COGNITIVE RADIO NETWORKS BASED ON BLOCKCHAIN MANAGEMENT: A REVIEW

Meena[1] Neha Gupta[2] Prerana Dhull[3] Dr. Vaibhav Jain[4] Dr. Monika Goyal[5]
[1]Research Scholar, Vaish College of Engineering , Rohtak
[2]Assistant Professor, Vaish College of Engineering , Rohtak
[3]Assistant Professor, Vaish College of Engineering , Rohtak
[4] Associate Professor, Vaish College of Engineering , Rohtak
[5]Assistant Professor, Vaish Mahilla Mahavidyalya, Rohtak

ABSTRACT

While the load of the Internet traffic over the fourth and fifth generation mobile communication network is escalating gradually, it lacks sufficient radio resources to support them gracefully. Hence, the effort of most of the current researcher is to maximize the utilization of limited radio resources. The dynamic spectrum access policy embraces a technology in which a mobile user obtains knowledge of its geographical, operational radio environment and its own internal state. Based on the knowledge, the user can opportunistically use the existing systems' radio resources, resulting into maximization of their utilization.

Keywords: CRN , Block Chain , Security , Ledger , Encryption.

DOI Number: 10.14704/nq.2022.20.12.NQ77044 **NeuroQuantology 2022; 20(12): 594-612**

I. INTRODUCTION

In DSA, the licensed spectrum band is allocated to a group of users, which are called primary users (PUs). The licensed bands are not exclusively granted to those users, only they have higher priority in using it. Other users, referred to as secondary users (SUs), can also use the licensed channel. In this scenario, when PUs are not using the channel, SUs are allowed to use that channel in a non-interfering manner. Thus, the utilization of the radio channels can be improved by reusing it in an opportunistic manner. In the context of DSA, the radio system employs a technology that obtains knowledge of its geographical and operational environment and set up policies and its internal state. This will help the system to autonomously and dynamically adjust its operational parameters and protocols to achieve predefined objectives. The system can learn from the results obtained [6]. The wireless network and the SU with such technology enablement create a new kind of network, called CRN. The operational radio environment of CRN can be characterized by the available radio systems such as the presence of LTE, UMTS, WLAN systems in the proximity of an UE, recent status of the spectrum usage i.e. the utilization of the licensed and unlicensed channels in the current area, coverage areas of different radio systems, and interference levels of them. Different radio systems have different internal state in terms of their load distribution, protocol configuration, transmission power distribution and frequencies used by its radios. The CRN geographical environment is characterized by the orientation and position of antennas of radios of CRN and other co-existing radio systems, the range of them, and also, the number of users with their distribution in a geographic area. The established policies include service agreement between the owner/operators of different radio systems, situated in the area where CRN is installed.

These operating bodies must have some policies on the usage of licensed and unlicensed bands. For example, these policies may describe frequency bands allowed to be used by the CRN under certain constraints, where such constraints include the maximum level of transmission power in operating and adjacent frequency bands to avoid interference to other radio systems. The usage pattern of radio resources includes the usage behavior of the frequencies by different other users, such as TV white band follows a particular pattern of its usage. The users‟ needs or preferences may include its higher demand of QoS for its application and so, higher bandwidth allocation; lower delay and fast download.

A reconfiguration decision is made by using the knowledge on the requirement by users. The decision also depends on some predefined objectives like improvement of spectrum usage. Based on this decision, the CRN tunes operational parameters and protocols of reconfigurable radios. The parameters include frequency range, output power, radio access technology, and modulation type. The learning capability of network is to make the decision to improve its future decisions. However, the learning capability also contributes to acquire knowledge and decision making.

Several deployment scenarios or, use cases of CRN are possible. In the following section, CRN scenarios, which are compatible with the existing cellular system, are discussed. Apart from the mobility events of the previous generation mobile communication networks, the CRN introduces a new kind of mobility event, called spectrum mobility, as discussed in Section 1.2.2.

1.2.1 Types of CRN

Two distinct types of CRN are defined [10]: Heterogeneous type and Spectrum sharing type. These two types are illustrated briefly.

1.2.1.1 Heterogeneous

This type of CRN is considered in these standards: IEEE draft standard P1900.4.1 [11], IEEE 1900.4 [6] and IEEE 802.21 [12]. Heterogeneous type CRN can be defined by a system with one or several operators, operating several Radio access networks (RANs) using the licensed frequency bands in their radio access technologies. These RANs have two types of base stations: one is legacy type, working in a particular radio access technology another one has the reconfigurable capability such that it can reconfigure itself to use a different frequency band, different from the frequencies, assigned to the operator and also, by using different radio access technologies as specified by the radio regulations for these frequency allocations. The operational cost of using legacy type base station is much lower than the cost of using reconfigurable type base station.

Also, there are two different types of terminals used in this type of CRN. One is the legacy type, designed to use a particular radio access technology and so, can only be

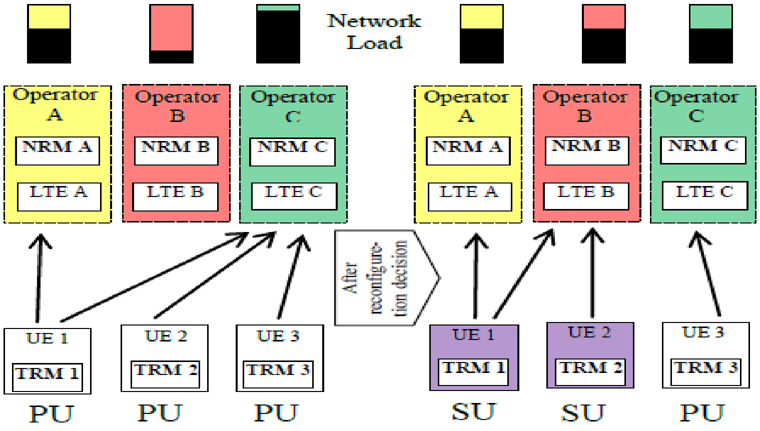

Fig 1 Heterogeneous type LTE-based CRN as defined in IEEE 1900.4

connected with the legacy type base station to one particular operator or other operators having roaming agreements with the home operator. Another type is reconfigurable which can be connected with both legacy and reconfigurable base stations as it has the capability to reconfigure itself to use different radio access technologies. These types of the terminal can handoff to a different RAN, using different radio access technology.

In the heterogeneous CRN, multiple deployment scenarios are possible. For example, the scenarios could be as follows:

- Legacy BS and reconfigurable terminal: Multiple legacy base stations of different radio access technologies and terminals having reconfigurable capability may decide to move from one radio access technology to another. In this case, terminal reconfiguration must be supported from the network side and so, some management entities must be installed in the network.
- Legacy BS and legacy terminal: One example scenario would be like that a legacy terminal may contain multiple simultaneous links with multiple operator‟s networks and sometimes performs cross operator handoff based on the decision from the network and terminal side.

One of the very interesting and realistic use cases of the application of CRN on multiple operators‟ LTE networks, called "LTE-based CRN" is indicated as the "distributed radio resource usage optimization" use case in the IEEE 1900.4 standard.

The co-existence of heterogeneous operator‟s LTE cell is very common due to the huge deployment of 4G mobile communication systems [10] by different operators. The IEEE 1900.4 standard can be applied to optimize radio resource usage and improve QoS. As shown in Figure 1.3, operator A, B and C operate LTE A, LTE B, and LTE C in three frequency bands in the same area. UE 1 and 2 have multi-homing capability where UE 3 is without multi-homing capability. So, UE1can have simultaneous connections with LTE A and C. UE 2 and 3 can have one LTE connection with LTE C. Currently, operator C is overloaded and so, it has poor QoS consistency level while operator B is underloaded with high QoS consistency level. So, the load is imbalanced with poor QoS at operator C‟s network. The entity network reconfiguration managers (NRMs) of all operators analyze context information such as load, QoS, etc. and dynamically create resource selection policies.

The terminal reconfiguration managers (TRMs) receive the information from NRMs and detect an imbalance of the load. TRM then, make reconfiguration decisions and requests the corresponding reconfiguration of their UEs. As UE 1 and 2 are with multi-homing capability, the TRMs of UE 1 and 2 decide to change its connection from LTE C to B. The TRM of UE 3 is without multi-homing capability and so, decides to remain connected with LTE C. Now, the load almost balanced and QoS is increased for operator C. The communication between NRM and TRM can be done by a logical channel, called a cognitive pilot channel (CPC), proposed in [13], by modifying PDSCH. CPC based network access is a promising scheme in LTE CRN, which can provide fast network access and put no strict requirements on UEs. The switching may also occur between operators to improve overall spectral efficiency. For example, a user at the cell edge, with bad channel condition and so, a high ratio of RBs required per packet, can be transferred to a comparatively closer network with better channel condition.

However, the distributed radio resource usage optimization application may improve the overall network efficiency, but a single operator‟s radio resource management becomes more challenging due to operator level roaming of UEs. Several current research work [14] [15] on CR application over heterogeneous networks, proposes strict priority of operator‟s premium users, named PUs, over the roaming user, named SUs. The end goal is to serve traffic flows from SUs without violating the QoS requirements of the PUs.

1.2.1.2 Spectrum sharing

In the spectrum sharing CRN, several RANs using the same or different radio access technologies can share the same frequency band. This type of CRN is standardized in IEEE 1900.4, IEEE draft standard P1900.6, IEEE draft standard P1900.4a, IEEE 802.11y, IEEE draft standard P802.19.1, IEEE draft standard P802.11af, IEEE draft standard P802.22, IEEE draft standard P802.22.1 and standard ECMA-392. Recent works on it lie mainly on incorporating TV white space into LTE‟s own spectrum and transfers some of the traffics from LTE to TV band at the time of overloading [13]. In this case, the CRN capabilities must protect the primary service (television broadcast) and also, the coexistence between other secondary systems. Another example scenario is that spectrum from licensed systems is shared by a cognitive radio base station (CRBS) and cognitive radio terminals (CRTs). The CRBS and the CRTs using CRN capability senses the frequency band to find temporarily vacant frequency bands. The CRBS and CRTs then can reconfigure themselves to use these vacant/idle frequencies. The network reconfiguration manager supports such reconfiguration.

One example scenario, called dynamic spectrum sharing is illustrated in IEEE 1900.4 standard. A particular frequency band (like TV band) is shared by a legacy operator‟s RAN i.e. the radio access technology of this RAN is enriched with the shared frequency band. In that case, the UE having CR capability, operating in that frequency band, can access the RAN for its data communication. The UE may be from another operator‟s network and try to access another network. The preference of the network for the UE depends on several parameters like charging, QoS, device battery power required and also, some special offer from the operator. If multiple such base stations (sharing TV band) from multiple operators exist in a common area of service, a UE can access any one or, both of them at a time. If the operators support roaming agreement among them, the UE can switch from one RAN to another for a better opportunity. The network entity, NRM, and the UE entity, TRM, shown in Figure 1.3 (these two entities are common in both types of CRNs as decision taking in a distributed way happens in both cases), jointly take a decision on this opportunistic network access process. The UE here acts as an SU in both the operator‟s network. The end goal of this kind of CRN is also not to violate the service of the PUs while allowing the SUs to access the network. In the spectrum sharing CRN, an SU can access a spectrum only during the absence of a PU. Whenever a PU requests for a spectrum, currently occupied by an SU, the SU has to leave that channel immediately and move to another empty channel if available (else suspend communication for the time being). This process of switching from one spectrum to another is called spectrum mobility [16] [17]. In the following section, the event, spectrum mobility is discussed.

1.2.2 Mobility in CRN

In dynamic spectrum sharing (i.e. in the spectrum sharing type CRN), spectrum mobility is an important event to consider. Without changing the regulation of licensed spectrum allocation, CRNs can maximize the spectrum utilization by accessing spectrum opportunistically. When the PUs is idling, the SUs can make use of unoccupied spectrum bands opportunistically. There are four important functions for the spectrum management in the CRN [18]: spectrum sensing, spectrum sharing, spectrum decision and spectrum mobility. In spectrum sensing, CR nodes look for spectrum holes that can be employed for SU communication. Based on the sensing results, the best available channel is decided for the SU communication. Spectrum sharing manages channel access among the CR nodes. Spectrum mobility is the event of switching from the current channel, demanded by a PU, to an idle channel to resume the ongoing communication.

The main goal of spectrum mobility is to perform seamless channel switchover while satisfying performance of SU communication in progress. Spectrum mobility has two processes: spectrum handoff and connection management. Spectrum handoff is the process of transferring ongoing communication from the current channel to another channel. It creates an additional delay in the ongoing communication that eventually affects SU performance. The connection management process adjusts and manages protocol stack parameters depending on the underlying wireless technologies.

II. BLOCK CHAIN MANAGEMENT

The block chain is a circulated record that records exchanges in sequential request [3]. The record is kept up with by each taking an interest hub in a blockchain network dissimilar to brought together record where record is kept up with on a worker and all hubs update exchanges on that worker as displayed in figure 2

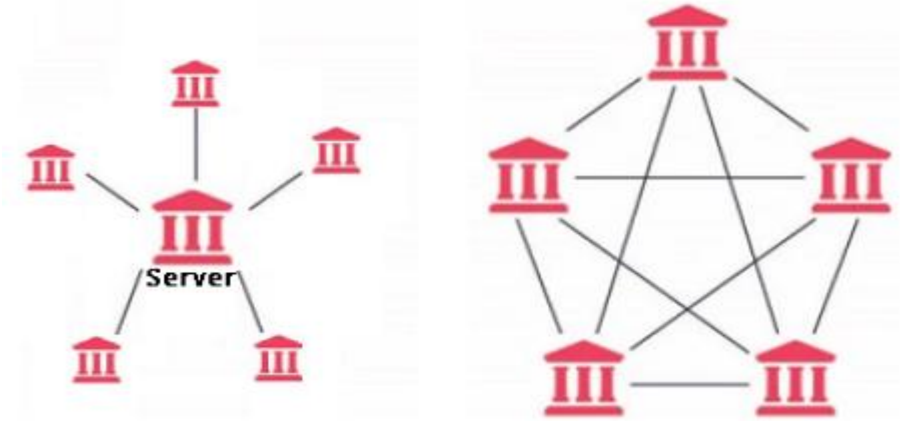

Figure 2: Centralized Ledger and Distributed Ledger

Blockchain has the following features which makes it a better alternative for business Processes.

- Immutability: Immutability implies no change after the exchange gets finished. Blockchain depends on hashing that creates special hash code for square of exchanges and any adjustment of exchange brings about change in hash code subsequently any change can be recognized and disposed of right away. Permanence is accomplished by making check and approval computational concentrated with the goal that it decreases the practicality of any assaults on control of blockchain information.
- Secure: Blockchain is secure as it includes broad utilization of cryptography to guarantee classification and exchanges are planned with extraordinary and secure personality of clients. This is accomplished by utilizing the private key of clients.
- Privacy: Privacy is tied in with securing individual character data of clients and blockchain guarantee that utilizing cryptography.
- Distributed: Transactional information in blockchain is put away in conveyed way and all organization hubs have a duplicate of complete chain of information to guarantee no weak link. At whatever point an exchange is started by a hub the duplicate of that exchange is shipped off every one of the hubs on the organization.
- Transparence: Transparency is guaranteed by including all hubs in exchange confirmation and all taking part hubs have a duplicate of the total blockchain.

III. BLOCKCHAIN-BASED ACCESS CONTROL

This section deliberates the different methodologies employed for blockchain-based access control and also privacy-based data sharing and retrieval process in blockchain-based cloud system. Here, the research papers are analyzed and several techniques employed for access control, privacy-based data sharing and retrieval method are divided into divided into four kinds, namely ledger-based blockchain techniques, encryption-based approach, smart contract-based blockchain model, and Ethereum-based blockchain model. Figure 3 exposes the categorization of different approach used for access control, privacy-based data sharing and retrieval schemes.

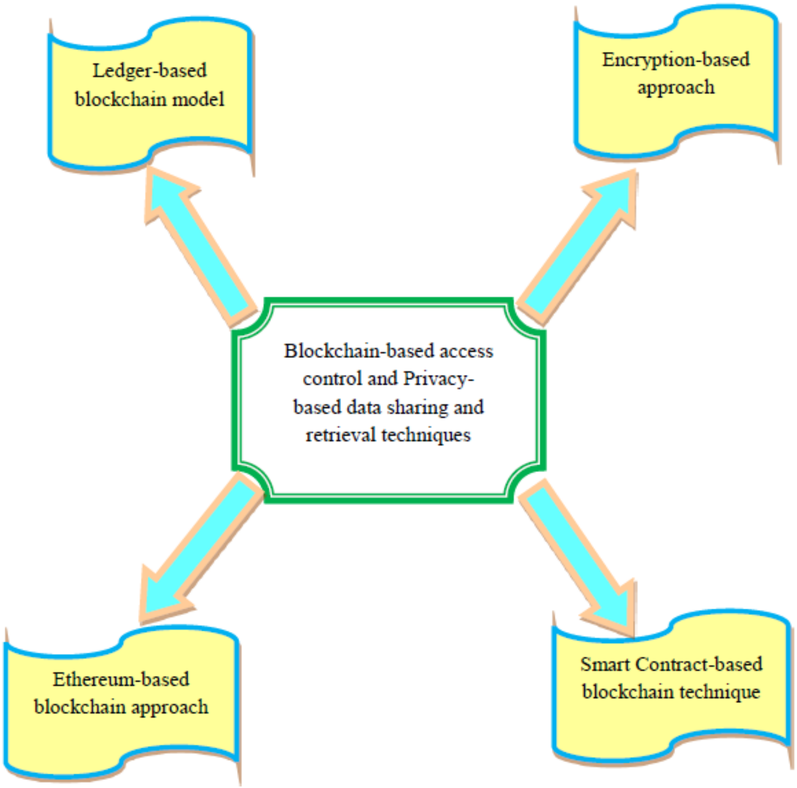
Ledger-based blockchain model
Encryption-based approach
Blockchain-based access control and Privacy-based data sharing and retrieval techniques
Ethereum-based blockchain approach
Smart Contract-based blockchain technique

Figure 3. Categorization of different approach used for access control, privacy-based data sharing and retrieval approaches

3.1 Ledger-based blockchain model

The existing research works based on ledger-based blockchain techniques are elucidated as follows, Rajput, A.R et al. [56] developed emergency access control management model (EACMS) for health record using blockchain system. In this model, various rules were employed based on smart contracts for controlling emergency situations and period length. Moreover, hyperledger composer was applied for generating Business Network Archive (BNA), which identifies the system capacity. Here, every transaction was disturbed with data fetching and authorization from ledger, which was performed by smart contracts. Besides, this model functions depends on smart contracts of ledger for providing effectual, secured and auditable system.

Qin, X et al. [75] introduced blockchain driven access control model through numerous attribute authorities for a secure cloud data sharing model. In this model, Shamir secret sharing and Hyperledger Fabric method was devised for implementation process, where every attribute was managed mutually through various authorities for avoiding single point failure. Moreover, the advantages of blockchain model was considered for establishing trust between multiple and develops smart contracts for estimating tokens for attributes, which decreases the computation and communication overhead in data user. Additionally, blockchain model assists for recording access control method in protected and auditable manner.

Ali, S et al. [81] devised blockchain-based decentralized data storage model. The metadata of files was accumulated on blockchain, while actual files were accumulated by Distributed Hash Tables (DHT) at various positions based on peer to peer network. Furthermore, the devised off-chain storage model obtains low latency and high throughput. This algorithm effectively reduces the project requirement on central computing resources for processing, uptime and accumulating.

Thwin, T.T. and Vasupongayya, S [87] presented blockchain enabled access control method for preserve privacy for personal health record scheme. In this model, blockchain was included for supporting tamper resistance feature. Moreover, cryptographic and proxy re-encryption algorithms were devised for preserving privacy of system. In addition, the features, like tamper resistance, revocability consent, and auditability were included for better performance.

Moreover, proxy re-encryption model enables the user for sharing their decryption abilities with others for security purpose.

3.2 Encryption-based techniques

This section explains about the literature survey of various encryption-based approaches used for access control and data sharing process,

Ma, M et al. [58] modelled Blochchain-based Distributed Key Management Architecture (BDKMA) for access control in Internet of Things model. In this model, fog computing structure was used for decreasing the latency and multi block chains operated in cloud for obtaining cross domain access model. In addition, blockchain model was applied for satisfying extensibility needs, fine grained auditability, decentralization, high scalability and privacy preserving standards for access control. Furthermore, system operation models as well as various authorization assignment nodes and group access models were devised for supporting system extensibility. The dynamic transaction collection duration alternations enable the system capacity for several structures. This algorithm effectively increases the performance of system and scalability with regards to network size.

Lin, Cet al. [62] designed blockchain-based system for secure mutual authentication, named BSeIn, for enforcing fine-grained access control systems. This technique mainly includes multi receiver's encryption, integrated attribute signature and message authentication code, and it affords security and privacy assurance. Here, both attribute signatures and blockchain was integrated for authenticating terminals, authenticate gateways as well as message authentication code. Furthermore, multi receiver's encryption process was used for offering confidentiality. Meanwhile, smart contracts were utilized for ensuring scalability and the request process was done by interaction of smart contracts.

Sun, J. and Fang, Y [86] modelled cross domain data sharing approach in electronic health data. In this technique, cryptographic model was included for enabling secure sharing of data in patient data privacy. This approach effectively integrates on-demand revocation, and fine-grained access control as well as access control was done using delegation model. Moreover, delegation process was included by both proxy signature-based and role-based model.

additionally, fine-grainead access control model was devised for satisfying more delicate as well as stringent control needs.

Gao, Het al. [88] introduced Blockchain-Based Security Sharing technique, termed BSSPD used for personal data with fine-grained access control. This algorithm was designed by incorporating ciphertext-policy attribute-based encryption (CP-ABE), blockchain as well as IPFS. The DO encrypts data sharing as well as accumulates the data on IPFS for increasing scheme decentralization. Furthermore, decryption key and address of shared data was encrypted using CP-ABE model. Here, encryption was performed depends on particular access policies as well as data owner utilizes blockchain for publishing information and distribute keys. The ciphertext keyword search model was employed for protecting data user privacy during the data retrieval process.

Ma, X et al. [90] designed effectual data sharing approach based on blockchain. At first, data owner shares the data along with multiple users, who fulfils the access policies. After that, searchable encryption approach was employed for solving the complexity of cipher text query. Moreover, data sharing was performed without the interaction of data owners with data queries. Here, CP-ABE algorithm was introduced for data encryption process. In addition, the CP-ABE approach effectively increases the data security during the data sharing process.

3.3 Ethereum-based blockchain approach

This section explicates various research works based on Ethereum-based methods for access control and data sharing and retrieval process,

Dagher, G.G et al. [61] presented privacy preserving model for interoperability of EHR based on blockchain model. In addition, this method uses smart contracts in Ethereum-based blockchain for delicate access control and data complication. Furthermore, more advanced cryptographic approaches was applied for security process. This model accumulates hashes of data references, when transferring definite query link information in private contract. Meanwhile, proxy re-encryption method was employed, which accumulates the small encrypted records and store keys on blockchain. After that, smart contract was utilized for access control by changing providers and patient's roles as well as third parties on block chain. This algorithm obtained enhanced decentralization level.

Wang, Set al. [37] modelled data storage and sharing model in decentralized storage structure. Furthermore, this technique incorporates Ethereum blockchain, decentralized storage system interplanetary file as well as Attribute-Based Encryption (ABE) approach. Moreover, data owner has the capacity for allocating secret key to encrypt shared data and data user through signifying success policy. The keyword search operation on cipher text of decentralized storage model was applied using smart contract on Ethereum blockchain, which solves cloud server issues. Furthermore, encrypted keyword index for shared file was produced and the encrypted keyword index was accumulated on Ethereum blockchain. After the deployment of smart contract, smart contract retrieves the accurate search result.

2.2.4 Smart Contract-based blockchain methods

The literature survey of existing research works based on Smart Contract-based blockchain techniques are elucidated as follows,

Ali, Get al. [42] developed Blockchain-based permission delegation and Access Control in IoT (BACI). This model was devised for permitting delegation as well as access control for IoT model, and it highly demands on query and event base permission allocation. After that, blockchain structure was applied for making decentralized, delegation services, trusted, secured and verifiable structure. The node with minimal permission group was allocated as well as essential permission was delegated to node in an event. This model mainly includes various elements, such as user device, IoT manager, IoT device, blockchain manager, smart contract, application manager and blockchain. This model efficiently controls the access control regarding to constrained devices.

Sultana, Tet al. [64] presented data sharing model along with access control approach relies on blockchain-based smart contracts in IoT. This approach was mainly designed for resolving various issues regarding authentication and trust for access control in IoT. Here, multiple smart contracts, including Register Contract (RC), Access Control Contract (ACC), and Judge

Contract (JC) were included for affording effectual access control management, where ACC controls the access system as well as RC was utilized for authenticating users in system. In addition, JC applied behaviour judging model in order to identify the subject the misbehaviour. Once misbehaviour detection was completed, then penalty was defined for the each subject.

Chen, Y et al. [65] introduced blockchain-based medical data sharing model using attribute enabled access control and privacy protection. In this technique, K-anonymity as well as searchable encryption approach was included for medical data sharing. Moreover, Hyperledger Fabric, consortium blockchain were employed for permitting data users in order to search encrypted medical data records. The attribute-based access control technique was included for assuring the user with appropriate attributes. Here, searchable encryption and K-anonymity effectively shares the medical data without the privacy leaking. In addition, prototype model was employed based on chaincode of Hyperledger Fabric.

Jaiman, V. and Urovi, V [67] developed consent approach for blockchain-based health data sharing policy. In this model, smart contract was utilized for representing individual consent for enabling data requesters. Then, the dynamic consent approach was extended by two schemes, such as Data Use Ontology (DUO) and Access Matrix (ADA-M). In this, DUO models individual consent of users, whereas ADA-M defines the queries from data request. The Ethereum blockchain was applied and estimates various data sharing circumstances.

Liu, Jet al. [68] presented blockchain-based privacy preserving data sharing model used for EHR electronic medical record, named as BPDS. The actual electronic medical record was accumulated securely in cloud as well as indexes were reserved in interfere proof consortium blockchain. Furthermore, the complexity of medical data leakage was highly decreased and the indexes of blockchain guarantees, that the electronic medical record was modified. Moreover, secure data sharing was automatically accomplished for pre-defined access permission of patients by smart contract. In addition, joint design of access control model as well as content extraction signature model was applied for affording privacy preservation in data sharing model.

Zhang, Y et al. [69] modelled blockchain structure for data sharing with fine grained structure in IoT. In this model, consensus technique was considered as Byzantine fault tolerance model. Originally, IoT data was encrypted after that, smart contract model was incorporated with attribute encryption model for realizing about fine grained sharing. Moreover, access strategies was placed on encrypted key, such that encrypted key was encrypted via attributes in order to decrypt the cipher text. After that, smart contract was employed for ensuring the scalability of access control table. Here, every data sharing request was interacted with smart contracts by transactions.

Xu, Het al. [70] introduced blockchain-based data security sharing model with fine grained access control. At first, hierarchical attribute-based encryption model was applied, which utilized hierarchical attribute model and multi level authorization center. In this approach, flexible and finer grained access control was implemented through allocating user attributes for various authorization centers. After that this model was integrated with fabric blockchain approach for resolving the large decryption cost issues for users in IoT. Additionally, smart contract in blockchain was performed high difficulty partial decryption model for decreasing user decryption overhead. Here, blockchain was utilized for realizing traceability of historical function for satisfying security needs of data restriction. At last, hierarchical attribute-based encryption model was included for obtaining better performance.

Yang, C et al. [40] devised blockchain-based access control model with privacy protection in cloud system, named AuthPrivacyChain. Initially, account address of node was utilized into blockchain as uniqueness as well as decreases access control permission of data, which was encrypted and accumulated in the blockchain. Then, access control process authorization revocation as well as authorization was devised. Here, this model was developed depends in Enterprise Operation System (EOS) as well as it protects authorized privacy. This approach encrypts and accumulates the access control rights in blockchain model, which successfully protects user privacy. Additionally, this model ensures availability, resource accountability, integrity, confidentiality and resource accountability as well as resists several internal and external attacks.

Makhdoom, I et al. [73] presented blockchain enabled model for privacy preserving and data sharing in smart cities, termed PrivySharing. This algorithm guarantees the user data for obtaining confidentiality and it was exposed to stakeholders included in smart contracts. After that, data owners were rewarded to share their data along with third parties or stakeholders. In addition, various European Union General Data Protection Regulation (EU GDPR) needs, like accessibility, sharing and purging with data owner.

Nguyen, D. Cet al. [76] devised blockchain for electronic health data sharing of mobile cloud enabled E-health system. A trustworthy access control model based on smart contracts was devised for obtaining secure data sharing between medical providers and patients. Moreover, prototype implementation was done based on Ethereum blockchain in real data sharing model on mobile application through cloud. Finally, peer to peer IPFS along with blockchain was combined for obtaining decentralized data sharing and data storage.

Shrestha, A.Ket al. [89] developed novel block chain model for user modeling with blockchains, which permits users for sharing the data without losing control and ownership. Here, user data obtained from repository was transformed to open data structure through shared stream into blockchain, such that other nodes capably process as well as utilize data. Furthermore, smart contracts were included, which verifies and performs agreed terms of data as well as converts the digital tokens as incentive to user. IN addition, smart contracts perform double deposit security process for guaranteeing the confidentiality. The blockchain and off-blockchain were integrated for generating data sharing and management process for privacy and security.

Guo, Y et al. [92] introduced blockchain-based structure for secure as well as reliable data sharing in distributed system. Here, data owner's permits for outsourcing their data to distributed model in encrypted structure. The data owner allocates the secret key for authorized users without extra round interface for creating acceptable search tokens by influencing smart contracts of blockchain. In addition, this approach effectively resolves the trust problems of query authorization. Finally, secure local index structure was designed for supporting encrypted keyword search along with forward privacy as well as blockhead overhead was moderated.

2.2.5 Other access and data sharing techniques

This section presents the various other access control as well as data sharing and data retrieval method for blockchain enabled cloud techniques are explained as follows: Ding, Set al. [34] presented novel attribute-based access control approach for Internet of Things structure. In this method, blockchain methodology was employed for recording attribute allocation for avoiding data tampering and single point failure. Additionally, access control scheme was optimized for obtaining lightweight computation and better effectiveness for IoT model. This model was simplified the access control structure as well as two parties by hash functions and signatures. Here, minimal quantity of consortium nodes was utilized for constructing this system for resisting several attacks.

Ouaddah, A et al. [32] devised privacy preserving access control method using blockchain technology in Internet of Things. Here, new decentralized pseudonymous as well as privacy

preserving authorization management model for controlling constancy of blockchain and access control of controlled devices. Moreover, authorization tokens were selected as access control model, which is delivered by emergency cryptocurrency solution. Here, blockchain was utilized for guaranteeing the access system in distributed structures as well as policies was ensured by interacting every entities.

Liu, X et al. [66] devised blockchain-based medical data sharing and data protection model for improving electronic health system. At first, several security properties including openness, decentralization and tamper resistance was satisfied. Additionally, reliable model was generated for accumulating medical data accessing historical data, while considering privacy preservation. After that, symptoms matching model was provided among each patients, and it permits to conduct mutual authentication as well as produces session key. Besides, enhanced consensus model was included by enhancing conventional delegated proof of stake, which was more reliable, secure, and proficient.

Eltayieb, Net al. [72] developed blockchain-based attribute enabled signcryption model for safe data sharing in cloud model. This approach satisfies various security need of cloud computing including unforgeability and confidentiality. Additionally, smart contracts were introduced in this technique for solving cloud storage issues. Here, this algorithm was integrated with the benefits of encryption and signature for obtaining confidentiality. This algorithm mainly depends on access structure tree for enforcing user access policy in various functions, like encryption and decryption.

Zheng, X et al. [54] modelled blockchain-based personal health care data distribution in cloud. A theoretical model to share individual continuous dynamic health data through blockchain structure on secure and transparent mode. In addition, data quality inspection approach using machine learning approaches was employed for controlling data quality. The General Data Protection Regulation (GDPR) manner was developed for enabling the users and shares the health data securely. In addition, the high quality personal health data was gathered for data sharing process. Then, various solutions was employed for sharing huge dimensional incessant dynamic data hast pointers for storage location. After that, the restrictions of continuous dynamic health data by incorporating cloud storage and blockchain. The huge dimension of health regarding data was accumulated in encrypted format on cloud. Then, data quality validation model was considered in this model for controlling data quality in both software and hardware by machine learning models.

Zhang, Z et al. [77] developed secure and location-sensitive data sharing process for cloud system. The new position verification model, named Ears was designed, which prevents both lengthening and shortening the distance fraud. Furthermore, it has capacity to tolerate the lengthening distance attack. In addition, Ears was included on higher network layer of wireless communication, which existing Distance-Bounding Protocol (DBP). This approach effectively avoids the strict time synchronization.

Zhang, X et al. [78] presented identity-based authorized encrypted diagnostic data sharing model in cloud system. This approach enables the user for authorizing and assistant in order to manage complicated encrypted diagnostic data sharing process. In addition, the data sharing method was performed by means of identity enabled encryption model with keyword search process. Meanwhile, patient can recover the medical data by submitting the trapdoor of related keyword. Besides, the security system for cipher text indistinguishability, authorization unforgeability, and trapdoor privacy was considered for data sharing process.

Sundareswaran, Set al. [79] modelled novel highly decentralized information accountability structure for data sharing in cloud. Here, object centered model was developed, which enables the closing logging model with user data. The Java Archives (JAR) file was included for generating travelling and dynamic object as well as guarantees any access to user data. In addition, distributed auditing model was implemented for strengthening the user control. This model was highly decentralized and platform independent, which does not need any dedicated storage system. The log record structure was updated for providing more assurance of authenticity and integrity.

Liu, X et al. [80] developed secure multi owner data sharing model, termed Mona for dynamic sets in cloud. The approved users were directly decrypt the data files devoid of communicating with data owners. In this technique, encryption computation as well as storage overhead was independent with quantity of revoked users. Moreover, user revocation was obtained by revocation lost exclusive of updating secret keys of residual users. Moreover, privacy preserving and secure access control to user was afforded, which assures any member in group to use cloud

resource. Additionally, actual identities of data owners were exposed through group manager, while disputes happen.

IV. LITERATURE REVIEW

Dubey Rajni et.al (2012) had recommended that Wireless-Spectrum was important, so these were reliably required for dynamic-shared range procedures just as the astute remote corresponding system, for instance, C.R.N. Notwithstanding the way that, C.R.N gave dependability, versatility, mindfulness, adaptability and flexibility to its customers yet it had moreover opens the doorway for mostly no. of risks and attacks. In this study, distinctive possible attacks and perils along with the potential methodologies are clarified. Moreover proposed a trusted securities technique empowering CR in order to gain the distribution calculation, conservers are accessible in CR system.

Parvin Sazia & Farookh Khadeer (2012) had given C.R consequently it was viewed as a fundamental (essential) framework to recognize whether a particular piece of the radio range was by and by being utilized, and it is used to rapidly include the pointless range without upsetting the transmissions of various customers. As CR had dynamically features, so an individual from CRNs might joint or left out the system whenever it is required. Such Features imply that the issues of secured correspondence in C.R.Ns turns out to be more basic than for another possible wire-less systems. Such System therefore proposed a trusted securities framework for communities dependent C.R.Ns.

Pei et al. (2012) have proposed C.R been viewed as the mostly encouraging strategy to eliminate the issues of spectral utility. C.R could examine the spectral bands & recognize free channeling that would be utilized by cognitives clients without any interference to essential (primary) clients. Because of the different dynamic attributes of C.R.Ns, adjustment & secured interaction are of more prominent approaches than different wireless systems. These papers proposed a dependent trust administration mechanism in terms of cognitive cycles, that could refer framework BER adequately & making out spectral distribution more sensible and secure. The final, simulated o/ps defined that the given schemes had the benefits of solid adjustment & least error rating.

Wang-Ji and Ray-Chen (2014) had proposed C.R organizations being applied methodology for range constraints. S.U get detecting instrument to taken-out in the fundamental customer's accessibility. This stir develops a trusted-based data gathering way to deal with adjust dangerous SU attack in range identification of the intellectual radio frameworks.

Bhattacharjee et al. (2015) have proposed communitarian location. An intellectual radio center takes part with others in the range recognition measure for a more exact detecting decision. A dangerous center point might dispatch S.S.D.F that the located recognizing reports are mutilated before it accomplishes the Fusion-Centers. The tasking of F.C was to assemble all out area detecting reports from the teamed up centers, thusly it arrives at the last detecting decisions. Chen et al. (2011), characterized a numerical system to portray confirmation for CRN correspondence yet this structure doesn't propose a total technique to build up trusted to guarantee security in C.R.Ns.

Dubey Rajni et al. (2012), proposed an original range detecting plan which can recognize getting out of hand SUs and settle on a general detecting choice by sifting through their revealed range detecting results, however their methodology didn't show how hubs could partake in range partaking in CRNs.

Bhattacharjee et al. (2015) proposed a methodology for synergistic range detecting in C.R.Ns yet themselves didn't showing however such methodology can improve securities in C.R.Ns. León et al. (2010) likewise given a strategies for securing helpful range detecting in CRNs yet they didn't show how security angles are improving to guarantee secure correspondence in C.R.Ns. Range identifying, range organization, otherworldly shared & portability of a range were a part of the hardships in C.R.N securities.

Guaranteeing dependable reach area is distant from everyone else the crucial applications in C.Rs. The major sign appraisal is idea in the introduced assessment. Trusted on range distinguishing happens assuming that the key signs are imitated and seen definitively. E.g, a pernicious client likewise as software engineers can translate the major (fundamental) client hail and incorporate the reach for intolerance (Ian F Akyildiz 2006).

The attack can be distinguished through transmitter affirmation strategies and area hell frameworks. Further, an intellectual customer recreates the fundamental (essential) customer for singular advantages. The fundamental sign can't be perceived as far as impedances at area gadgets. Fundamental customer signal distinguishing proof gets irksome if these usage the spread range signal or changing the boundaries by a threatening customer. These issues can be discarded using the clouding usage (Haykin and Simon 2010).

Further, the cloud application to take out the incorporated terminal issue was overseen in the papers. The reaction for check issues were given in (Chen et al. 2008) & limit recognizing could be seen sufficiently via different clients in a charming circumstance. At the point when remote reach is recognized, the better open groups would be seen through neighborhood perceptions and quantifiable messages. The ordinary controlling issue consolidates the trading of security keys betn the focuses. The endorsement among the focuses gives security and reliability of the exchanges. These techniques gives the ideal protections anyway the mysterious hubs issue really remains.

The blockage issue, covered up terminal issue, transfer of keys bet^n the center points and dangerous customer acting could be discarded via the clouding usage. The securities to clouding actually stays an opened issue. Vindictive development could be from externally or amongst the intellectual customers. Uniting the cryptographically frameworks or modernized mark dependent fundamental sign ID might help in perceiving the threatening customers. More work is needed toward this path (FCC 2003).

Range versatility incorporates ordinary control channel, working recurrence range just as the area info. It needs the present area of the fundamental customer and working reach, with the goal that the auxiliary customer can clear the had range when PU enters. Range convey ability depends on the fundamental customer passageway and auxiliary customer relocated. The clouding usage would settle various attacking & covered nodes issues in intellectual frameworks like abrupt section of the fundamental customer (Chen 2008).

Mao et al. (2011) proposed an original trust-mindful asset assignment plot in a concentrated C.R.Ns that dependability is estimated as a vital factoring for S.Us to accessing the framework assets. The plan can recognize acting mischievously SUs & channel out pernicious assaults as amplifying the complete bit pace of S.Us yet such methodology didn't proposed a structure for a dependability estimation to guarantee secured range partaking in C.R.Ns.

Pei et.al (2012) told a trusted the executives modeling via the entire psychological cycling for concentrated C.R.Ns to tackle the securities dangers buying via conniving elements, for example, egotistical, malevolent, and perfect hubs, yet they didn't show how range dynamic happens in a range sharing component. In any case, like a trusted limits sharing system had n't being given in the writing to defeat the delicate securities dangers in C.R.Ns. To sum up the issue, there was no approach proposing in the writing that range could be partaken in a safe manner in C.R.Ns. To conquer the above issue, a Trusted techniques for Securing and dynamic range accessing in CRNs is proposed.

Parvin et al. (2011) have suggested that the quick advancement of distant applications, Cognitive Radio (CR) has been considered as a mentioning thought for improving the utilization of obliged radio range resources for future far off trades just as versatile processing. The exceptional conduct of Cognitive Radio Networks (CRNs) makes security to be an intricate methodology. Since a person from CRNs might joined/left the framework at whatever point it is conceivable, the challenges of supported secureness correspondence in CRNs ends up being mostly fundamental than for other common distant frameworks. This work thusly proposes electronic mark based secure correspondence for perceiving compelling fundamental customers in CRNs. The security examination is analyzed to guarantee that the proposed approach achieves security verification.

Muhammad Ayzed Mirza et al. (2018) resolved an issue of deferral brought about by a band choice cycle that straightforwardly influences the security and execution. They have proposed a group based trade control data with other bunch heads and other customary hubs.

As indicated by CRN design, the key hubs (León et al. 2010) produce and store the entirety of the significant information, for example, the distinctive keys that are utilized to convey in the arrange and play out the significant responsibilities regarding keeping up with the security of the organization. There isn't a lot of work in the writing which chooses a hub as the vital job to work with framework security.

Ping xie et al. (2018) considered the physical-layer security for transmission in underlay psychological radio organizations, where comprising of an essential source-objective pair, an optional transmitter collector pair and a typical busybody. To send information in got and dependable way, they proposed a transmission convention for an underlay intellectual radio organization.

León et al. (2010) have proposed a scholarly radio framework that involves Cognitive Base Station (CBS) and distinctive Cognitive Users (CUs) inside seeing various snoop, where CUs communicate their stacks of info to C.B.S under a fundamental customer's Q.o.S constraining as the busybody co-work to hinder the intellectual transmissions from CUs to C.B.S.

Weifeng Mou et al. (2017) has investigated the security performance of multiple relaying CRN with collaborative distributed beamforming scheme against passive eavesdropping attacks. El-Hajj (2011) have proposed Cognitive Radio (CR) as a novel innovation that guarantees to resolve the spectral issue by permitting secondary clients to exist together with essential clients without making impedance to their correspondence.

Here, a brief diagram of the CR innovation is given as a point by point investigation of the security assaults focusing on Cognitive Radio Networks (CRNs) together with the related mitigation methods. The assaults as for the layer they target beginning from the physical layer and traveling to the vehicle layer is classified.

V. PROBLEM FORMULATION

This part plans a psychological remote organization model dependent on block-chained. The model incorporates the administration focal point of the block-chained, an essential client, a psychological base station (combination focus), and numerous hubs (intellectual clients). A few hubs are in range detecting state, and different hubs are in quiet state. This model is a brought together helpful range detecting model. Every hub can just trade data with the combination community. The detecting data of every hub is shipped off the combination place for preparing, and the combination community takes care of back data to every hub.

There is no immediate correspondence between hubs, so a unified engineering assists with further developing data preparing productivity [26]. The combination place isn't just liable for correspondence with the hubs, yet additionally for correspondence with the blockchain the board community, sending the nodes information to the administration places for capacity, and the square chain the executives community will likewise call the node information to the integrated places. The square chain the board community and the combination place are a significant collaboration system for choosing dependable hubs. it tends to be seen that not all hubs take part in helpful detecting simultaneously, however a few hubs are conceivable noxious hubs. This is on the grounds that the hubs are assembled, and the hub with the most noteworthy trust esteem is chosen to take an interest in helpful detecting, vindictive hubs are hindered from taking part in agreeable detecting. The object is to further develop energy productivity and augment the augmentation the functioning existence of psychological organization. In the reason of fulfilling the detecting execution, the energy utilization is diminished. The justification gathering the hubs and assessing the trust worth of the hubs is principally on the grounds that the topographical areas of the hubs are unique, and the hubs near the essential client get solid signs, which can be gotten acceptable insight exactness based on devouring less energy. At the point when the way misfortune brought about via the significant gaps via the essential client is bigger, or the channeling isn't acceptable, & the hub via extreme Reweighed blurring gets more fragile signs from the essential client, and requirements to performing longest detecting activities, & devours most energies could making out detecting decisions. Since the essential client's sign is frail and handily influenced by obstruction, these hubs are inclined to making wrongs decisions. These judging outputs were not helpful for the assurance of the essential client, that carries difficulties to the securities of psychological remote organizations. Thusly, it is essential for the security work of psychological remote organizations to assess hubs and select hubs with high unwavering quality to take an interest in helpful detecting.

VI. CONCLUSION

The existing research works related to access control and data sharing for blockchain driven cloud techniques are explicated in this chapter. The various techniques implemented for efficient access control and data sharing models are categorized into four categories, namely ledger-based blockchain techniques, encryption-based approach, smart contract-based blockchain model, and Ethereum-based blockchain, which is elaborated in above section. Furthermore, the research gap and issues experienced in access control and data sharing for blockchain enabled cloud techniques are also included in above sections.

REFERENCES

[1] Z. He, Z. Cai, J. Yu, X.Wang, Y. Sun, and Y. Li, ``Cost-efficient strategies for restraining rumor spreading in mobile social networks,'' IEEE Trans. Veh. Technol., vol. 66, no. 3, pp. 2789_2800, Mar. 2017.

[2] L. Xie, Y. Ding, H. Yang, and X. Wang, ``Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs,'' IEEE Access, vol. 7, pp. 56656_56666, Apr. 2019.

[3] S. Iqbal, A.W. Malik, A. U. Rahman, and R. M. Noor, ``Blockchain-based reputation management for task of_oading in micro-level vehicular fog network,'' IEEE Access, vol. 8, pp. 52968_52980, Mar. 2020.

[4] Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen, and Y. Zhang, ``Blockchain empowered arbitrable data auditing scheme for network storage as a service,'' IEEE Trans. Services Comput., vol. 13, no. 2, pp. 289-300, Mar. 2020.

[5] X. Zhou, W. Liang, K. Wang, H. Wang, L. T. Yang, and Q. Jin, ``Deep learning enhanced human activity recognition for Internet of healthcare things,'' IEEE Internet Things J., vol. 7, no. 7, pp. 6429_6438, Jul. 2020.

[6] J. Shi, R. Li, andW. Hou, ``Amechanism to resolve the unauthorized access vulnerability caused by permission delegation in blockchain-based access control,'' IEEE Access, vol. 8, pp. 156027-156042, Aug. 2020.

[7] T.-H. Kim, R. Goyat, M. K. Rai, G. Kumar, W. J. Buchanan, R. Saha, and R. Thomas, ``A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks,'' IEEE Access, vol. 7, pp. 184133_184144, Dec. 2019.

[8] Y. Xu, C. Zhang, G. Wang, Z. Qin, and Q. Zeng, ``A blockchain-enabled de-duplicatable data auditing mechanism for network storage services,'' IEEE Trans. Emerg. Topics Comput., early access, Jun. 29, 2020, doi: 10.1109/TETC.2020.3005610.

[9] S. Zhu, Z. Cai, H. Hu, Y. Li, and W. Li, ``ZkCrowd: A hybrid blockchain- based crowdsourcing platform,'' IEEE Trans. Ind. Informat., vol. 16, no. 6, pp. 4196_4205, Jun. 2020.

[10] Y. Tian, Z. Wang, J. Xiong, and J. Ma, ``A blockchain-based secure key management scheme with trustworthiness in DWSNs,'' IEEE Trans. Ind. Informat., vol. 16, no. 9, pp. 6193_6202, Sep. 2020.

[11] H. Tangsen, L. Xiaowu, and C. Qingjiao, ``Research on an evaluation algorithm of sensing node reliability in cognitive networks,'' IEEE Access, vol. 8, pp. 11848_11855, Jan. 2020.

[12] X. Zhou,W. Liang, K. I.-K.Wang, R. Huang, and Q. Jin, ``Academic influence aware and multidimensional network analysis for research collaboration navigation based on scholarly big data,'' IEEE Trans. Emergency. Topics Comput., early access, Jul. 26, 2019, doi: 10.1109/TETC.2018.2860051.

[13] M. Salah, O. A. Omer, and U. S. Mohammed, ``Spectral efficiency enhancement based on sparsely indexed modulation for green radio communication,'' IEEE Access, vol. 7, pp. 31913_31925, Jul. 2019.

[14] T. A. Butt, R. Iqbal, K. Salah, M. Aloqaily, and Y. Jararweh, ``Privacy management in social Internet OS vehicles: Review, challenges and blochchain based solutions,'' IEEE Access, vol. 7, pp. 79694_79713, Jun. 2019.

[15] Z. Cai, X. Zheng, and J. Yu, ``A differential-private framework for urban traffic owes estimation via taxi companies,'' IEEE Trans. Ind. Informat., vol. 15, no. 12, pp. 6492_6499, Dec. 2019.

[16] Z. Cui, F. Xue, S. Zhang, X. Cai, Y. Cao,W. Zhang, and J. Chen, ``A hybid blockchain-based identity authentication scheme for multi-WSN,'' IEEE Trans. Services Comput., vol. 13, no. 2, pp. 241_251, Mar. 2019.

[17] Y. Wang, M. Liu, J. Yang, and G. Gui, ``Data-driven deep learning for automatic modulation recognition in cognitive radios,'' IEEE Trans. Veh. Technol., vol. 68, no. 4, pp. 4074_4077, Apr. 2019.

[18] Y. Xu, Q. Zeng, G. Wang, C. Zhang, J. Ren, and Y. Zhang, ``An efficient privacy-enhanced attribute-based access control mechanism,'' Concurrency Comput. Pract. Exper., vol. 32, no. 5, p. e5556, Mar. 2020, doi:10.1002/cpe.5556.

[19] X. Zhou, W. Liang, K. I.-K. Wang, and S. Shimizu, ``Multi-modality behavioral influence analysis for personalized recommendations in health social media environment,'' IEEE Trans. Comput. Social Syst., vol. 6, no. 5, pp. 888_897, Oct. 2019.

[20] X. Liu, H. Huang, F. Xiao, and Z. Ma, ``A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs,'' IEEE Internet Things J., vol. 7, no. 5, pp. 4101_4112, May 2020.

[21] Y. Lin, Z. Cai, X. Wang, and F. Hao, ``Incentive mechanisms for crowd- blocking rumors in mobile social networks,'' IEEE Trans. Veh. Technol., vol. 68, no. 9, pp. 9220_9232, Sep. 2019.

[22] D. Zheng, C. Jing, R. Guo, S. Gao, and L.Wang, ``A traceable blockchain- based access authentication system with privacy preservation in VANETs,'' IEEE Access, vol. 7, pp. 117716_117726, Sep. 2019.

[23] X. Zhou, Y. Hu,W. Liang, J. Ma, and Q. Jin, ``Variation LSTM enhanced anomaly detection for industrial big data,'' IEEE Trans. Ind. Informat., early access, Sep. 11, 2020, doi: 10.1109/TII.2020.3022432.

[24] C. Xu, K.Wang, P. Li, S. Gou, J. Luo, B.Ye, and M. Guo, ``Making big data open in edges: A resource-efficient block-based approach,'' IEEE Trans. Parallel Distrib. Syst., vol. 30, no. 4, pp. 870_882, Apr. 2019.

[25] T. Shu,W. Liu, T.Wang, Q. Deng, M. Zhao, N. N. Xiong, X. Li, and A. Liu, ``Broadcast based code dissemination scheme for duty cycle based wireless sensor networks,'' IEEE Access, vol. 7, pp. 105258_105286, Jul. 2019.

[26] Z. He, Z. Cai, and X. Wang, ``Modeling propagation dynamics and developing optimized countermeasures for rumor spreading in online social networks,'' in Proc. IEEE 35th Int. Conf. Distrib. Comput. Syst. (ICDCS), Jun. 2015, pp. 205_214.

[27] H. Feng,W.Wang, B. Chen, and X. Zhang, ``Evaluation on frozen shells quality by blockchain based multi-sensors monitoring and SVM algorithm during cold storage,'' IEEE Access, vol. 8, pp. 54361_54370, Mar. 2020.

[28] Z. Liu, D. Wang, J. Wang, X. Wang, and H. Li, ``A blockchain-enabled secure power trading mechanism for smart grid employing wireless networks,'' IEEE Access, vol. 8, pp. 177745_177756, Sep. 2020.

[29] Y. Xu, C. Zhang, Q. Zeng, G. Wang, J. Ren, and Y. Zhang, ``Blockchain- enabled accountability mechanism against information leakage in vertical industry services,'' IEEE Trans. Netw. Sci. Eng., early access, Feb. 27, 2020, doi: 10.1109/TNSE.2020.2976697.

[30] R. T. Yazicigil, T. Haque, P. R. Kinget, and J. Wright, ``Taking compressive sensing to the hardware level: Breaking fundamental radio-frequency hardware performance tradeoffs,'' IEEE Signal Process. Mag., vol. 36, no. 2, pp. 81_100, Mar. 2019.