Differential Privacy in Blockhain Technology: A Futuristic Approach

Muneeb Ul Hassan, Mubashir Husain Rehmani, and Jinjun Chen

***Abstract*—Blockchain has received a pervasive attention because of its decentralized, tamper-proof, and transparent nature. Blockchain works over the principle of distributed, secured, and shared ledger, which is used to record, and track data within a decentralized network. This technology has successfully replaced certain systems of economic transactions in organizations and has the potential to overtake various industrial business models in future. Blockchain works over peer-to-peer (P2P) phenomenon for its operation and does not require any trusted-third party authorization for data tracking and storage. The information stored in blockchain is distributed throughout the decentralized network and is usually protected using cryptographic hash functions. Since the beginning of blockchain technology, its use in different applications is increasing exponentially, but this increased use has also raised some questions regarding privacy and security of data being stored in it. Protecting privacy of blockchain data using data perturbation strategy such as differential privacy could be a novel approach to overcome privacy issues in blockchain. In this article, we discuss integration of differential privacy in certain blockchain based scenarios. Moreover, we highlight some future application scenarios in which integration of differential privacy in blockchain can produce fruitful results.**

***Index Terms*—Differential privacy, blockchain, privacy preservation**

I. Blockchain and Differential Privacy: A Revolutionizing Integration

A. *Blockchain Technology*

Blockchain technology first emerged as a tool to manage cryptocurrency in 2008 when S. Nakamoto introduced “Bitcoin” as first P2P digital cash system using blockchain [1]. Blockchain works over the phenomenon of decentralizing the system using a shared distributed ledger, which is basically a data structure which contains transactions list in an ordered form. For instance, the ledger can record all exchanged goods in a market or can store information of transactions carried out between multiple bank accounts. After every transaction in blockchain, the information stored on distributed ledger is replicated over all the blockchain nodes [2]. The ledger is capable to store large amount of data as it usually records the entire history of transactions or changes that take place among all blockchain nodes in order to backtrack any transaction. Contrary to traditional databases that have central trusted environment or trusted third-party environment to store records, blockchain works over distributed set of nodes/users. Each individual node has information regarding the transactions being carried out in the network. Similarly, each node is linked with its predecessor node by using a cryptographic pointer, that makes the transactions and sharing of information more secure.

These decentralized system and shared ledger functionalities of blockchain also make it an optimal choice among researchers for quick, easy, more secure, and efficient way of data exchange and storage in different ways of life. Researchers are integrating blockchain technology in certain domains of everyday life. For examples, researches are being carried out to implement blockchain in real-estate, asset management, Internet of Things (IoT), healthcare, and assisting wedding scenarios. All of these applications show that blockchain is going to take over certain major daily life domains in future.

Furthermore, by considering a higher level of divisions, blockchain can be categorized into two sub domains named as public and private blockchain. However, these decentralized transactions come up with certain privacy risks and attacks that require solution before integration of blockchain in our everyday life. In this section, we present details about operation phases, types and the privacy issues in blockchain.

1) Operation Phases of Blockchain: There are certain basic phenomenon that constitute the backbone of blockchain known as operation phases. In operation phases, we discuss the consensus and mining phenomenon of blockchain.

a) Consensus and Mining in Blockchain: In order to eliminate a trusted third party or centralized entity, a specific consensus is being followed by all nodes of blockchain so that no conflict arises in future. All nodes participate in the consensus and allow the transaction in the network, the update is then replicated in the ledger and broadcast throughout the blockchain. Similarly, mining is a process to collect the transaction data, and create block to attach it to blockchain database. These blocks are also validated by all other nodes to maintain transparency in blockchain. The nodes doing mining are known as *miners*, and they use their computational power to create a block as early as possible, in order to get the mining reward. The winning of reward is carried out using different blockchain consensus approaches [3]. For example, proof of work (PoW), proof of importance (PoI), proof of stake (PoS), practical Byzanite fault tolerance (PBFT), proof of space (PoSpace), and measure of trust (MoT). The technique used in Bitcoin and many other technologies of blockchain is PoW, in which a hard-mathematical puzzle is solved by miners to validate the transaction and win the reward. This

M. Ul Hassan and J. Chen are with the Swinburne University of Technology, Hawthorn VIC 3122, Australia (e-mail: muneebmh1@gmail.com; jinjun.chen@gmail.com)

M.H. Rehmani is with the Department of Computer Science, Cork Institute of Technology, Rossa Avenue, Bishopstown, Cork, Ireland (email: mshrehmani@gmail.com).

reward is further added to the network of blockchain. Another cryptocurrency named as Ether [4] follows PoW or PoS, in which pseudo-random way is used to choose the miner. Mining chance of a node depends upon the wealth of that specific node. For instance, the more wealth a node has, the greater will be its chance to mine the block and get the reward. Similarly, other mentioned mechanisms for consensus are also used in few applications of blockchain in order to enhance trust in the network [3].

2) Privacy of Blockchain: Blockchain technology is well-known for its secure transaction mechanism, authentication and encryption are used in blockchain are the two most important services offered by blockchain to ensure data security. These services are implied in blockchain via cryptography using public key encryption, in which the participants are required to have public and private information of keys by which they can manage respective transactions. Public key cryptography works over the principle of two types of keys; *public keys* (distributed network keys)and *private keys* (secret individual keys).

Blockchain-based distributed public key infrastructure (PKI) is the most common method provide functionality of key management for cryptography in blockchains. Blockchain-based PKI approaches are distributed entities and do not have any centralized access point or trusted third-party. Furthermore, in order to ensure transparency in the public system, these approaches do not require any prior trustworthiness from the nodes or participants of the system. Several blockchain approaches for PKI encryption such as Instant Karma PKI, Pemcor, Gan's approach, Blockstack, and Certcoin have been discussed in literature to provide secure transaction among blockchain nodes. After analysing above discussion, it is clear that a considerable amount of work has already been done over securing blockchain. However, the privacy aspect of blockchain is not completely addressed till now. Adopting the measures to secure blockchain are certainly valuable, but one cannot neglect the need of privacy in blockchain.

S. Nakamoto in [1] discusses that if the identity of owner of a private key gets revealed, it can then lead to disclosure of other transactions by same owners by using linking phenomenon. Similarly, the anonymity property, which is considered to be the most important feature of blockchain can also be compromised by using certain attacks [5]. Therefore, privacy preservation in applications of blockchain is an important issue that need to be addressed. Few researchers worked over enhancing the privacy of using different strategies. For example, Axon in [6] discusses two-level anonymity to overcome privacy issues of blockchain.

Similarly, the authors in [7] discussed overcoming transactional privacy (e.g., confidentiality) issues in a public blockchain to mitigate the privacy challenges and enhance trust parameter in blockchain. However, we believe that using differential privacy preservation strategy in blockchain, that uses data perturbation mechanism to protect private data can be state-of-the-art solution to resolve certain privacy issues of blockchain. In Section II, we discuss the integration of differential privacy with blockchain technology.

B. Differential Privacy

The idea of preserving privacy by adding adequate amount of noise in the data was first introduced by C. Dwork in 2006 [8]. Differential privacy was introduced to protect the privacy of statistical databases by adding noise to the data before query evaluation. However, researchers started using the concepts of differential privacy in other critical domains too and found out that differential privacy is one of the most useful privacy preserving strategy to protect personal data. Differential privacy perturbs sensitive data by adding a specific value of noise (after calculation) to preserve individual privacy. Differential privacy guarantees that presence or absence of any specific participant in a dataset does not affect the query output results of that database. This concept of differential privacy is further applied by researchers in various applications as well, for example real-time health data monitoring, IoT data, energy systems, etc. To further understand differential privacy, we discuss two examples, and important parameters of differential privacy in this section.

1) Example one: A smart electric meter reports the data usage of Hazel's house after every 5 minutes, the information reported to electric utility contains the units of electricity consumed in previous 5 minutes. This real-time reporting of units can provide certain useful benefits, such as real-time price querying, future demand response calculation, reducing electricity short-fall during peak hours, etc. Thus, the smart meter user Hazel can enjoy advanced power management by reporting his instantaneous usage of electricity. However, if this private data gets leaked or any adversary gets access to this data, then it can easily infer the lifestyle and daily routine of Hazel [9]. Furthermore, this adversary can even extract the time of use of any particular appliances in a specific time slot by using non-intrusive load monitoring (NILM) techniques. This privacy breach of smart meter of Hazel can easily be protected by using differential privacy concepts. In this case, differential privacy integrated in smart meter will perturb the data by adding adequate amount of noise to prevent exact real-time reporting of data, so that even if any adversary gets access to this critical data, it will not be able to infer the exact usage at a specific interval of time. Because the transmitted data is efficiently perturbed, so that it can be used for demand response, and other required tasks but the daily routine cannot be inferred from the data.

2) Example Two: Jack is an athlete who is preparing himself for next Olympics, he has to perform certain workouts and exercises in a day in order keep him fit according to the requirement. His coach asked him to get daily check-up by a nearby hospital, so that they can to see the health improvements in the required time span. The daily report data of Jack is stored in database of hospital, and the record of Jack can only be accessed by his coach or the concerning doctor. However, a survey company requests hospital admin to perform query evaluation for a survey regarding upcoming health issues. However, if that survey organization comes-up to be an adversary, it can then perform certain queries to get to know the exact stats of jack. For example, regarding the heartrate, the adversary can execute a query that "How many males in the database have heartrate from 50 to 60", then it can execute "How many people having heartrate from 50 to 60 named Jack". Similarly, adversary can get exact information of Jack by executing different types of queries. This disclosure of specific training data of Jack can be a major threat to privacy of a future athlete of Olympics. The survey conducting organization can even blackmail and may claim financial support in order to not publicize his reports. In order to protect such events to happen, differential privacy technique can be used by databases before query evaluation. Differential privacy ensures database privacy during query evaluation by adding a certain amount of noise in such manner that presence or absence of any specific individual (Jack in this case) will not have any effect in output query results. So, the adversary could not guess with confidence regarding medical records of Jack.

3) Sensitivity and Noise Addition Mechanism: Two important parameters to consider while including differential privacy in any data are sensitivity calibration and adequate noise calculation. *(i) Sensitivity* is said to be the parameter controlling the level of indistinguishability of data. For example, in a statistical database, the random value of a parameter y may be 1, or may even be 10,000, thus, the domain of this parameter y will be $y \in [1, 10^5]$. An adversary submits a query to calculate aggregate of each value of y such as $SUM(y)$, this query may also involve the value of participant whose privacy is intended to be protected. In this scenario, the differential privacy mechanism calculates noise according to the standard deviation and sensitivity within the dynamic range of 10^5. Thus, the added noise potentially hides the critical value and adversary is not able to approximate the presence or absence of a particular individual. But if the query is quite certain and to the point, then high level of noise needs to be added that requires a high level of sensitivity. However, using high sensitivity value will reduce the usefulness of data. Thus, an adequate trade-off between the privacy and truthfulness needs to be maintained by adjusting value of sensitivity accordingly. Usually the value of sensitivity varies from scenario to scenario, such as applications requiring high level of privacy use large sensitivity values and vice versa. Researchers also proposed various solutions, such as choosing dynamic sensitivity values, in which the value of sensitivity will automatically vary according to the nature and requirement of analysts and data provider [10].

(ii) Noise Addition mechanism is basically the protective phenomenon that calculates minimum noise value which is required to protect privacy of data. The output magnitude of noise depends directly upon the sensitivity value. This mechanism has a base function that requires input of certain parameters to calculate noise amount. Generally, three noise addition mechanism such as Laplace mechanism, Exponential mechanism, and Gaussian mechanism are used by researchers to calculate noise value. Similar to sensitivity, exact choice of noise addition mechanism also depends upon the nature of application. For example, in case of numerical output, Laplace and Gaussian mechanisms are generally used, while Exponential mechanism is used in case of non-numerical output [11].

II. Motivation of Using Differential Privacy in Blockchain

Blockchain is a revolutionizing technology that has changed the concept of digital form of trading or data storing. Because of its decentralized nature, blockchain is considered to be next generation of secure storage. However, certain issues regarding blockchain still require solution before its implementation in everyday life scenarios. One of the major parameter that requires considerable attention is preserving data and transaction privacy for blockchain applications. As identification of every user of blockchain in the decentralized network is carried by its public key, which means that the identities are not 100% private or anonymous.

Any adversary can act as a third-party analyst to analyse the transaction taking place inside the network and in turn may be able to infer original identities of individuals. Similarly, if we see the decentralized nature of blockchain, various scenarios of blockchain can be observed that are not protected and needs more privacy indulgence to protect personal data of blockchain nodes. For example, whenever a transaction occurs in a financial blockchain system, the information about the transaction is broadcast throughout the decentralized network. This broadcast is done to ensure that every node has updated information, and the ledger that keeps the records is uniform throughout the network. However, this information can be maliciously used by any adversary to keep records of a specific individual and backtrack all his transactional and financial details. Similarly, in blockchain based IoT devices, the exchange of information between different devices can be compromised by adversary to get certain illegal benefits. Moreover, the application of blockchain in real estate, asset management, and finances do also have risk of privacy leakage because of distributed nature. As the identities or critical information can be leaked during transaction broadcast. Furthermore, data stored in certain decentralized blockchain databases can also be utilized for conducting surveys. However, if the survey conducting organization becomes an adversary and tries to extract personal information, then the complete privacy of blockchain system can easily be compromised.

Till now, only anonymization and derivatives of anonymization strategy have been discussed in the literature to preserve individual privacy of blockchain [6]. However, various experiments revealed that anonymization is not a complete form of privacy, as any anonymized data can be combined with similar datasets to reveal personal information [12]. In order to overcome these issues, we consider that integration of differential privacy with modern blockchain technology can be a viable solution to protect its privacy. Differential privacy is well-known for its efficient privacy preservation in statistical databases, and real-time environment. Therefore, in order to protect privacy of all similar applications of blockchain, differential privacy proves to be one of the most favourable solution.

Dynamic nature of differential privacy makes its implementation suitable in blockchain scenarios. For example, in case of real-time data transmission or broadcast in blockchain applications, point-wise data perturbation strategy of differential privacy can efficiently add noise to data without disturbing the level of required accuracy [13]. Point-wise data perturbation requires the error rate that is tolerable by the receiver, after that algorithm calculates noise within that specific range and adds it into the data. So that, any observer adversary will not be able to accurately guess the exact value of data. Similarly, giving statistical blockchain data to others for analysing can first be protected using differential privacy. In case of statistical blockchain data, a sense of indistinguishably can be created via differential privacy, and the query analyst could not predict with conviction regarding availability of a specific blockchain node in the dataset. Another use case of differential privacy in blockchain technology could be the efficient preserving of identities of individuals during broadcast,in which differential privacy can perturb the identity in such a way that the information is still useful to complete transaction, but the nodes or adversary in the network will not be able to judge the exact identity of sender or receiver. Hence, the formal definition and theoretical model of differential privacy has the ability to control the privacy of only the crucial information within a set of data. Hence, we can say that addition of differential privacy in blockchain-based applications can be proven fruitful in certain tremendous ways. A brief summary about integration of differential privacy in certain blockchain scenarios is given in Section III.

III. Integration of Differential Privacy in Blockchain Scenarios

Blockchain is emerging as one of the most promising technology that has the potential to raise communication, storage, and transparency in transactions to the next level. According to Tractica (a market intelligence firm), the annual revenue generated via certain enterprise blockchain applications can reach up to U.S $ 19.9 billion at the end of year 2025 [24]. Blockchain technology is paving its paths in multiple industrial and academic domains, such as machine learning, smart grid, cloud computing, crowdsensing, and healthcare. Certain experiments have been conducted by researchers to study the effect of integration of blockchain in these domains, and amazingly maximum of experiments outperformed their expectations from perspective of security, transparency, and data storage. With the success of these experiments, many industries have started practical implementation and also started shifting their traditional storage to blockchain based storage in order to facilitate their users with the maximum possible facilities [25]. However, as discussed earlier, blockchain itself is a good option to enhance security and trust, but it is not pre-equipped with any privacy preservation technology. Blockchain provides pseudo anonymity via key encryption, although this pseudo anonymity is not sufficient enough to provide complete privacy guarantee [26]. Therefore, there is a huge need to integrate external privacy preservation strategy before practical implementation of blockchain. In order to do so, we discussed the integration of differential privacy with blockchain, as dynamic nature and strong theoretical basis of differential privacy can protect privacy of blockchain efficiently. In this section, we discuss certain projects and researches which integrated differential privacy in their scenarios.

A. Integration of Differential Privacy in Machine Learning Algorithms for Blockchain Data Training

Machine learning is being used as tool to develop promising solutions to our problems by getting deeper insights of available data in almost every field such as, bioinformatics, finance, and agriculture, and wireless communication [27]. Similarly, machine learning is also being integrated with certain practical applications such as blockchain, healthcare, etc. This integration has led foundation to numerous possibilities and many new fields in data analytics are originating.

In machine learning, usually a machine learning model is used to train a computer using a pre-available dataset. In traditional scenarios, this dataset is available in a centralized formation. However, in case of blockchain, this training is carried out in a decentralized distributed manner, and there are multiple computing nodes that are responsible to carry out learning process [28]. Since, the data is distributed among all computing nodes, the learning process should be equipped with some privacy preserving strategy in order to protect privacy during machine learning. In order to solve this problem, Chen *et al.* in [14] proposed a differential privacy based decentralized machine learning approach which protects users' privacy while carrying out machine learning using stochastic gradient descent (SGD). Authors named the proposed strategy as "LearningChain" and claimed that their proposed strategy provided private learning along with reducing error rate. The presented strategy works over the phenomenon of perturbing normalized local gradient information before mining it into blockchain, in this way the data is protected before making it tamper-proof, and only the desirable protected record is mined into blockchain network. Furthermore, the authors used a public blockchain and carry out consensus using proof-of-work (PoW) consensus mechanism. Moreover, to protect the system from byzantine attacks, the authors worked over l-nearest aggregation algorithm, that protects private data before during the collection by making it indistinguishable from its neighbors. The complete model was developed over Ethereum network and is studied using MNIST [29], and Wisconsin breast cancer datasets [30].

Another work that discusses the integration of differential privacy in blockchain based machine learning scenario is presented by Kim *et al.* in [15]. The proposed work enhances usability and transaction latency along with protecting privacy by carrying out experiments with repeated-additive noise via differential privacy. This repeated-additive noise is used in conjunction with local gradient, and is further improvised to protect blockchain user privacy. The authors implemented a private blockchain that mines the blocks using PoW consensus mechanism. Authors claimed that they enhanced users trust in distributed machine learning by introducing efficient perturbation mechanism via differential privacy. Moreover, the authors claimed to improve users' participation by overcoming adversarial and collusion attacks in the network. Keeping in view all the discussion, we can conclude that differential privacy protection strategy efficiently protects users privacy during decentralized blockchain based machine learning scenarios.

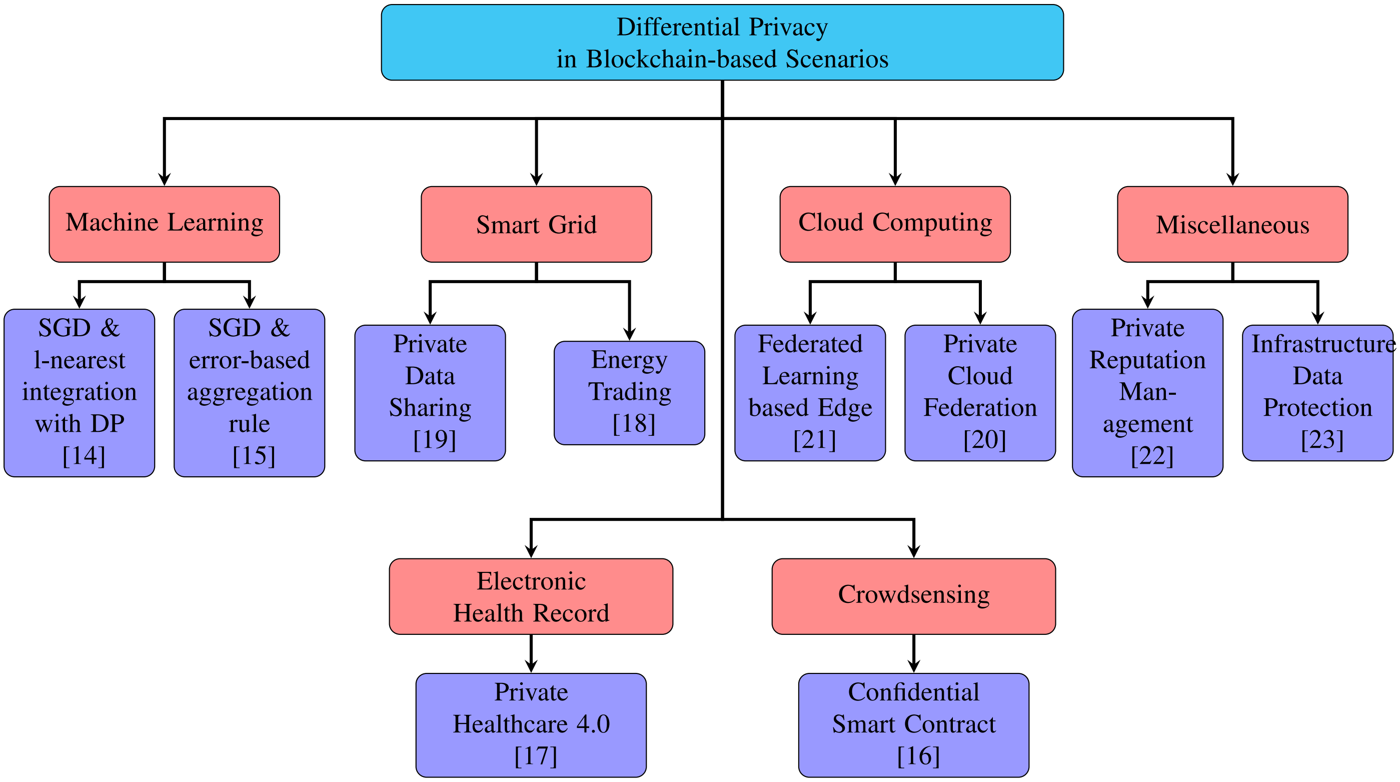

Fig. 1: Overview of differential privacy integration with machine learning, smart grid, cloud computing, crowdsensing, and healthcare applications operating over blockchain network.

B. Projects Considering Integrating of Differential Privacy with Blockchain based Smart Grid

Recent advances regarding deployment and development of smart grid has opened numerous research and industrial challenges. One of such challenge is to effectively manage and perform all operations of smart grid such as communication, energy trading, renewable energy management, etc [31]. Researchers are actively working to overcome these challenges and are transforming smart grid to cope-up with all mentioned issues. One possible solution to effectively manage smart grid operation is its integration with blockchain technology.

Many possible scenarios are beings explored to integrate blockchain technology with smart grid. For example, blockchain is deployed at certain layers of smart grid to provide security to its users, such as consumption layer, generation layer, etc. Recently, a case study regarding deployment of blockchain based micro-grid in Kazakhstan is presented in researchers in [32], in which they discussed the energy trading possibilities of Kazakhstan using blockchain. Literature shows that a lot of works are discussing integration of smart grid with blockchain, however plenty of works are neglecting the need of privacy preservation in this scenario. Blockchain is a publicly distributed ledger, and this raises the need of integration of privacy protection in such model. Majority of operations performed in smart grid scenarios comes under the field of real-time data analytics, therefore integrating modern noise addition mechanism of differential privacy seems to be one of the most prospective solution to overcome these challenges.

One such work to provide private energy trading in modern blockchain-based smart grid scenario is carried out by authors in [18]. The authors proposed their own private energy trading model by following the basic implementation details of differential privacy and compared their proposed models with existing differential privacy approaches. The proposed mechanism works over phenomenon of blockchain-based token bank to store and carry out transactions during energy trading. Similarly, the mechanism achieves effects of differential privacy by preventing linkability and overcoming datamining and linking attacks along with consuming minimal computational power. Furthermore, another work integrating differential privacy in deregulated smart grids operating over blockchain is provided in [19]. The authors worked over enhancement of proof-of-authority (PoA) mechanism via integrating it with PageRank mechanism to formulate reputation scores. Moreover, the authors added Laplace noise to protect users privacy in order to encourage more participating users. Authors claimed that their proposed strategy enhances trust by overcoming similarly, and double spending attacks of blockchain-based smart grid users. The above discussion illustrates that privacy requirements should seriously be considered while integration of blockchain with smart grid, and more research efforts are required to provide smart grid users a trustable atmosphere.

C. Integrating Differential Privacy with Blockchain-based Cloud Computing

The paradigm of cloud is being used by industries since long time, however researchers are enhancing this paradigm

TABLE I
OVERVIEW OF INTEGRATION OF DIFFERENTIAL PRIVACY PROTECTION STRATEGIES IN BLOCKCHAIN BASED SCENARIOS

Major Domain	**Sub-Category**	**Ref #**	**Technique Name**	**DP Mechanism Integration**	**Noise Type**	**Outcome Enhancements**	**Block-chain Type**	**Consen-sus**	**Considered Attacks**	**Compl-exity**
Machine Learn-ing	SGD & l-nearest	[14]	LearningChain	Perturbed normalized local gradient vector	$\mu(a) \propto e^{(-\beta \|a\|_2)}$	• Error rate	Public (permissi-onless)	PoW	• Byzantine attacks	–
	Error based ag-gregation	[15]	Privacy-preserving learning for permissioned blockchain	Repeated-additive noise in conjunction with local gradient	Gaussian	• Usability • Transaction latency & complexity	Private (permissi-oned)	PoW	• Adversarial attacks • Collision attacks	$O(k.d)$
Smart Grid	Energy trading	[18]	Private energy trading in SG	A mechanism to achieve effect of DP	Structural bounded noise	• Prevented linkability w.r.t energy degree	Conso-rtium (permissi-oned)	Self designed	• Data mining attacks • Linking attacks • Identity attacks	$O(n)$
	Private Data Sharing	[19]	Fair data sharing in private smart grid	Use pagerank algorithm to deduce private reputation	Laplace	• Customer participation • Gas consumption	Public (permissi-onless)	PoA	• Double spending attack	–
Cloud Com-puting	Cloud Federa-tion	[20]	Differential privacy based data sharing	Autonomous smart contract based privacy budget allocation	Laplace	• budget consumption • workload	Private (permissi-oned)	pBFT	• Re-identification attack	–
	Federated Learning based Edge	[21]	Private survey feature extraction using DP and FL	DP noise is added with extracted features	Laplace	• Test accuracy	Public (permissi-onless)	PoW	• Model poisoning attack	–
Crowd-sensing	Confidential smart contract	[16]	Aggregating & storing private crowdwisdom	Integrating zero-knowledge proofs and DP to protect privacy	Geometric distri-bution $Geom(\alpha)$	• Computation time • Gas cost	Public (permissi-oned)	PoW	• Statistical attacks • Side-channel attack	–
Elec-tronic Health Records	Private healthcare 4.0	[17]	Secure blockchain based healthcare	Discussed integration of DP	–	• Efficient maintenance & storage	Public (permissi-onless)	Proof of Votes	–	–
Miscel-laneous	Controlled data sharing & reputation manage-ment	[22]	DP based controllable data sharing model	Control policy working over DP phenomenon	Laplace	• Price balance • Reputation score	Public (permissi-onless)	PoC	–	–
	Infrast-ructure data protection	[23]	Enhanced access control for infrastr-ucture data via DP	DP layered protection used for aggregation	Laplace	• Processing time	Public (permissi-onless)	PoW	• Query attack	–

day by day and are moving towards more modern and advanced cloud computing models. One such model is the use of edge/fog computing to benefit cloud by providing quick access to important tasks [33]. Another model proposed by researchers is to extract features of cloud by using machine learning algorithms [34]. Similarly, works are being carried out to integrate blockchain with edge computing in order to provide reliable storage, control and network access along with providing the functionality of large scale network servers [24]. These works motivated many researchers to explore the field of blockchain-based edge and cloud computing and many researches are being carried out to enhance its efficiency and time-delay [35].

On the other hand, some researchers also pointed out the flaw of privacy leakage in blockchain-based cloud systems and highlighted certain privacy issues in this implementation [36]. In order to overcome these issues, researchers are integrating privacy protection strategies with blockchain-based cloud and integrating differential privacy with blockchain-based cloud is one of a prospective solution. One such works that integrated differential privacy with data sharing with federation based decentralized cloud is carried out in [20]. The authors integrating the emerging concept of cloud federation with differential privacy in order to allocate autonomous privacy budget during blockchain mining. The proposed work enhanced work load during query execution and claimed that the given mechanism answers query more effectively along with protecting privacy. Private/permissioned blockchain model is used by researchers along with byzantine fault tolerant (BFT) consensus mechanism to ensure the cooperation and control by some specific authorized nodes. Furthermore, the authors claimed that the proposed mechanism successfully tackles all re-identification attacks due to its data perturbing nature.

Another domain of federated learning based edge computing is explored by Zhao *et al.* in [21]. The authors extracted survey features from crowd edge nodes using differential privacy and federated learning approach along with ensuring that none of the private data of IoT users is analysed. Furthermore, Laplace noise is added to extracted features of crowdsensing before mining the results to blockchain. The provided mechanism overcome model-poisoning attack along with enhancing test accuracy for blockchain feature extraction. From the above discussion, it can be seen that blockchain-based edge and cloud computing is not completely secure and private. Therefore, researches should be carried out to enhance privacy in such decentralized cloud scenarios.

D. Integration of Differential Privacy in Crowdsensing Operating over Blockchain

The domain of crowdsensing was introduced to collect data from sensor-rich IoT devices, in order to carry out behavioural analysis and certain other similar tasks. This domain of crowdsensing strengthened its roots because of its vast advantages in the field of healthcare, environmental monitoring, and intelligent transportation [37]. Because of this, researchers also explored the domain of integration of crowdsensing with emerging blockchain technology, and this exploration provided to be a type of ideal exploration. The immutable nature of blockchain ledger ensured security and tamper-resistance of data. However, on the other side, this technology also poses certain risks related to data confidentiality and privacy. The public available of decentralized ledger raises serious doubts regarding the privacy of data rich sensors and users are raising questions regarding confidentiality of their data.

In order to overcome this catasttrophy, researchers are working over integrating advances privacy preserving strategies with crowdsensing in order to provide a trustworthy atmosphere to its users. One such step is the integration of differential privacy with crowdsensing, which is carried out by Duan *et al.* in [16]. Moreover, the authors worked over privacy preserving aggregation and storage of crowd wisdom using differential privacy. Furthermore, the authors also integrated zero-knowledge-proofs with differential privacy perturbation to ensure further confidentiality of data. The presented model claims to enhance computational power along with reducing gas cost spent during block mining. The authors ensured that their proposed strategy efficiently overcome statistical and side-channel attacks due to differential privacy and zero-knowledge-proofs protection.

After critically viewing all the discussion, it is clearly evident the differential privacy protects privacy of blockchain based crowdsensing nodes in an efficient manner. Therefore, researches need to focus over integrating modern decentralized crowdsensing scenarios with differential privacy.

E. Integrating Differential Privacy in Decentralized Healthcare

Healthcare 4.0 is considered to be one of the core part of modern smart cities, in which every patient, doctor, and hospital will be connected with each other in order to perform certain functions such as remote health monitoring, fitness programs, and elderly care, etc [38]. However, because of quick urbanization, traditional healthcare devices and systems are not capable enough to meet demands and requirements of citizens. Similarly, traditional healthcare systems do not provide enough transparency and trust because they can be tampered, and data can be changed via some adversarial attacks. Therefore, trend of integration of blockchain with healthcare is increasing day by day and many hospitals and healthcare centres have started implementing blockchain based healthcare. This trend has provided numerous benefits, although it also raises some serious privacy concerns because of public availability of data. As data over blockchain is stored in a decentralized distributed ledger and every node has a copy of that ledger, therefore, some malicious node can intrigue into private data of a blockchain node.

Researchers are actively working to integrate privacy preservation strategies with blockchain based healthcare systems. One of such effort involves integration of differential privacy in decentralized healthcare, in which private data of patients is efficiently perturbed in order to protect their privacy. The authors in [17] proposed a secure blockchain based healthcare system operating over proof of votes consensus mechanism. The authors further added that they added noise in their data using differential privacy protection to ensure user privacy. From the above discussion it can be seen that blockchain-based healthcare required additional privacy preservation mechanism to protect users' privacy. However, no such work that provide simulation based analysis over protecting healthcare records privacy is available in literature yet. Therefore, researches need to be carried out in this particular domain, in order to provide healthcare users a trusted and private atmosphere.

F. Miscellaneous

Blockchain has been proved to be fruitful in majority of daily-life domains, similarly, integration of blockchain with differential privacy is also giving viable results in majority of similar domains. Some other works that involve integration of differential privacy and blockchain has been carried out in the field of controllable data sharing and infrastructure data protection. Both of the domains are of huge importance to our everyday life and require more discussion from their privacy perspective.

One such work is carried out by Dong *et al.* in the field of balanced and self-controllable data sharing in blockchain using differential privacy. The authors worked over control policy phenomenon and designed it using basics of differential privacy perturbation. Authors enhanced price balance and ensured that users can have self-control over their private data, so that they can use blockchain without the fear of losing their private information. Anther similar work that integrated differential privacy with infrastructure management domain is carried out by Alnemari textitet al. in [23]. Author enhanced query processing time in decentralized blockchain network and provided a layer-wise perturbation structure for differential privacy integration with infrastructure management data. After viewing the discussion, it can be concluded that there are still certain domains in blockchain systems that require considerable attention from perspective of their privacy protection.

G. Summary and Lessons Learnt

Blockchain based systems and scenarios such as machine learning, smart grid, healthcare, cloud computing, and crowd-sensing are gaining stability day by day and a lot of researches are being carried out to enhance their efficiency, throughput, privacy, and security issues. A major issue that these systems is facing is the leakage of privacy due to their transparent and publicly available nature. Therefore, researchers are moving towards addition of privacy preservation strategies with these systems. In doing so, researchers have analysed many privacy preservation mechanisms in blockchain scenarios and provided their technical and theorical pros and const. Keeping in view their implementation and protection outcomes, it can be said that differential privacy comes out to be one of the most optimal method to protect privacy of blockchain systems.

The discussion above provided a brief overview of integration of differential privacy in certain blockchain domains, and it also shows that researches are now being conducted to enhance differential privacy in order to fit into decentralized scenarios completely. However, still a lot of room is left and there is a need for researchers to focus over protection and enhancement of privacy in blockchain based scenarios.

IV. Future Applications of Differential Privacy in Blockchain

The blockchain has the ability to transform the stability, transparency, and security of daily networks, provided the fact that is should only be applied to the required applications, because integrating blockchain not a panacea for every problem of centralized network. Similarly, while applying blockchain to any application, its privacy protection should be taken care of. In this section, we discuss privacy protection of few applications of blockchain using differential privacy. Figure 2 depicts the integration of differential privacy in blockchain applications to protect data privacy. Similarly, Table II gives a brief overview about the privacy requirements and parameters needed to preserve while integrating differential privacy in applications of blockchain.

A. Internet of Things

The notion of IoT was first introduced to address and manage devices that were connected using radio-frequency identification (RFID) wireless technology. With the passage of time, this IoT concept shifted from RFID technology to Internet based connections. Currently, IoT devices are on an urge to take over world in every aspects of our everyday life. The scope of IoT is not limited only to a few selected domains, as it does accumulate almost every domain in which a physical device is connected to Internet or any other device using Internet protocol (IP). Few common examples of IoT systems include farming, modern energy systems (smart grid), healthcare systems, transportation systems, etc. Similarly, further advancements in IoT systems involves its integration with blockchain technology. Among IoT applications, blockchain can be integrated into applications that involve sensing, identity management, data storage, real-time data transmission, wearables, supply chain management, and other similar scenarios. Certain companies such as IBM took a step ahead and talked regarding blockchain as a technology to democratize IoT future [43]. However, the data exchange between these P2P IoT networks also raises large number of privacy issues. For instance, all blockchain users are identified with the help of their public key or their hash, which can be used to track all transactions because public key is not anonymous. Therefore, protecting blockchain IoT data using efficient privacy protection strategy (such as differential privacy) is important. In this section, we discuss three major applications regarding integration of differential privacy in IoT systems via blockchain technology.

1) Energy Systems (Smart Grid): An important application of blockchain-based IoT system is energy sector. Integration of blockchain-based technology in energy systems can be applied to large number of scenarios such as smart meter usage reporting, individual device consumption information, grid utility data aggregation, etc. Similarly, the authors in [44] discussed that blockchain-based decentralized energy systems will be intelligent enough to pay for consumption of energy from each device. This basically can eradicate the need of a central entity to collect and distribute bills among houses/buildings. However, keeping in view the shared nature of blockchain-based energy systems, it can easily be said that the identities of energy devices / smart meters are not protected. Furthermore, the owner/user of particular device/meter can also be tracked by using public broadcast data. Therefore, any adversary can easily get energy consumption information of a particular home or individual. In this way, the routine of residents of that home can be estimated and personal privacy is at risk. One of the effective way to protect this information is to perturb the data using differential privacy before broadcast into the network.

In a scenario of blockchain-based decentralized smart meter network, every smart meter is calculating its billing information after every 10 minutes and is reporting the transaction details publicly on ledger in order to keep the track. From this data, any intruder can predict the identity and then can check the usage patterns of that specific house. These patterns

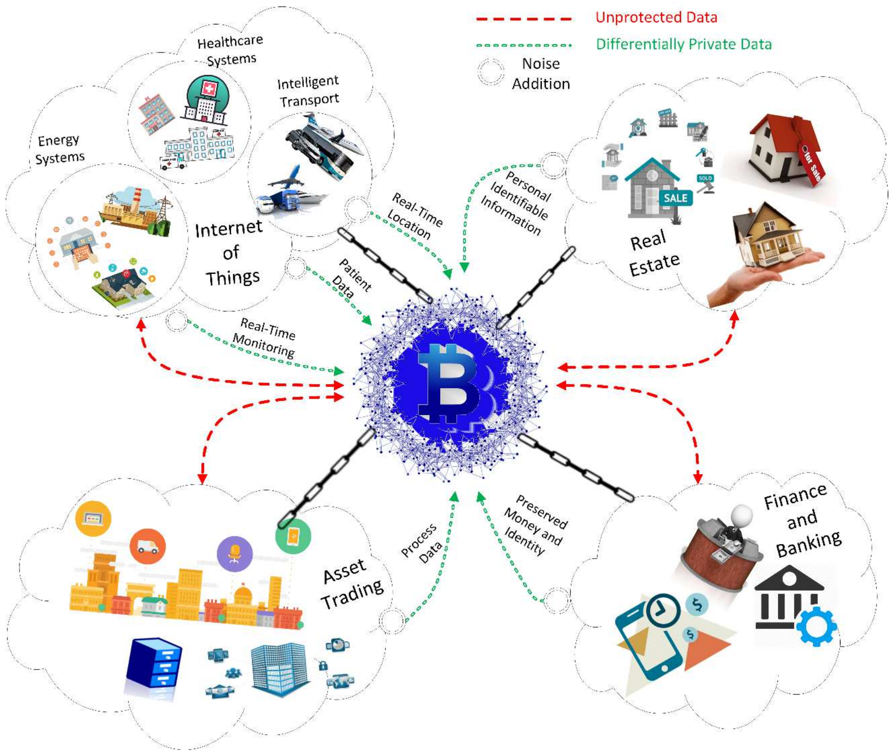

Fig. 2: Application scenarios of integration of differential privacy in blockchain-based Systems (such as Internet of Things (IoT), real estate management, asset trading, and finance Trading).

TABLE II
PRIVACY REQUIREMENTS AND PRESERVED PARAMETERS OF INTEGRATION OF DIFFERENTIAL PRIVACY IN APPLICATIONS OF BLOCKCHAIN

Application Name	Sub Domain	Type of Data	Required Privacy Level	Parameters to Preserve
Internet of Things (IoT)	Energy Systems [19]	Time-Series	Medium	• Real-time monitoring • User identity
	Healthcare Systems [17]	Time-Series & Statistical	Very High	• Patients' identity
	Intelligent Transportation Systems [39]	Time-Series	Medium	• Vehicle location • Driver identity • Freight data
Real Estate	Trading (Buying & Selling) [40]	Time-Series	High	• Buyer & seller identity
Asset Management	Virtual or Physical Resources [41]	Time-Series	Medium	• Package location • Processing steps
Finance and Banking	International Transfer [42]	Time-Series	Very High	• Sender & Receiver identity • Exchanged amount

can be used by adversary to plan any illegal activity, such as theft, etc. Smart meter cannot even stop transmitting this real-time data, because this data is used by grid utility for certain calculations, such as demand response, future load forecasting, etc. However, if we will integrate differential privacy in this scenario, the risks factor can easily be reduced to minimum. Differential privacy integrated with blockchain-based smart meter will resist meter from reporting the accurate instantaneous value of meter reading, instead it will perturb the consumption value with some calculated noise according to the requirement. So, the smart meter will be reporting a new value in which noise is added. That is why, even if any adversary gets access to this reported data, it will not be able to make a confident guess regarding the usage of particular home. Similar concept of differential privacy can also be applied over different scenarios of integration of blockchain in energy systems. However, the amount of added noise depends upon the allowed error-rate by utility/user. Hence, while integrating differential privacy with blockchain-based shared energy systems, this trade-off between accuracy and privacy needs to be addressed efficiently.

2) Healthcare Systems: Blockchain-based healthcare applications are trending among research community now, and researchers are working over fusion of decentralized management for healthcare using blockchain technology. For example, in [45] the authors presented the scenario of blockchain-based IoT sensors in pharmaceutical industry in order to verify the quality, temperature, packaging, and transportation of medicines to hospitals or chemists. The complete procedure from manufacturing to hospital storage is transparent and is accessible for general public. This complete idea seems quite appealing, but it comes up with certain privacy risks for both; the manufacturing company, and the public. In this way, any unlicensed company can get to know the exact manufacturing ingredients, experimental environment, and transportation conditions of process and can produce a similar medicine with identical name to confuse the buyers. However, this condition can easily be protected using differential privacy strategies. For instance, while reporting the ingredients or the medicine number in blockchain ledger, differential privacy algorithm can protect the exact ingredient number or the device name by perturbing it with an optimal noise, so that any intruder will not be able to make accurate assumptions regarding the presence or absence of any specific ingredient in the medicine. However, the actual manufacturing details are stored in the private blockchain database, in order to backtrack in any uncertain case.

3) Intelligent Transportation System: The advancements in intelligent transportation system (ITS) has given birth to numerous new fields, and integration of blockchain with transportation is one of them. The major reason behind this merger is to enhance the security of vehicular networks by using key encryption [46]. On one hand, this fusion enhanced security in ITS, but on the other hand this has increased privacy risks within transportation network. For example, every vehicle will be connected to each other in a vehicular network of ITSs, and every vehicle will be exchanging different sensor's information with each other. This communication can be made more secure by using key encryption technology of blockchain, so that nobody from outside the network will be able to decode the broadcast message. However, the users within a public blockchain can identify get information regarding other users. For instance, a car X reports its location, traffic situation, and meteorological data with time stamp. Similarly, another car Y in the blockchain network receives this information and uses it. Since, it is a public blockchain, the real identity of owner of car X can easily be revealed by using its hash value and public cryptography key. This leakage of information poses serious privacy threats to vehicle user, because its travelling routine can be observed by collecting the transmitted information. However, differential privacy integration with blockchain-based ITS can protect this information from getting leaked. Data perturbation mechanism of differential privacy can perturb the private information of vehicles' owner in such a way that only the minimum required information is sent to broadcast after addition of noise. Similarly, this privacy preservation of differential privacy can also be applied to other scenarios of ITSs, such as blockchain-based railway freight, and public transportation system that can be made publicly accessible in order to provide real-time update to travellers.

B. Real Estate

Dealings and transactions in real estate world needs to be transparent and opaque, but middlemen are generally required in order to do a fair deal now a day. The complete process of involving middlemen such as broker, inspectors, and notaries public is cumbersome and expensive. In order to overcome this situation, researcher community is working over implementation of blockchain-based real estate setup. As the first motto of a blockchain based system is transparency and security, so these types of systems would totally eliminate the need of middlemen for security purpose. The decentralized public ledger of blockchain will allow the sellers to advertise their properties using broadcast in the network, and similarly buyers can select their desired properties, contact sellers, make transactions, and register properties with their names, and broadcast the sold notification to the network just by using blockchain-based setup. In this way, blockchain will remove the use of expensive, and cumbersome middlemen. This system will work similar to Bitcoin, which is successfully in running from past decade. However, certain uncertainties related to privacy needs to be addressed before implementation of this system in everyday lives. For example, after the successful purchase of any property, or while advertising a specific property, the identities of buyer and seller should not be publicized. It is enough in a trade that only buyer and seller know each other, without the interference of any third person.

Making the identities public will provide a sense of insecurity for people who are trading very often or are generating good revenues. In this case, just the protection using public key cryptography is not enough, because experiments have shown that identities can be tracked using hash and public keys. To protect this process, and in order to make it more secure and private differential privacy based blockchain real estate system will be a viable solution. As broadcast of information after a successful purchase is important, in order to avoid multiple transactions for same property, but differential privacy implemented in this scenario can perturb the user identity and other personally identifiable information (PII) in order to preserve privacy. So, in differentially private blockchain based real estate systems, one can broadcast the transaction information without the risk of revealing PII to public. However, one of the biggest challenge in application of differential privacy in this scenario is the identification of accurate PII parameters. As there is no predetermined rule to declare that the specific piece of information is counted in PII or it is not in PII. Therefore, the identification and declaration of PII could be done via some sort of mutual agreement inside the network in which all nodes do agree. Thus, we consider that after resolution of this PII problem, implementation of differential privacy in blockchain-based real estate trading system can be an optimal solution to preserve individual privacy.

C. Asset Management

The concept of asset management and trading is similar to property trading, but asset management can include any sort of physical or virtual asset ranging from software service to a physical computer. Therefore, blockchain-based asset management can be a key solution to add up transparency and efficiency in the process. For example, in case of a physical resource, the process initiates from serialization and terminates at deployment of asset. Every step during the process is reported using decentralized blockchain network. However, this decentralization broadcast may also lead to certain privacy related issues. For instance, an adversary can track the exact process and can replicate the asset qualities. Moreover, if some critical asset needs to be deployed or delivered, then the adversary can know the exact location of asset along with the timestamp, which could be a big risk for the safety of asset. The involvement of differential privacy in this asset trading scenario can reduce this privacy loss risk to minimum. As the data perturbation technique of differential privacy can efficiently add up noise in required information and can protect data being leaked during broadcast. However, during data perturbation in asset management, the added amount of noise needs to be carefully addressed. Because process step and asset information are quite critical and excess noise can destroy usefulness of data, while less noise can risk privacy leakage. So, the careful analysis about required privacy needs to be taken before implementing differential privacy in blockchain-based asset management.

D. Finance and Banking

Blockchain was first introduced to deal with cryptocurrency such as Bitcoin and Ethereum, later on researchers identified various other benefits of using blockchain in other setups as well. However, the benefits of blockchain in this online currency cannot be underestimated. Therefore, research community is thinking of using this technology again, but in perspective of official finances and banking. Instead of cryptocurrency, the new currency that researchers are working over to introduce in the market is digital currency. One potential application of blockchain in finances is international money transfer. The complete process of international money transfer is sluggish, tiresome, and very expensive because it is usually done with the involvement of middlemen. This process takes several currencies, and banks before the receiver is able to collect the money. Similarly, some services such as Western Union are fast, but they are extremely expensive. The use of blockchain in finance will eradicate the unnecessary need of middlemen and will also save a lot of time and money. As everything will happen within an open blockchain environment that ensures transparency in transactions. It is an important aspect that transactions are clear and are visible to people in the network, so that nobody is able to perform duplicate transactions. However, this transparency may also cause some privacy concerns too. For example, people in the network can get to know regarding the financial dealings of a specific person. Or adversaries can target a person who is doing large transactions and may use this information for any illegal purposes. Similarly, the place to receive the payment needs to be protected, so that any thief might not be able to perform robbery if a big transaction needs to be received somewhere. Keeping in view all these points, it can be said that protecting certain amount of information during financial dealings is mandatory. One of the most efficient way to protect this information is perturbing the private information using differential privacy protection. Differential privacy can efficiently perturb the desired information without risking the transparency of transaction.

V. Conclusion

Blockchain is an emerging technology and has a very gigantic future in the next five years. Along with these advancements, certain issues of blockchain needs to be addressed with time. One of the major issue of blockchain is its privacy concerns and information leakage in practical applications. In order to overcome information leakage and protect blockchain privacy, modern data perturbation technique named as differential privacy can be use used. In this paper, we present a brief discussion regarding the functionality of blockchain, and differential privacy by considering their operation phases and important parameters. Furthermore, we present a brief summary about the integration of differential privacy in decentralized blockchain technology. Finally, we concluded the article with discussion regarding practical implementation of differential privacy in blockchain-based everyday life applications such as Internet of Things, real estate, asset management and finances.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *http://bitcoin.org/bitcoin.pdf*, 2008.

[2] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 7, pp. 1366–1385, 2018.

[3] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Communications Surveys & Tutorials, in Print*, 2018.

[4] "Ethereum blockchain app platform. (2017)," [Online]. Available: https://www.ethereum.org/.

[5] J. Herrera-Joancomartí and C. Pérez-Solà, "Privacy in bitcoin transactions: new challenges from blockchain scalability solutions," in *Modeling Decisions for Artificial Intelligence*. Springer, 2016, pp. 26–44.

[6] L. Axon, "Privacy-awareness in blockchain-based pki," *University of Oxford*, 2015.

[7] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[8] C. Dwork, "Differential privacy," in *Proceedings of the 33rd International Conference on Automata, Languages and Programming - Volume Part II*, ser. ICALP'06. Berlin, Heidelberg: Springer-Verlag, 2006, pp. 1–12.

[9] T. Wang, Z. Zheng, M. H. Rehmani, S. Yao, and Z. Huo, "Privacy preservation in big data from the communication perspective—a survey," *IEEE Communications Surveys & Tutorials, in Print*, 2018.

[10] E. ElSalamouny and S. Gambs, "Differential privacy models for location-based services," *Transactions on Data Privacy*, vol. 9, no. 1, pp. 15–48, 2016.

[11] C. Dwork, A. Roth *et al.*, "The algorithmic foundations of differential privacy," *Foundations and Trends® in Theoretical Computer Science*, vol. 9, no. 3–4, pp. 211–407, 2014.

[12] Y.-A. De Montjoye, L. Radaelli, V. K. Singh *et al.*, "Unique in the shopping mall: On the reidentifiability of credit card metadata," *Science*, vol. 347, no. 6221, pp. 536–539, 2015.

[13] G. Eibl and D. Engel, "Differential privacy for real smart metering data," *Computer Science-Research and Development*, vol. 32, no. 1-2, pp. 173–182, 2017.

[14] X. Chen, J. Ji, C. Luo, W. Liao, and P. Li, "When machine learning meets blockchain: A decentralized, privacy-preserving and secure design," in *IEEE International Conference on Big Data (Big Data)*, 2018, pp. 1178–1187.

[15] H. Kim, S. Kim, J. Y. Hwang, and C. Seo, "Efficient privacy-preserving machine learning for blockchain network," *IEEE Access*, pp. 1–1, 2019.

[16] H. Duan, Y. Zheng, Y. Du, A. Zhou, C. Wang, and M. H. Au, "Aggregating crowd wisdom via blockchain: A private, correct, and robust realization," in *IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 2019, pp. 43–52.

[17] J. Vora, A. Nayyar, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and J. J. Rodrigues, "Bheem: A blockchain-based framework for securing electronic health records," in *IEEE Globecom Workshops (GC Wkshps)*, 2018, pp. 1–6.

[18] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," *IEEE Transactions on Industrial Informatics, in Print*, 2019.

[19] O. Samuel, M. A. Nadeem Javaid, Z. Ahmed, M. Imran, and M. Guizani, "A blockchain model for fair data sharing in deregulated smart grids," in *IEEE Global Communications Conference: Communication & Information Systems Security, USA*, 2019, pp. 1–7.

[20] M. Yang, A. Margheri, R. Hu, and V. Sassone, "Differentially private data sharing in a cloud federation with blockchain," *IEEE Cloud Computing*, vol. 5, no. 6, pp. 69–79, 2018.

[21] Y. Zhao, J. Zhao, L. Jiang, R. Tan, and D. Niyato, "Mobile edge computing, blockchain and reputation-based crowdsourcing iot federated learning: A secure, decentralized and privacy-preserving system," *arXiv preprint arXiv:1906.10893*, 2019.

[22] X. Dong, B. Guo, Y. Shen, X. Duan, Y. Shen, and H. Zhang, "A self-controllable and balanced data sharing model," *IEEE Access*, vol. 7, pp. 103 275–103 290, 2019.

[23] A. Alnemari, S. Arodi, V. R. Sosa, S. Pandey, C. Romanowski, R. Raj, and S. Mishra, "Protecting infrastructure data via enhanced access control, blockchain and differential privacy," in *International Conference on Critical Infrastructure Protection*. Springer, 2018, pp. 113–125.

[24] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1508–1532, 2019.

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

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

[27] C. Luo, J. Ji, Q. Wang, X. Chen, and P. Li, "Channel state information prediction for 5g wireless communications: A deep learning approach," *IEEE Transactions on Network Science and Engineering, in Print*, 2018.

[28] W. Xiong and L. Xiong, "Smart contract based data trading mode using blockchain and machine learning," *IEEE Access*, vol. 7, pp. 102 331–102 344, 2019.

[29] L. Deng, "The mnist database of handwritten digit images for machine learning research [best of the web]," *IEEE Signal Processing Magazine*, vol. 29, no. 6, pp. 141–142, 2012.

[30] A. Asuncion and D. Newman, "Uci machine learning repository," 2007.

[31] M. H. Rehmani, M. Reisslein, A. Rachedi, M. Erol-Kantarci, and M. Radenkovic, "Integrating renewable energy resources into the smart grid: Recent developments in information and communication technologies," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 2814–2825, 2018.

[32] D. Orazgaliyev, Y. Lukpanov, I. A. Ukaegbu, and H. S. K. Nunna, "Towards the application of blockchain technology for smart grids in kazakhstan," in *21st International Conference on Advanced Communication Technology (ICACT)*. IEEE, 2019, pp. 273–278.

[33] J. Moura and D. Hutchison, "Game theory for multi-access edge computing: Survey, use cases, and future trends," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 260–288, 2018.

[34] T. K. Rodrigues, K. Suto, H. Nishiyama, J. Liu, and N. Kato, "Machine learning meets computation and communication control in evolving edge and cloud: Challenges and future perspective," *IEEE Communications Surveys Tutorials, in Print*, pp. 1–1, 2019.

[35] S. Wang, X. Wang, and Y. Zhang, "A secure cloud storage framework with access control based on blockchain," *IEEE Access*, vol. 7, pp. 112 713–112 725, 2019.

[36] S. Pavithra, S. Ramya, and S. Prathibha, "A survey on cloud security issues and blockchain," in *3rd International Conference on Computing and Communications Technologies (ICCCT)*. IEEE, 2019, pp. 136–140.

[37] X. Zhang, Z. Yang, W. Sun, Y. Liu, S. Tang, K. Xing, and X. Mao, "Incentives for mobile crowd sensing: A survey," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 54–67, 2015.

[38] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Communications Surveys & Tutorials, in Print*, 2019.

[39] T. Jiang, H. Fang, and H. Wang, "Blockchain-based internet of vehicles: Distributed network architecture and performance analysis," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4640–4649, June 2019.

[40] A. Spielman, "Blockchain: digitally rebuilding the real estate industry," Ph.D. dissertation, Massachusetts Institute of Technology, 2016.

[41] Y. Zhu, Y. Qin, Z. Zhou, X. Song, G. Liu, and W. C.-C. Chu, "Digital asset management with distributed permission over blockchain and attribute-based access control," in *International Conference on Services Computing (SCC)*. IEEE, 2018, pp. 193–200.

[42] A. A. Alidin, A. A. A. Ali-Wosabi, and Z. Yusoff, "Overview of blockchain implementation on islamic finance: Saadiqin experience," in *Cyber Resilience Conference (CRC)*. IEEE, 2018, pp. 1–2.

[43] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," *IEEE Access*, 2018.

[44] T. Lundqvist, A. de Blanche, and H. R. H. Andersson, "Thing-to-thing electricity micro payments using blockchain technology," in *IEEE Global Internet of Things Summit (GIoTS)*, 2017, pp. 1–6.

[45] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere-a use-case of blockchains in the pharma supply-chain," in *IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, 2017, pp. 772–777.

[46] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1832–1843, 2017.

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, Hawthorn VIC 3122, Australia. His research interests include privacy preservation, blockchain, game theory, and smart grid.

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.

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 PhD 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.