thus anonymization provides a feasible approach to hide identifiable information from intruders. For example, the authors in [73,74] anonymized electronic health (e-health) data to protect patients privacy. In [73], Wu et al. used the concept of bilinear pairing to protect identity and location of patient. They took a step further, and prevented location leakage during communication and message transmission among patients. Similarly, the authors prevented blockchain data from sybill attacks and preserved information safety. In order to do this, the authors used anonymous ID and protected these IDs using common secret keys with PoW consensus mechanism. The proposed concept enhanced confidentiality of message and achieved untraceability in e-health hospital records. Moving further to the next scenario, the authors in [74] proposed a BSPP protocol to protect data of consortium blockchain-based e-health system. The authors identified that identity leakage of patients can cause various harmful effect and thus emphasized over protection of original identity. In order to protect identity, authors used the concept of pseudo identities as an evidence for conformance proof. Such strategy is developed in which only the designated doctor is able to check pseudo identities of patients, and any adversary cannot trace the actual identities. In this paper, authors considered hospital server and outside eavesdropper as an adversary and protected the data from sybil attack using the provided mechanism. Furthermore, the presented algorithm do also provide searchable confidentiality in which the hospital staff can search from patients data without inferring private information. Another important aspect of the presented paper is its unique consensus mechanism named as "proof-of-conformance" in which the patients registers for a specific doctor in the hospital, and the doctor generates the PHI records of patients and encrypt keys and protect it using pseudo identities.

4.3.2. Financial transactions

Another important application of blockchain-based IoT is finance industry. Financial transactions contains certain PIIs that can lead to leakage of private information and can lead to identification of sender or receiver of certain transaction. Protecting such information before carrying out any transaction is important for blockchain-based financial service providers. For protection of financial blockchains, researchers proposed two anonymization based strategies named as ZeroCoin and ZeroCash. Both anonymization based cryptocurrencies try to prevent personal transactional data leakage using the concept of zero-knowledge proof. In [75], the authors presented an anonymous transaction strategy named as ZeroCoin. In ZeroCoin, the identity of payee, receiver, and transactional amount is preserved by anonymizing certain PIIs. The goal of strategy is to preserve identify and remove data leakage during linking data. The authors further prevented the information leaking the spent cash, and stated that spent information can be a potential information source for attackers. ZeroCoin also claims that its transactions are completely private and cannot be traced back using transactional graph reading mechanisms. Similarly, Saason et al. proposed ZeroCash as a new version of private transactional cash for blockchain-based financial systems. Non-iterative knowledge arguments are used to protect traceability and user identity in the transactional data. Furthermore, the authors claimed that ZeroCash successfully protects transaction amount, identities, and users' account balance in a public blockchain along with prevention from double spending attacks.

4.3.3. Vehicular networks

Vehicular networks are also an important application of blockchain-based IoT systems that included the interconnection and information sharing among vehicles using distributed ledger technology. Protecting data using anonymization is also implemented in vehicular network scenario in which authors integrated blockchain IoT with fog computing [77]. First the authors introduced fog computing as a solution to latency, and demonstrated that fog computing can cause latency issues but on the other hand it raises certain privacy and security concerns as well such as false reporting attacks. In order to solve these attacks and privacy issues, the authors proposed a carpooling scheme named as FICA. The strategy focused mainly over protection individual privacy in case of query evaluation. Thus a privacy preserving range query algorithm is implemented that protects the data from traceability and auditability. The authors ensured safe query evaluation along with conditionally anonymous traceability in PoS consensus and demonstrated that both internal and external adversaries will not be able to trace identities of users from protected data. Another work in vehicular network considered to protect network announcements of vehicles interlinked with each other [78]. The authors first discussed that forwarding announcements in a vehicular network can reveal identities using sybil attacks, and then discussed the motivation of users regarding the announcement forwarding. In order to overcome these two aforementioned issues, authors proposed a privacy preservation strategy named as CreditCoin. In first step, the authors ensured vehicles that transmission of messages using blockchain network will not leak their privacy because of ring signature anonymized announcements. Furthermore, users were motivated to share their traffic details in order to get incentives from the network via PoW consensus mechanism.

4.3.4. Energy systems

The trend of development and implementation of blockchain-based IoT energy systems are increasing rapidly. Energy utilities are using the concept of blockchain to efficiently trade the energy between the buyers and suppliers. This trading can lead to leakage of identities of buyers and sellers which is a serious threat to privacy of such system. In [79], a multi signature, blockchain based system is developed to efficiently trade energy between various micro-grids without the need to trusted third party. However, this trading raises certain privacy issues in the network and identities can be disclosed using similar method. Therefore, authors worked over anonymous P2P messaging streams to protect micro-grid users' identities during their communication. The proposed strategy efficiently anonymize identities during energy price negotiation and during trading transactions using proof-of-concept (PoC) consensus mechanism. In doing so, the authors protected the smart grid environment from double spending, sybil, and DoS attacks.

Weaknesses of anonymization:

Anonymization provides a strong privacy guarantee to most of blockchain-based IoT systems, but they are also prone to certain type of attacks. One of the major attack against anonymized data is linking attack, in which the data from external sources is combined with the protected anonymized data to obtain critical data of IoT users [90]. Similarly, anonymization does not guarantee 100% privacy as the chances of disclosure are always there because it is not possible to obtain a specific definition of PII, as PII may vary from case to case. Moreover, anonymization also limits the details of records to a certain extent, and sometimes the analyst/receiver is not able to extract required useful information from an anonymized dataset. Another important issues to highlight in here is missing linkability in combined datasets obtained from big data application. Two similar data sets are anonymized in such a way that they are no more useful for big data organization, as the linkability between them is removed and the original data is lost [91]. Thus keeping the original records searchable and linked while anonymizing data for privacy preservation is also a potential problem. Therefore, researches needs to carry out to make anonymization more efficient and untraceable in blockchain-based IoT system.

4.4. Mixing

Coin mixing protocols were introduced to facilitate anonymity in financial transaction of blockchain-based IoT systems. Traditional mixing approaches were not totally decentralized and transactions are usually carried via trusted third-party servers that take inputs of transactions from different users and intermix the transactions to hide the value and identities from adversaries. In transactions of mixing phenomenon, every blockchain IoT user transmits its encrypted fresh address to the mixer (third-party), which afterwards decrypts and shuffles the addresses randomly and send it back to transmitter nodes [92]. However, recent mixing strategies do not require involvement of third-party for mixing. In context of financial IoT blockchain transactions, CoinShuffle, and Mixcoin protocols were developed by researchers to protect individual privacy. In [80], CoinShuffle strategy was proposed by Ruffing et al. to practically decentralize financial transactions of Bitcoin. The strategy ensured the removal of third-party and carried out mixing by maintaining the decentralized nature of blockchain. CoinShuffle works over the phenomenon of accountable anonymous communication within a blockchain network. The authors focused to develop a strategy in which they preserved traceability, verifiability and internal linkability from transaction data by mixing transaction details without third-party interference. The authors used PoW mechanism with mixing protocol to protect double spending, and DoS attacks from active network attacks in the blockchain environment. Similarly

in [81] the authors proposed Mixcoin strategy for anonymous accountable financial transactions. The strategy works over the phenomenon of sequential mixing, in which splitting and mixing of transactions are carried out according to the sequential state of users. The proposed strategy ensured transactional privacy so that no adversary will be able to infer personal details of any blockchain user. The technique further used signature based accountability that prevents data linking attacks over the blockchain data and thus preventing any sort of global passive adversary from inferring into personal information.

Weaknesses of mixing:

Mixing approach works well in case of financial transactions, but the anonymity level of mixing protocols is low and can be compromised easily as they are prone to intersection and sybil attacks [63]. Similarly, mixing approaches do not guarantee complete privacy as the transaction can also be backtracked by analysing transactional graphs that may lead to breakage of privacy of each transaction. Therefore, efficient mixing protocols needs to be developed in order to overcome these challenges in financial IoT systems.

4.5. Differential privacy

Differential privacy is an efficient privacy preservation strategy to maintain the confidentiality of data without risking its leakage. C. Dwork first introduced the concept of differential privacy by presenting a mechanism that effectively protect database privacy by adding noise during query evaluation [93]. This concept strengthened further and many researchers started applying different variants of differential privacy in daily life applications. Currently, researchers are developing various differential privacy based IoT systems, which works over the concept of data perturbation in real-time and dynamic environment [94]. Similarly in context of blockchain-based IoT systems, differential privacy based data perturbation mechanism can be used to protect IoT nodes data.

4.5.1. Healthcare data

Hospitals and medical centres keep patients' data for the sake of record and future medical precautions. The trend of decentralized storage of healthcare records is increasing dramatically because of ease of access. However, the transparent nature of these decentralized blockchain systems may cause leakage in patients' privacy. Thus, differential privacy protection can be an effective way to protect such data from intruders. In [82], Dagher et al. highlighted that data perturbation mechanism of differential privacy can be used to preserve privacy of their blockchain-based health system mechanism. Furthermore, they discussed that differential privacy strategy can efficiently add noise in health transactions so that any adversary analysed may not be able to infer any critical information from stored data using man-in-the-middle attacks. Therefore, they suggested that integration of differential privacy can be a valuable approach to protect blockchain-based IoT systems privacy.

Weaknesses of differential privacy:

Differential privacy is a lightweight privacy protection strategy that can easily be implemented in various blockchain-based IoT systems, however, this lightweight privacy preservation strategy do also comes up with certain weaknesses. One major concern regarding differential privacy is its trade-off between accuracy and privacy which is directly linked with its data perturbation mechanism. As to enhance the level of privacy one increases the amount of added noise, but on other hand this noise addition can lead to severe loss of accuracy and precision in the data [95]. Therefore, a healthy trade-off between privacy and accuracy is required while perturbing the data using differential privacy noise addition mechanism. Thus, efficient differential privacy strategies that enhances privacy level along with this reduction of this trade-off are required in future blockchain-based IoT systems.

Keeping in view all the above discussion, it can be said that a large amount of work has previously been carried out in order to preserve blockchain-based IoT systems privacy, but it is an emerging field that still requires a lot of exploration.

5. Challenges and future research directions

Currently, blockchain implementation in Internet of Things systems and applications is facing several challenges from privacy perspective. Researchers are integrating blockchain in various IoT applications, but certain privacy preservation parameters do also need to be considered before such integration. In this section, we discuss few challenges, open issues, and future research direction from the perspective of privacy during integration of blockchain technology with different applications of IoT.

5.1. Industrial IoT

The trend of using blockchain technology in industrial IoT (IIoT) systems is increasing because of its decentralized and transparent nature [96]. For example, IIoT sensors equipped in a manufacturing plant would perform better in a decentralized environment. This is because information after every step will be transmitted to every other IIoT blockchain node by updating the decentralized ledger. Thus, the chances of failure and injury would reduce, as every sensor will be aware about its surrounding devices through decentralized updating phenomenon. However, the failure chances will reduce due to decentralization, but this advancement do also comes up with the increase in computational overhead for every sensor node. Thus, lightweight blockchain-based IIoT protocols are required for such decentralized systems. Thus, incorporating encryption privacy preservation with blockhain-based IIoT systems is fairly challenging because of its high computational cost [97]. Therefore, researches are required to develop light-weight privacy preserving encryption approaches. Furthermore, another important aspect of blockchain-based IIoT is that the suppliers and operation personals can also check the quality, accurate insight, and completion time for every manufacturing step. Thus it will increase the trust of buyers and sellers regarding the specific manufactured project. However, this advancement in blockchain-based IIoT systems comes up with certain privacy issues too. For instance, IIoT technologies are used extensively on a very large scale, therefore there are many commercial and political interests in industries [98]. Because of these sort of interests, many intruders and adversaries try to launch attacks targeting the real-time sensors and databases of IIoT system to damage or infer critical information of that industry. In previous literature, many researches are carried out to overcome certain privacy issues of IIoT systems, such as use of anonymity [99] and differential privacy [100] to preserve the integrity of data during industrial automation. However, these approaches require major amendments before integration in blockchain scenario. Therefore, privacy protection of such systems is very important, and researchers should focus over preserving privacy of blockchain-based IIoT systems.

5.2. Internet of farming things

Farming sector is being improved by the use of IoT technologies, one of the biggest example is the use of RFID in agricultural food supply chain system [101]. An IoT based supply chain included real-time reporting of process of production, processing, distribution, storage, and sales of agricultural products such as vegetables. This traceability system helps improve safety, supervision, farming, and processing standards of farming and agricultural industry. This tracing and tracking becomes more efficient when we involve blockchain technology in agricultural and farming IoT system [102]. This integration of blockchain in farming IoT systems will reduce delays and misplacement along with the eradication of intermediate dependencies. Nevertheless, this transparency and traceability has improved the quality, and freshness of products, but it also raised numerous privacy concerns. One such example is the leakage of exact location and process of any agricultural product. Adversaries can use this real-time precise data for various unauthorized purposes such as damaging a specific product at any unprotected stage or getting information regarding addition of certain ingredients in a product. Smart contract privacy preservation has great potential in blockchian-based farming IoT because of its dynamic nature. Leakage of private information during supply chain can be controlled by writing efficient codes according to the privacy requirement. Similarly, mixing strategy will also work well in farming IoT blockchain, however extracting useful information from mixed data can be a challenging task while maintaining computational complexity to a specific level. Thus, efficient privacy protection up to a certain level is required in such systems in order to avoid intruders' activity. So, future researches should consider the integration of privacy preservation strategies in these systems by focusing mainly over smart contract and mixing strategies.

5.3. Smart cities

Smart cities are considered as a complicated and complex paradigm of IoT because they aim to manage and resolve public issues by introducing ICT solution [103,104]. Smart cities are being designed to use IoT resources in the most efficient way, which will result in enhancement of service quality and reduction in operational cost [105]. To advance the concept of smart cities a bit further, researchers have started working over integration of blockchain with advanced smart city technologies. Few researchers suggested that blockchain can eradicate various security threats of smart cities because of its decentralized environment [106]. Although, blockchain is very advantageous for smart cities, but this decentralized nature also brought numerous privacy threats along with. The interconnected decentralized smart city network will generate huge amount of data from different processes and sensors, this data will be stored on decentralized blockchain databases. Since blockchain is a public network, so the risk of private data leakage is very high. Any intruder can join public blockchain of smart city and may try to obtain and infer critical information regarding personal lives and behaviours of smart city residents, thus resulting in serious privacy issues. Privacy protection in blockchain-based smart cities cannot easily be categorized into few predetermined domains [107]. However, certain techniques such as differential privacy, anonymization, and smart contract can widely be used for various smart city applications because the major requirement is to protect the data exchange between different processes. According to the perspective of light-weight privacy protection in smart cities, differential privacy comes up as one of the most viable option, as it gives strong privacy guarantee along with the control over data utility as well. Similarly, smart contracts are also considered as a futuristic technology in smart city applications working over blockchain because of their adaptable and programmable nature. However, implementation of differential privacy and smart contracts is still a challenge in future smart cities, because of limited capabilities of sensors used during smart city communication. Keeping in view all above discussion, implementation of blockchain in smart cities require proper privacy measures needs for data storage and transmission between nodes, sensors, and processes.

5.4. Mobile crowd sensing

With the increasing smart devices, a new way of sensing named as mobile crowd sensing (MCS) has been introduced, which utilizes the power of smart device users and obtain the benefit of large-scale sensing using IoT technologies [108,109]. MCS is considered to be a diverse and versatile platform that will replace the traditional infrastructure using static sensing. Certain modalities of smart devices such as GPS, air quality, audios, etc. are used by MCS systems in order to sense their accurate surroundings. This efficient MCS improves asset utilization, quality of service, product monitoring and workplace safety by reporting real-time data to surrounding devices [110]. Current MCS architecture is facing certain issues such as security and cost. In order to overcome these issues, researchers are working over development of a decentralized MCS architectures by the help of blockchain technology. Moreover, researches are being carried out to make a blockchain based reward system for MCS users [111]. However, all this development do also raises certain privacy issues, as blockchain-based MCS architecture will be open for public access and anyone can join in to transmit and receive crowd sensing information. This transparency raises the issues of anonymity for MCS users, crowd sensor is required to provide a certain level of anonymity to MCS users while still reporting the real-time data to the network. Blockchain-based crowd sensing system needs to ensure via some strong privacy protection mechanism that sensing is anonymous and no real identities of MCS user gets leaked to adversaries. One strategy to preserve privacy of MCS users is to use anonymization, in this way the original identities does not get revealed even if any adversary get access to private data. However, anonymization comes up with certain challenges such as data linking and selection of parameters which are required for privacy protection. Another potential application could be the addition of noise in MCS users' data using differential privacy protection strategy, however, maintaining the trade-off between accuracy and privacy can be challenging task in decentralized MCS environment because users are reporting their data in a real-time environment. Therefore, modern researches over blockchain-based MCS needs to focus more over time efficient, real-time, and light-weight privacy preservation strategies.

6. Conclusion

The trend of integration of Internet of Things (IoT) systems in our daily life is increasing exponentially, and it has benefited our lives in many ways. This advancement has raised certain security and authentication challenges such as mining, hacking, and service denial attacks because of centralized nature, but blockchain technology came up as an optimal way to overcome these challenges. However, blockchain-based IoT systems are also vulnerable to various privacy threats that needs to be resolved before their practical implementation. In this article, we have presented a brief overview of the importance of privacy preservation in blockchain-based IoT systems is discussed along with highlighting some attacks. Furthermore, we have extensively covered five major privacy preservation strategies being used in

blockchain-based IoT systems named as anonymization, encryption, mixing, private contract, and differential privacy. Within these privacy preservation strategies, we briefly surveyed the applications of IoT being used in our daily lives such as healthcare, finances, energy systems, vehicular networks, and wearable devices. Finally, we concluded the article by mentioning and highlighting certain challenges and future research directions in blockchain-based IoT systems.

Acknowledgment

This paper research is partially supported by Australian Research Council projects of DP170100136 and LP140100816.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: A survey on enabling technologies, protocols, and applications, IEEE Commun. Surv. Tutor. 17 (4) (2015) 2347–2376.
[2] A. Ericsson, Ericsson mobility report: On the pulse of the networked society, Ericsson, Sweden, Tech. Rep. EAB-14, 61078, 2015.
[3] L. Zhou, L. Wang, Y. Sun, P. Lv, BeeKeeper: A blockchain-based IoT system with secure storage and homomorphic computation, IEEE Access (2018) (in press).
[4] T. Wang, Z. Zheng, M.H. Rehmani, S. Yao, Z. Huo, Privacy preservation in big data from the communication perspective—a survey, IEEE Commun. Surv. Tutor. 21 (1) (2019) 753–778.
[5] Y.-A. de Montjoye, E. Shmueli, S.S. Wang, A.S. Pentland, Openpds: Protecting the privacy of metadata through safeanswers, PLoS One 9 (7) (2014) 98790.
[6] O. Novo, Blockchain meets IoT: an architecture for scalable access management in IoT, IEEE Internet Things J. 5 (2) (2018) 1184–1195.
[7] T. Salman, M. Zolanvari, A. Erbad, R. Jain, M. Samaka, Security services using blockchains: A state of the art survey, IEEE Commun. Surv. Tutor. 21 (1) (2019) 850–880.
[8] M. Pilkington, Blockchain technology: principles and applications, in: Research Handbook on Digital Transformations, vol. 225, 2016.
[9] T.M. Fernández-Caramés, P. Fraga-Lamas, A review on the use of blockchain for the internet of things, IEEE Access (2018) (in press).
[10] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G.M. Voelker, S. Savage, A fistful of bitcoins: characterizing payments among men with no names, in: Proceedings of the ACM conference on Internet measurement conference, 2013, pp. 127–140.
[11] N. Fabiano, The internet of things ecosystem: The blockchain and privacy issues. the challenge for a global privacy standard, in: IEEE International Conference on Internet of Things for the Global Community, IoTGC, 2017, pp. 1–7.
[12] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, On blockchain and its integration with IoT. challenges and opportunities, Future Gener. Comput. Syst. (2018) (in press).
[13] G.W. Peters, E. Panayi, Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money, in: Banking Beyond Banks and Money, Springer, 2016, pp. 239–278.
[14] W. Gao, W.G. Hatcher, W. Yu, A survey of blockchain: Techniques, applications, and challenges, in: IEEE 27th International Conference on Computer Communication and Networks, ICCCN, 2018, pp. 1–11.
[15] A. Brandão, H. São Mamede, R. Gonçalves, Systematic review of the literature, research on blockchain technology as support to the trust model proposed applied to smart places, in: World Conference on Information Systems and Technologies, Springer, 2018, pp. 1163–1174.
[16] T. Salman, M. Zolanvari, A. Erbad, R. Jain, M. Samaka, Security services using blockchains: A state of the art survey, IEEE Commun. Surv. Tutor. (2018) (in press).
[17] W. Ejaz, A. Anpalagan, Blockchain technology for security and privacy in internet of things, in: Internet of Things for Smart Cities, Springer, 2019, pp. 47–55.
[18] Y. Yang, Y. Yang, J. Chen, M. Liu, Application of blockchain in internet of things, in: International Conference on Cloud Computing and Security, Springer, 2018, pp. 73–82.
[19] M.A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, H. Janicke, Blockchain technologies for the internet of things: Research issues and challenges, IEEE Internet Things J. (2018) (in press).
[20] M.S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M.H. Rehmani, Applications of blockchains in the internet of things: A comprehensive survey, IEEE Commun. Surv. Tutor. (2018) (in press).
[21] J. Herrera-Joancomartí, C. Pérez-Solà, Privacy in bitcoin transactions: new challenges from blockchain scalability solutions, in: Modeling Decisions for Artificial Intelligence, Springer, 2016, pp. 26–44.
[22] M. Conti, S. Kumar, C. Lal, S. Ruj, A survey on security and privacy issues of bitcoin, IEEE Commun. Surv. Tutor. (2018) (in press).
[23] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Gener. Comput. Syst. (2017) (in press).
[24] L. Zhu, B. Zheng, M. Shen, S. Yu, F. Gao, H. Li, K. Shi, K. Gai, Research on the security of blockchain data: A survey, 2018, arXiv preprint arXiv:1812.02009.
[25] J. Wahab, Privacy in blockchain systems, 2018, arXiv preprint arXiv:1809.10642.
[26] Q. Feng, D. He, S. Zeadally, M.K. Khan, N. Kumar, A survey on privacy protection in blockchain system, J. Netw. Comput. Appl. (2018) (in press).
[27] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008, (online), http://bitcoin.org/bitcoin.pdf.
[28] A.M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, O'Reilly Media, Inc., 2014.
[29] F. Tschorsch, B. Scheuermann, Bitcoin and beyond: A technical survey on decentralized digital currencies, IEEE Commun. Surv. Tutor. 18 (3) (2016) 2084–2123.
[30] T.T.A. Dinh, R. Liu, M. Zhang, G. Chen, B.C. Ooi, J. Wang, Untangling blockchain: A data processing view of blockchain systems, IEEE Trans. Knowl. Data Eng. 30 (7) (2018) 1366–1385.
[31] J.R. Douceur, The Sybil Attack in International Workshop on Peer-to-Peer Systems, Springer, 2002, pp. 251–260.
[32] M.C.K. Khalilov, A. Levi, A survey on anonymity and privacy in bitcoin-like digital cash systems, IEEE Commun. Surv. Tutor. (2018) (in press).
[33] D. Puthal, N. Malik, S.P. Mohanty, E. Kougianos, G. Das, Everything you wanted to know about the blockchain: Its promise, components, processes, and problems, IEEE Consumer Electron. Mag. 7 (4) (2018) 6–14.
[34] Hyperledger, 2017, (online), Available: https://www.hyperledger.org.
[35] M. Castro, B. Liskov, et al., Practical byzantine fault tolerance, in: OSDI, vol. 99, 1999, pp. 173–186.
[36] G. Sachs, Blockchain–putting theory into practice, in: the-blockchain. com, 2016, pp. 25–32.
[37] J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang, Z. Wang, Consortium blockchain-based malware detection in mobile devices, IEEE Access 6 (2018) 12118–12128.
[38] Bitcoinwiki, proof of work (online), https://en.bitcoin.it/wiki/Proof_of_work.
[39] Wikipedia, proof of space (online), Available: https://en.wikipedia.org/wiki/Proof-of-space.
[40] G. Zyskind, O. Nathan, et al., Decentralizing privacy: Using blockchain to protect personal data, in: IEEE Security and Privacy Workshops, SPW, 2015, pp. 180–184.
[41] Bitcoinwiki, proof of stake (online), Available: https://en.bitcoin.it/wiki/Proof_of_Stake.
[42] Wikipedia, nem (cryptocurrency) (online), Available: https://en.wikipedia.org/wiki/NEM_(cryptocurrency).
[43] Ethereum blockchain app platform, 2017, (online), Available: https://www.ethereum.org/.
[44] K. Ashton, et al., That internet of things thing, RFID J. 22 (7) (2009) 97–114.
[45] A. Zanella, N. Bui, A. Castellani, L. Vangelista, M. Zorzi, Internet of things for smart cities, IEEE Internet Things J. 1 (1) (2014) 22–32.
[46] S.B. Baker, W. Xiang, I. Atkinson, Internet of things for smart healthcare: Technologies, challenges, and opportunities, IEEE Access 5 (2017) 26521–26544.
[47] P. Castillejo, J.-F. Martinez, J. Rodriguez-Molina, A. Cuerva, Integration of wearable devices in a wireless sensor network for an e-health application, IEEE Wirel. Commun. 20 (4) (2013) 38–49.
[48] L. Catarinucci, D. De Donno, L. Mainetti, L. Palano, L. Patrono, M.L. Stefanizzi, L. Tarricone, An IoT-aware architecture for smart healthcare systems, IEEE Internet Things J. 2 (6) (2015) 515–526.
[49] M.H. Rehmani, M. Reisslein, A. Rachedi, M. Erol-Kantarci, M. Radenkovic, Integrating renewable energy resources into the smart grid: Recent developments in information and communication technologies, IEEE Trans. Ind. Inf. 14 (7) (2018) 2814–2825.
[50] Q. Wang, X. Liu, J. Du, F. Kong, Smart charging for electric vehicles: A survey from the algorithmic perspective, IEEE Commun. Surv. Tutor. 18 (2) (2016) 1500–1517.

[51] K.-D. Kim, P.R. Kumar, Cyber–physical systems: A perspective at the centennial, Proc. IEEE 100 (Special Centennial Issue) (2012) 1287–1308.
[52] Z. MacHardy, A. Khan, K. Obana, S. Iwashina, V2x access technologies: Regulation, research, and remaining challenges, IEEE Commun. Surv. Tutor. (2018) (in press).
[53] S. Rimer, An IoT architecture for financial services in developing countries, in: IEEE IST-Africa Week Conference, 2017, pp. 1–10.
[54] V. Dineshreddy, G. Gangadharan, Towards an internet of things framework for financial services sector, in: IEEE 3rd International Conference on Recent Advances in Information Technology, RAIT, 2016, pp. 177–181.
[55] P. Veena, S. Panikkar, S. Nair, P. Brody, Empowering the edge-practical insights on a decentralized internet of things, in: Empowering the Edge-Practical Insights on a Decentralized Internet of Things, vol. 17, IBM Institute for Business Value, 2015.
[56] G. Prisco, Slock. it to introduce smart locks linked to smart ethereum contracts, decentralize the sharing economy, Bitcoin Mag. (Nov) (2015) (online), Available: https://bitcoinmagazine.com/articles/sloc-it-to-introduce-smart-locs-lined-to-smart-ethereum-contractsdecentralize-the-sharing-economy-1446746719, (Accessed: 20 May 2016).
[57] Modum, 2017, (online), Available: https://modum.io.
[58] Chain of things, 2017, (online), Available: https://www.blockchainofthings.com.
[59] P.A. Schott, Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, The World Bank, 2006.
[60] M. Gill, G. Taylor, Preventing money laundering or obstructing business? financial companies' perspectives on know your customer procedures, British J. Criminology 44 (4) (2004) 582–594.
[61] D. Ron, A. Shamir, Quantitative analysis of the full bitcoin transaction graph, in: International Conference on Financial Cryptography and Data Security, Springer, 2013, pp. 6–24.
[62] J. Barcelo, User privacy in the public bitcoin blockchain, 2014, URL: http://www.dtic.upf.edu/~jbarcelo/papers/20140704/_User_Privacy_in_the_Public_Bitcoin_Blockchain/paper.pdf.
[63] M. Conti, S. Kumar, C. Lal, S. Ruj, A survey on security and privacy issues of bitcoin, IEEE Commun. Surv. Tutor. 20 (4) (2018) 3416–3452.
[64] P. Otte, M. de Vos, J. Pouwelse, Trustchain: A sybil-resistant scalable blockchain, Future Gener. Comput. Syst. (2017).
[65] C. Günther, A survey of spoofing and counter-measures, Navig., J. Inst. Navig. 61 (3) (2014) 159–177.
[66] Z. Yang, K. Yang, L. Lei, K. Zheng, V.C. Leung, Blockchain-based decentralized trust management in vehicular networks, IEEE Internet Things J. (2018) (in press).
[67] G. Danezis, Statistical disclosure attacks, in: IFIP International Information Security Conference, Springer, 2003, pp. 421–426.
[68] R. Henry, A. Herzberg, A. Kate, Blockchain access privacy: challenges and directions, IEEE Secur. Privacy 16 (4) (2018) 38–45.
[69] H. Zhao, Y. Zhang, Y. Peng, R. Xu, Lightweight backup and efficient recovery scheme for health blockchain keys, in: IEEE 13th International Symposium on Autonomous Decentralized System, ISADS, 2017, pp. 229–234.
[70] R. Yuan, Y.-B. Xia, H.-B. Chen, B.-Y. Zang, J. Xie, Shadoweth: Private smart contract on public blockchain, J. Comput. Sci. Tech. 33 (3) (2018) 542–556.
[71] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, in: IEEE symposium on security and privacy, SP, 2016, pp. 839–858.
[72] Z. Lu, Q. Wang, G. Qu, Z. Liu, BARS: a blockchain-based anonymous reputation system for trust management in VANETs, in: 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering, TrustCom/BigDataSE, 2018, pp. 98–103.
[73] H.-T. Wu, C.-W. Tsai, Toward blockchains for health-care systems: Applying the bilinear pairing technology to ensure privacy protection and accuracy in data sharing, IEEE Consumer Electron. Mag. 7 (4) (2018) 65–71.
[74] A. Zhang, X. Lin, Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain, J. Med. Syst. 42 (8) (2018) 140.
[75] I. Miers, C. Garman, M. Green, A.D. Rubin, Zerocoin: Anonymous distributed e-cash from bitcoin, in: IEEE Symposium on Security and Privacy, SP, 2013, pp. 397–411.
[76] E.B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, M. Virza, Zerocash: Decentralized anonymous payments from bitcoin, in: IEEE Symposium on Security and Privacy, SP, 2014, pp. 459–474.
[77] M. Li, L. Zhu, X. Lin, Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing, IEEE Internet Things J. (2018) (in press).
[78] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, Z. Zhang, Creditcoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles, 2018.
[79] N.Z. Aitzhan, D. Svetinovic, Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams, IEEE Trans. Dependable Secure Comput. 15 (5) (2018) 840–852.
[80] T. Ruffing, P. Moreno-Sanchez, A. Kate, Coinshuffle: Practical decentralized coin mixing for bitcoin, in: European Symposium on Research in Computer Security, Springer, 2014, pp. 345–364.
[81] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J.A. Kroll, E.W. Felten, Mixcoin: Anonymity for bitcoin with accountable mixes, in: International Conference on Financial Cryptography and Data Security, Springer, 2014, pp. 486–504.
[82] G.G. Dagher, J. Mohler, M. Milojkovic, P.B. Marella, Ancile: Privacy-Preserving Framework for Access Control and Interoperability of Electronic Health Records Using Blockchain Technology, vol. 39, Sustainable Cities and Society, 2018, pp. 283–297.
[83] K.-A. Shim, A survey of public-key cryptographic primitives in wireless sensor networks, IEEE Commun. Surv. Tutor. 18 (1) (2016) 577–601.
[84] N. Szabo, Smart contracts: building blocks for digital markets, EXTROPY: J. Transhumanist Thought (16) (1996).
[85] D. Macrinici, C. Cartofeanu, S. Gao, Smart contract applications within blockchain technology: A systematic mapping study, Telemat. Inform. (2018).
[86] L. Sweeney, K-anonymity: A model for protecting privacy, Internat. J. Uncertain. Fuzziness Knowledge-Based Systems 10 (05) (2002) 557–570.
[87] N. Li, T. Li, S. Venkatasubramanian, t-closeness: Privacy beyond k-anonymity and l-diversity, in: IEEE 23rd International Conference on Data Engineering, ICDE, 2007, pp. 106–115.
[88] B. Zhou, J. Pei, The k-anonymity and l-diversity approaches for privacy preservation in social networks against neighborhood attacks, Knowl. Inf. Syst. 28 (1) (2011) 47–77.
[89] S. Ji, P. Mittal, R. Beyah, Graph data anonymization de-anonymization attacks and de-anonymizability quantification: A survey, IEEE Commun. Surv. Tutor. 19 (2) (2016) 1305–1326.
[90] G. Danezis, Statistical disclosure attacks, in: IFIP International Information Security Conference, Springer, 2003, pp. 421–426.
[91] V. Torra, G. Navarro-Arribas, Big Data Privacy and Anonymization, Springer International Publishing, 2016, pp. 15–26.
[92] M. Moser, R. Bohme, D. Breuker, An inquiry into money laundering tools in the bitcoin ecosystem, in: IEEE eCrime Researchers Summit, eCRS, 2013, pp. 1–14.
[93] C. Dwork, Differential privacy, in: Proceedings of the 33rd International Conference on Automata, Languages and Programming - Volume Part II, ser. ICALP'06, Springer-Verlag, Berlin, Heidelberg, 2006, pp. 1–12.
[94] C.R.G. Rodríguez, et al., Using differential privacy for the internet of things, in: IFIP International Summer School on Privacy and Identity Management, Springer, 2016, pp. 201–211.
[95] M.U. Hassan, M.H. Rehmani, J. Chen, Differential privacy techniques for cyber physical systems: A survey, 2018, arXiv preprint arXiv:1812.02282.
[96] D. Miller, Blockchain and the internet of things in the industrial sector, IT Prof. 20 (3) (2018) 15–18.
[97] P. Barbosa, A. Brito, H. Almeida, A technique to provide differential privacy for appliance usage in smart metering, Inform. Sci. 370 (2016) 355–367.
[98] X. Lu, Q. Li, Z. Qu, P. Hui, Privacy information security classification study in internet of things, in: IEEE International Conference on Identification, Information and Knowledge in the Internet of Things, IIKI, 2014, pp. 162–165.
[99] C. Yin, S. Zhang, J. Xi, J. Wang, An improved anonymity model for big data security based on clustering algorithm, Concurr. Comput.: Pract. Exper. 29 (7) (2017) 3902.
[100] C.R.G. Rodríguez, et al., Using differential privacy for the internet of things, in: IFIP International Summer School on Privacy and Identity Management, Springer, 2016, pp. 201–211.
[101] L. Ruiz-Garcia, L. Lunadei, The role of RFID in agriculture: Applications, limitations and challenges, Comput. Electron. Agric. 79 (1) (2011) 42–50.
[102] F. Tian, An agri-food supply chain traceability system for china based on rfid & blockchain technology, in: IEEE 13th International Conference on Service Systems and Service Management, ICSSSM, 2016, pp. 1–6.
[103] A. Zanella, N. Bui, A. Castellani, L. Vangelista, M. Zorzi, Internet of things for smart cities, IEEE Internet Things J. 1 (1) (2014) 22–32.
[104] H.T. Mouftah, M. Erol-Kantarci, M.H. Rehmani, Transportation and Power Grid in Smart Cities: Communication Networks and Services, Wiley, 2018.
[105] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications, IEEE Internet Things J. 4 (5) (2017) 1125–1142.

[106] K. Biswas, V. Muthukkumarasamy, Securing smart cities using blockchain technology, in: IEEE 18th International Conference on High Performance Computing and Communications, HPCC/SmartCity/DSS, 2016, pp. 1392–1393.
[107] L. Edwards, Privacy, security and data protection in smart cities: A critical eu law perspective, Eur. Data Prot. L. Rev. 2 (2016) 28.
[108] B. Guo, Q. Han, H. Chen, L. Shangguan, Z. Zhou, Z. Yu, The emergence of visual crowdsensing: challenges and opportunities, IEEE Commun. Surv. Tutor. 19 (4) (2017) 2526–2543.
[109] B. Guo, Z. Wang, Z. Yu, Y. Wang, N.Y. Yen, R. Huang, X. Zhou, Mobile crowd sensing and computing: The review of an emerging human-powered sensing paradigm, ACM Comput. Surv. 48 (1) (2015) 7.
[110] V. Pilloni, How data will transform industrial processes: crowdsensing, crowdsourcing and big data as pillars of industry 4.0, Future Internet 10 (3) (2018) 24.
[111] C. Tanas, S. Delgado-Segura, J. Herrera-Joancomartí, An integrated reward and reputation mechanism for mcs preserving users privacy, in: Data Privacy Management, and Security Assurance, Springer, 2015, pp. 83–99.

Muneeb Ul Hassan received his Bachelor degree in Electrical Engineering from COMSATS Institute of Information Technology, Wah Cantt, Pakistan, in 2017. He received Gold Medal in Bachelor degree for being topper of Electrical Engineering Department. Currently, he is pursuing the Ph.D. degree from Swinburne University of Technology, Australia. His research interests include privacy preservation, blockchain, differential privacy, Internet of Things, decentralized IoT systems, security and privacy issues, Ad-Hoc networks, cyber physical systems, smart grid, cognitive radio networks, and big data. He is a reviewer of various journals, such as the IEEE *Communications Surveys & Tutorials*, IEEE *Journal on Selected Areas in Communications*, Elsevier *Future Generation Computing Systems*, *Journal of Network and Computer Applications*, *Computers & Electrical Engineering*, IEEE *ACCESS*, Wiley *Transactions on Emerging Telecommunications Technologies*, IEEE *Journal of Communications and Networks*, Springer *Wireless Networks*, *Human-centric Computing and Information Sciences*, and KSII *Transactions on Internet and Information Systems*. He also has been a Reviewer for various conferences, such as IEEE Vehicular Technology Conference *(VTC)-Spring* 2019, Vehicular Technology Conference *(VTC)-Fall* 2018, IEEE International Conference on Communications *(ICC) - 2019*, International workshop on e-Health Pervasive Wireless Applications and Services *e-HPWAS'18*, IEEE Globecom 2018 workshop: Security in Health Informatics *(SHInfo2018)*, Frontiers of Information Technology 2018.

Mubashir Husain Rehmani (M'14-SM'15) received the B.Eng. degree in computer systems engineering from Mehran University of Engineering and Technology, Jamshoro, Pakistan, in 2004, the M.S. degree from the University of Paris XI, Paris, France, in 2008, and the Ph.D. degree from the University Pierre and Marie Curie, Paris, in 2011. He is currently working as Assistant Lecturer at Cork Institute of Technology (CIT), Ireland. He worked at Telecommunications Software and Systems Group (TSSG), Waterford Institute of Technology (WIT), Waterford, Ireland as Post-Doctoral researcher from Sep 2017 to Oct 2018. He served for five years as an Assistant Professor at COMSATS Institute of Information Technology, Wah Cantt., Pakistan. He is currently an Area Editor of the *IEEE Communications Surveys and Tutorials*. He served for three years (from 2015 to 2017) as an Associate Editor of the *IEEE Communications Surveys and Tutorials*. Currently, he serves as Associate Editor of *IEEE Communications Magazine*, Elsevier *Journal of Network and Computer Applications (JNCA)*, and the *Journal of Communications and Networks (JCN)*. He is also serving as a Guest Editor of Elsevier *Ad Hoc Networks* journal, Elsevier *Future Generation Computer Systems* journal, the *IEEE Transactions on Industrial Informatics* and Elsevier *Pervasive and Mobile Computing* journal. He has authored/ edited two books published by IGI Global, USA, one book published by CRC Press, USA, and one book with Wiley, U.K. He received "Best Researcher of the Year 2015 of COMSATS Wah" award in 2015. He received the certificate of appreciation, "*Exemplary Editor of the IEEE Communications Surveys and Tutorials for the year 2015*" from the IEEE Communications Society. He received Best Paper Award from IEEE ComSoc Technical Committee on Communications Systems Integration and Modeling (CSIM), in IEEE ICC 2017. He consecutively received research productivity award in 2016–17 and also ranked # 1 in all Engineering disciplines from Pakistan Council for Science and Technology (PCST), Government of Pakistan. He also received Best Paper Award in 2017 from Higher Education Commission (HEC), Government of Pakistan.

Dr. Jinjun Chen is a Professor from Swinburne University of Technology, Australia. He is Deputy Director of Swinburne Data Science Research Institute. He holds a Ph.D. in Information Technology from Swinburne University of Technology, Australia. His research interests include scalability, big data, data science, data systems, cloud computing, data privacy and security, health data analytics and related various research topics. His research results have been published in more than 160 papers in international journals and conferences, including various IEEE/ACM Transactions.