Indonesian Journal of Computer Science
ISSN 2549-7286 (*online*)
Jln. Khatib Sulaiman Dalam No. 1, Padang, Indonesia
Website: ijcs.stmikindonesia.ac.id | E-mail: ijcs@stmikindonesia.ac.id

A Literature Review on Access Control in Networking Employing Blockchain

Patikiri Arachchige Don Shehan Nilmantha Wijesekara
nilmantha@eie.ruh.ac.lk
Department of Electrical and Information Engineering, Faculty of Engineering, University of Ruhuna, Galle 80000, Sri Lanka

Article Information

Submitted : 12 Feb 2024
Reviewed: 22 Feb 2024
Accepted : 27 Feb 2024

Keywords

access control,
blockchain,
encryption-formed AC,
smart contracts,
AC manager
blockchain-formed AC;
networking,
tokens,
distributed AC,
transactions

Abstract

Access Control (AC) in networking attempts to make sure that only authorized devices perform actions formed upon privileges defined for them with a view to prevent malicious users' entry and interaction in the communication grid. Blockchain solutions contain an arrangement of related blocks that naturally safeguards the trustworthiness, defending the incontestability, defend masked-identity of its transactions/transfers due to scattered consensus strategies and cryptographic solutions. Our survey comprehensively reviews BC-formed AC in broad scope of networking considering AC techniques while breaking down into 4 propositions and assessing them in terms of blockchain roles, AC technique and approach, network elements, and rest. We stockpiled a primary sample of 79 bibliographic references by weeding out them for screening criteria sought from scientific information reservoirs exploiting a qualitative and extensive strategy. Formed upon this survey, in blockchain-formed AC, blockchain can be exploited as an AC manager to administrate network devices and access information, implement automatic AC by means of smart contracts, secure storage of AC related data to reinforce overall AC security, and for safe data exchanging in the operation of AC. Minute assessment highlights that from blockchain-formed AC, 52.5% provide AC using blockchain itself or using smart contracts, 92.5% exploit sequential blockchain, 35% exploit PBFT consensus, provide 100% fine-grained and host-formed AC, 85% decentralized AC, 87.5% have single-factor authentication, 92.5% provide dynamic AC, and 45% have opted for IoT. Finally, we evaluate the chances and difficulties of the principle of blockchain-formed AC and then giving recommended actions to beat them.

A. Introduction

Access control (AC) implements mechanisms and policies to manage and regulate entry, interaction, and privileges of network devices to make sure that only authorized devices perform actions defined by the privileges successfully restricting malicious users' entry and interaction in the network [1]. Within encryption formed AC such as ones harnessed in broadcast encryption, public key infrastructure, attribute-formed encryption, identity-formed encryption, etc., content providers encrypt the content and supply to the network where the clients will authenticate and obtain decryption keys to access the content [2]. On the other hand, in encryption independent AC, access rules are not formed upon encryption, but on others such as a metadata file (manifest), user interests, digital signature, certificates, etc. [3]. Traditional AC authorization models exploited mandatory AC where the centralized administrator that defines parties having accessibility rights and normal users who are unable to modify AC policies [4]. Similarly, discretionary AC is also a centralized AC schema that offers privileges considering user group where users also are able to optionally grant privileges where subjects that can access objects are explicitly defined [5]. However, there are more modern AC authorization models that grants authorization formed upon roles, attributes, capabilities, organization, time, geography, behavior, etc. [6].

Access control techniques among others discretionary AC are static in its approach where AC rights are predefined, in contrast to dynamic AC that considers dynamic parameters among others attributes, time, behavior, etc. which is more adaptive than user centric static AC [7]. Moreover, the approach of AC can be fine-grained where AC for individual hosts is provided for resources just like data flows, in contrast to coarse-grained network level AC for network traffic [8]. The user authentication performed for verifying user identities in the operation of AC can be founded on a single-factor or founded on multiple factors such as password, tokens, biometric factors, to provide strong authentication [9]. Furthermore, in distributed AC, each node is responsible for managing its own policies whereas in conventional centralized AC such as ones typically harnessed in discretionary and mandatory AC, AC policies are managed by a centralized entity [10]. For overcoming drawbacks of both centralized and distributed AC, in hierarchical AC, there exist multiple AC layers with inheritance where lower layers function similar to distributed approach and higher levels are more centralized [11].

A blockchain intrinsically contains of an arrangement of blocks interconnected in a sequential or multi-directional pattern rooted in the structure of the chain of blocks [12]. Concretely, transactions/blocks are joined together with a predetermined block/transaction retaining the hashed representation of several source transactions/blocks setting them unmodifiable [13]. In addition, they implement a common accord system including proof-formed common accord or vote-formed common accord for approving the blocks amid equals earlier a transaction/block is incorporated to the chain of blocks [14]. Additionally, they implement strong hash processes to defend the trustworthiness and virtual signature for defending transaction incontestability [15]. Besides, they may encompass sturdy cryptographic solutions including privacy preserving verification and advanced cryptography for safeguarding versus quantum breaches [16] amplifying the elements of confidentiality guardianship in

blockchain. Still, unique blockchain inherently that avoid cryptographic solutions including unbalanced key encryption for defending the confidentiality guard, is not perfectly confidentiality guarding owing to blockchain transfers/transactions are with masked identity indicating that transfers/transactions are established by a secure tokenized address substituting genuine addresses of participants [17]. Moreover, the measure of confidentiality assurance is flexible corresponding to the chain of blocks category: controlled, cooperative, and uncontrolled. Uncontrolled blockchain is the legacy fully scattered blockchain whereas controlled and cooperative blockchains exhibit a distinct measure of authoritarian rule granting augmented discretion and data authorization management than uncontrolled [18]

Pursuant to our inspection, blockchain formed AC in networking is four folded. First, blockchain has been exploited as a manager to administrate network devices and access information [19], keys related to authentication [20], AC policies [21], etc. Secondly, Smart Contracts (SCs) exploited on blockchain has been extensively put to use for implement automatic AC by verifying access privileges [22], providing authentication [23], generating and revocations of keys [20], auditing [24], etc. In the third category, blockchain is exploited as a secure storage for AC related data such as encrypted content in encryption formed AC [25] or storing tokens, attributes, signatures, certificates, etc. in encryption independent AC [26] to reinforce the security of overall AC process. Finally, blockchain facilitate secure data sharing in the operation of AC by a conventional technique with a view to prevent falsification of data, repudiation, and mutation [27].

Few surveys confront blockchain formed AC specifically in Internet of Things (IoT) and healthcare and do not concentrate on the wide category of networking [28], [29], [30], [31]. None of these 4 surveys stated before concentrate on the wide category of networking and do not present blockchain formed AC frameworks in connection with AC methods and distinctly identify the role of blockchain in each framework. However, there are two survey papers [32] and [33] that are somewhat closer work to ours that review on blockchain formed access AC in networking. Still, paper [33] concentrates on role-formed, discretionary, and attribute formed AC only while paper [32] reviews AC in connection with different network domains rather than AC technique and both of them do not identify and emphasize the blockchain roles and lack a thorough analysis. In contrast to these works, our work on the other hand, reviews blockchain-formed AC solutions in networking comprehensively considering all encryption formed AC methods, encryption independent AC methods, and diverse authorization models in blockchain formed AC and categorize the existing work formed upon the specific blockchain function (role) in each technique. Moreover, we analyze the existing work in terms of blockchain related and AC related parameters to identify disparities and difficulties finally providing recommended actions to overcome them.

Figure 1 highlights the content summary of this literature review.

1.1 Contributions to Contemporary Literature

- We classed and briefly examine a recap of different AC strategies (Section 3).
- Approaches of AC in telecommunication networks are briefly examined (Section 4).

- A recap of blockchain framework is displayed (Section 5).
- Inspect on contemporary blockchain-formed AC frameworks in networking systems (Section 6).
- Assess minutely on the inspected blockchain-formed AC frameworks (Section 7).
- Chances and difficulties of blockchain formed AC is explored (Section 8).
- Recommended actions and prospective directions for exploiting blockchain formed AC is displayed (Section 9).

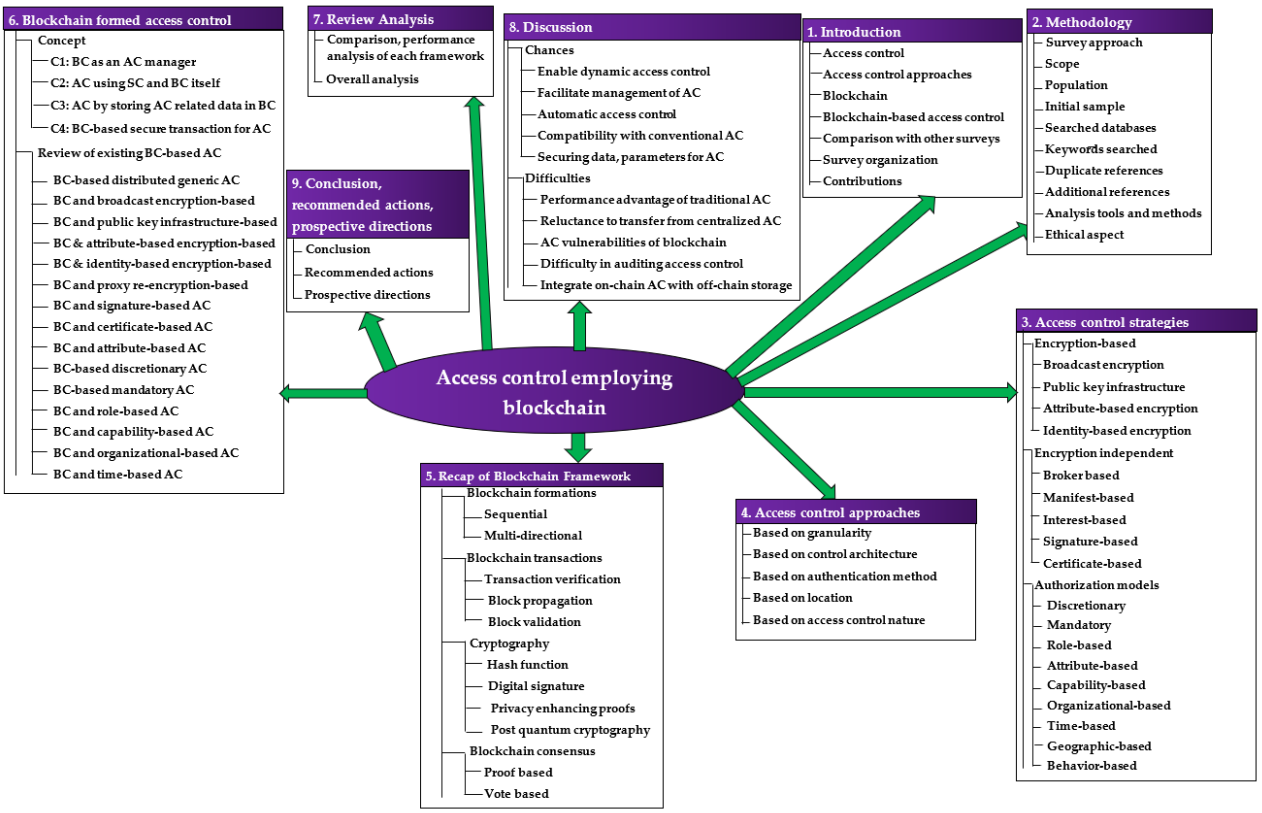


Figure 1. Content summary of this literature review on AC in networking exploiting blockchain.

B. Methodology

This survey inspects the prevalent original research on blockchain-formed AC in networking accessible to readers through past decades exploiting a qualitative and extensive strategy [34]. In addition to that, it looks at a plethora of elements of AC in Networking and blockchain platform. Accordingly, all pioneering scientific publications and online documents appearing in publications on AC in networking, blockchain-formed network AC, and blockchain compose the complete dataset in the scope of this exploration. However, complete dataset references are inscrutable to inspection in this exploration. Accordingly, exploiting relevant search parameters and screening criteria, we brought together 84 references from pioneering scientific publications and online documents.

We sought IEEE Xplore information technology database, ScienceDirect scientific information reservoir, Google Scholar scholarly content locator, ACM

internet-formed library, Wiley internet-formed library, and MDPI resource query system. The search parameters we regularly opted were "Network AC" OR "Blockchain-formed network AC" OR "Blockchain and broadcast encryption formed AC" OR "Blockchain" OR "Blockchain and public key infrastructure formed AC" OR "Blockchain and attribute encryption formed AC" "Blockchain and identity encryption formed AC" OR "blockchain and proxy re-encryption formed AC" OR "blockchain and signature formed AC" OR "Blockchain and certificate formed AC" OR "Blockchain and attribute formed AC" OR "Blockchain-formed discretionary AC" OR "Blockchain-formed mandatory AC" OR "Blockchain and role-formed AC" OR "blockchain and capability formed AC" OR "Blockchain and organizational formed AC" OR "Blockchain and time-formed AC".

Few components for weeding out the articles crafted the screening criteria. First, research paper compels the utilization of English and afterwards, it should be greatly fitting to the search parameter. Thirdly, in an effort to ameliorate the precision of conducted survey, periodical papers were provided preferential treatment compared to symposium proceedings and preliminary writings. Yet, we didn't advocate for scholarly research of an individual article publisher in the screening criteria; as an alternative, we perceived all article publishers in a similar fashion. The last screening criterion announces that an individual research paper ought to be made public in the midst of years of 1970 and 2023.

The primary sample was dropped to 79 bibliographic references thereafter it was coming across that 5 bibliographic references were multiplicate. In addition to that, we referred to expositions and explanations in connection with the assorted topics given in this survey using 15 research papers. To relate this survey with antecedent surveys, we posteriorly integrated 6 increased survey articles to the compilation of research, making the full sum of bibliographic references to 100.

To examine extant blockchain-formed AC in networking in accordance with few components, including blockchain characteristics, AC characteristics, network traits, and execution, we exploited the charted data layout for survey narrative investigation. In addition to that, we formulated data plots exploiting the Microsoft's data analysis software to equitably analyze survey data affiliated with AC-formed and blockchain-formed components [35].

Ethics are inconsequential as a result of this survey associates with telecommunication systems.

C. A Recap of Access Control Strategies

3.1 Encryption formed AC

In encryption-formed AC, the information suppliers encrypt the content and provide them to the network where end users are required to authenticate and get keys for decrypting to access the encrypted content.

3.1.1 Broadcast Encryption (BE)

In BE, a unique group key is put to use for encrypt the content for all viewers where each viewer in the group needs to utilize a user specific sub-key to decrypt the content. Note that these sub-keys are generated formed upon the group key. When users need to be revoked, the group key is changed and dispersed among the

group such that the banned users cannot decrypt the content using the old sub-key. The process of broadcast encryption-formed AC is highlighted in Figure 2.

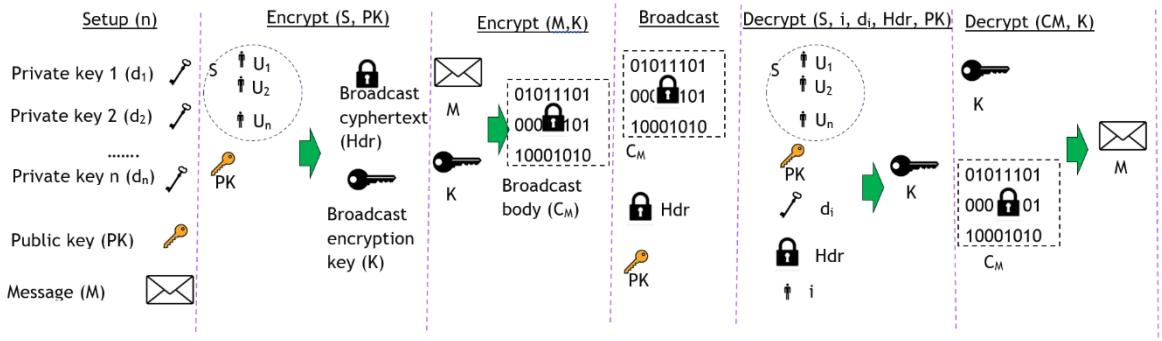


Figure 2. The process in broadcast encryption-formed AC technique.

In [1], a conspiracy proof broadcast encryption technique using cyphertext and secret keys of constant size for a given set of receivers having a linear public key system has been studied. A broadcast encryption scheme for a mobile adhoc network (MANET) has been designed with an efficient approach for key distribution by using a single bilinear pairing computation for the group members to obtain a session key without exchanging information messages to obtain a group key and has been resistive against cyphertext attacks [2].

3.1.2 Public Key Infrastructure

Public key infrastructure also known as non-symmetric key cryptography use a pair of public key and private key for encryption and decryption respectively.

Session formed - In session-formed AC, a secure session is established among the client and provider after client authentication and authorization at the beginning of the session. The end user requests for information from the supplier by supplying the end user's non-secret key where the provider will supply the content by encrypting with the end user's non-secret key for the end user to decrypt it using its secret key. A session formed AC technique in Information Centric Networking (ICN) having a key distribution protocol to secure the confidentiality of content during information delivery and a dynamic naming system to enhance user privacy has shown provided high communication security and privacy for the session [36].

Proxy re-encryption - In proxy re-encryption, an intermediate proxy such as a router is accountable for re-encrypting the content which has been encrypted using one public key to be encrypted using another public key without revealing the content to the proxy (third party) such that the proprietor of the new non-secret key is able to access the content. A cyphertext attack and collusion resistive proxy re-encryption formed AC scheme for ICN has been exploited for data sharing among subscriber and cooperators with a lower communication overhead [37].

Probabilistic model - In probabilistic AC, bloom filters are put to use for store the public keys of the authorized clients using a probabilistic model. In this approach, the content can be delivered using symmetric key encryption and symmetric key can be sent from the provider to the client by encrypting with the client's public key. In [38], for Named Data Networking (NDN), public key cryptography alongside symmetric key cryptography is exploited for AC while a

probability formed data structure using a bloom filter is to screen consumer requests not having required credentials.

3.1.3 Attribute formed Encryption

In AC formed on attribute formed encryption, each client and data are associated with attributes. There are 2 main types of encryption techniques as key-policy and cyphertext-policy.

key-policy attribute-formed encryption -In this approach, access policies are embedded in the encryption key derived from the content attributes. Data is encrypted using this policy specific encryption key and end-users can unencrypt it only if their features match the protocol specified in the encryption key. Key-policy attribute-formed cryptography has been exploited to offer fine-grained AC in virtualized network environments by providing searchable encryption to create trapdoors to support gates such as AND, OR, etc. by encrypting keywords to match AC policy [39].

Cyphertext-policy attribute-formed encryption - In this scheme, the ciphertext contains the AC policy with client attributes. The end-users can unencrypt the data if their features adhere to the protocol associated with the encrypted data. The encryption key is derived from client attributes in this scenario. A cyphertext policy attribute-formed encryption technique using elliptic curve cryptography without bilinear pairing function having a feature for attribute revocation has resulted in a low computational overhead for wireless body-area networks [40].

3.1.4 Identity formed Encryption

In identity-formed encryption, the identifying information of the client including email address or username is harnessed in public and private key generation. Specifically, private keys for each client are generated formed upon their identity using a secret key producer (a centralized authority) while the non-secret key is generated by considering user identity and private key generator's master public key. A function formed fine-grained AC technique for IoT networks uses identity-formed encryption for preventing applications from performing unauthorized functions has resulted a constant operation cost and prevented over-privileged access [41]. An identity-formed encryption that is leakage robust to catch leakage from secret key owner and encrypting agent by defining a post obstacle input scheme having a leakage function family defined before proving non-secret key and post-obstacle query to provide leakage has been effective in providing AC for sensor networks [42].

3.2 Encryption Independent AC

In encryption independent AC methods, access policies are resolute independent from the technique of encryption.

3.2.1 Broker-formed

Broker-formed AC exploits an external entity known as broker to manage AC decisions among users. The broker is responsible for determining user permissions and privileges, evaluating the access requests, and enforcing AC policies [43]. However, this approach has weakness of fundamental weak spot and the system's trust is dependable on the trustworthiness of the broker. A broker formed AC by acquiring and processing knowledge to mediate AC between user, devices, and network resources while maintaining user credentials and negotiate

among brokers to realize credibility among trustees has been posited for distributed AC [44].

3.2.2 Manifest-formed

Manifest formed AC utilizes a metadata file known as manifest associated with each resource to define AC policies such as the list of authorized users, the operations that each user can perform, and the constraints under which the control policies are enforced, etc. This technique attempts to minimize communication overhead associated with AC by using manifests. In [45], content object manifests have been put to use for detach encrypted objects from the AC policy in content centric networking and has attempted to maximize in-network caches utilization.

3.2.3 Interest-formed

Interest-formed AC is utilized usually in content-centric networking that grants access to resources formed on user interests rather than permissions. This is a user-centric approach that can adapt to dynamic user interests and varying content availability. It enables providing AC even for the cached content. In an interest-formed AC scheme in NDN, content producers authorize users sign interest packets where by signature checking unsubscribed users can be forbidden by discarding interest packets [46].

3.2.4 Signature-formed

In signature formed AC, digital signatures are put to use for implement AC policies formed upon the authenticity of the digital signature where each user has their own digital signature. This technique allows strong authentication and authorization compared to other non-encryption formed techniques. In a secure edge-formed AC scheme for ICN, network edge performs anonymous authentication by using group signatures while using hash chain to minimize communication overhead where content providers can retrieve feedback using the signatures [47].

3.2.6 Certificate-formed

Certificate-formed AC exploits certificates issued by trusted certificate authority containing user identity, roles, and access rights to verify the identity and permissions of users for authentication and AC. Even though this can provide high level of AC, the security can be compromised when the certificate authority is attacked or behave maliciously. A secure certificate-formed AC scheme has been exploited in an IoT network to mitigate security attacks such as replay, impersonation, etc. preserving anonymity [3].

3.3 Authorization models

3.3.1 Discretionary AC

Discretionary AC is a centralized AC technique that offers legitimate end-users the entry to objects using formed on the user group. In DAC, users can also grant privileges to other users while object owners specify the subjects which can access objects using AC policies. The AC depends on the subject's access rights. DAC involves in AC lists and matrices containing access rights that have been assigned to each object for the subjects to perform action. In [48], a series of steps to prevent information leakage in discretionary AC is presented including encoding security rules as mandatory AC policies, prioritizing user files, examining abnormal recipients, etc.

3.3.2 Mandatory AC

Mandatory AC is another centralized AC model where AC is relying on the centralized administration that defines parties who have accessibility rights and normal users who cannot modify AC rules. This model creates security labels that controls access to the objects where there are different sensitivity levels for the data. In [4], mandatory AC is implemented in a distributed system considering the user hierarchy using preliminary key distribution.

3.3.3 Role-formed AC

In role-formed AC, permissions are assigned to the roles. A role is a responsibility or task assigned to a group of users. End-users are allotted to roles, formed on their capabilities [49]. Users being members of the roles are inherited with role's permissions, thus, users of a role can execute actions or access objects if the role has required permissions. Role-formed AC can implement hierarchical authorization by implementing hierarchical roles. The metamodel of role-formed AC is visually highlighted in Figure 3.

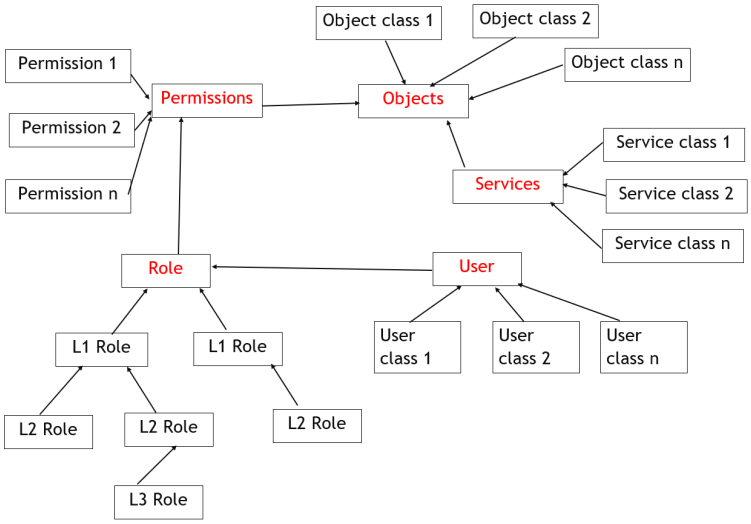


Figure 3. The metamodel of role-formed AC.

Role-formed AC has been exploited in a vehicular adhoc network to provide a solution for the problems of poor AC and sensitive data isolation by using a hierarchy of roles and objects to protect data sensitivities and provide strong AC [50].

3.3.4 Attribute-formed AC

Attribute formed AC grants admission to resources considering the features of objects and subjects. In contrast to role formed AC, permissions in attributed-formed AC are associated with attributes related to subject or object (Ex: subject_username="Nilmantha", object_type="private"). These permissions are specified as an attribute-formed policy. Actions such as read, write, execute can be granted to subjects to undertake the actions on the objects if attribute-formed policy is satisfied. A dynamic attribute-formed AC scheme for the Software-Defined Networking (SDN) control plane uses exponential smoothing to threshold of flow entry insertion and access time upper limit and using single and multi-case filters for fine grained permission management [51].

3.3.5 Capability formed AC

Capability formed AC has tokens/tickets/keys that grants rights or permissions (capability) for the entity holding those token access an object. A federated capability formed AC scheme has been exploited in an IoT network where there is a federated capability delegation technique using a propagation tree to represent access permission propagation and revocation where the access authorization is processed locally [52].

3.3.6 Organizational-formed AC

Organizational formed AC has been posited to overcome the drawbacks of role-formed AC by providing the notion of organization to the concepts of user, object, action, and roles in the role-formed AC. In this model, the user can declare data as temporal, historic, and spatial and allows inter-organizational AC. An organizational formed AC in Wi-Fi networks is presented in [53], where space and time constraint provide AC formed on requestor's role in the organization limiting possible attacks due to having only privileges to undertake actions inside the organization.

3.3.7 Time-formed AC

In time-formed AC, access rights to users are enforced formed on specific time intervals. This further allows users to put time-formed restrictions on their own resources. For providing time-formed AC to multi-characteristic information in IoT networks, single-direction hash chain scheme by encrypting using a sub-key and partitioning data into a two-dimensional subspace representing generation time and attribute has been exploited [54].

3.3.8 Geographic-formed AC

In geographic-formed AC, the admission to resources can be restricted considering geographical location of the users. Similar to time-formed AC, users can put geographic-formed restrictions for their own resources [55]. An improved camera-formed geo-fencing system to localize users accurately and estimate proximity to objects with a view to provide geographical location formed AC in wireless local area networks has been effective compared to a conventional geographical location formed AC [56].

3.3.9 Behavior-formed AC

In behavior-formed AC, users' behaviors are evaluated and granted access for entities formed on the output of the behavior analysis. This model typically behaves in a non-centralized mode. BEAM is a behavior formed AC scheme in SDN that analyzes the network behavior to dynamically grant permissions that can be upgraded or downgraded which can be further verified and build trust [6].

Table 1 highlights a recap of contemporary literature on different AC strategies.

Table 1. A recap of contemporary literature on different AC strategies.

AC strategy	Contemporary literature	Methods	Performance
Broadcast encryption	Collusion-resistant AC [1]	Broadcast encryption with a linear public key system	Collusion resistant AC
	Non-interactive BE [2]	Key distribution by using a single bilinear pairing computation	Resistive against cyphertext attacks
Public key	Session-formed	Key distribution protocol,	High communication security

infrastructure	AC [36]	dynamic naming system	and secrecy of session
	Proxy re-encryption [37]	Proxy re-encryption formed AC	Cyphertext attack and collusion resistive, low overhead
	Probability-formed AC [38]	Probabilistic DS bloom filter + cryptography	Low system, performance overhead
Attribute-formed encryption	Key-policy attribute [39]	Key-policy attribute-formed cryptography to encrypt keywords	In real-world applications, secure and feasible
	Ciphertext policy attribute [40]	Ciphertext policy attribute formed encryption-elliptic curve	Low computational overhead
Identity-formed encryption	IoT-FBAC [41]	An unauthorized action preventing function for IBE	Constant operation cost, prevented over-privileged access
	Post challenge [42]	Post challenge input model with a leakage function family	Leakage resilient AC
Broker-formed	ADAM [44]	Maintaining user credentials and negotiate among brokers	Adheres to AC policies and principles
Manifest-formed	Manifest-formed AC [45]	Manifest to decouple encrypted content from AC policy	Maximize in-network caches utilization
Interest-formed	Interest-formed AC [46]	Interest packets that authorize users by signature checking	Reduce in-network traffic, low complexity key management
Signature-formed	Secure AC [47]	Anonymous authentication by using group signatures	Slight delay to retrieve user content, low overhead
Certificate-formed	Anonymous AC [3]	Anonymity preserving security-formed AC	Better trade-off of security vs. communication, computation costs
Discretionary AC	Data leakage mitigation [48]	Encoding security rules, prioritizing user files, etc.	Mitigate data leakage in AC
Mandatory AC	Mandatory AC [4]	Consider user hierarchy using preliminary key distribution	No performance evaluation presented
Role-formed AC	RBAC-vehicular [50]	Hierarchy of roles, objects to protect data sensitivities	Ensure AC and improve data confidentiality
Attribute-formed AC	DACAS [51]	Exponential smoothing, single & multi-case filters	2ms runtime overhead, high flexibility with context attributes
Capacity-formed AC	Federated AC [52]	Federated capability delegation using a propagation tree	Offer scalable, light weight, and fine-grained AC
Organizational-formed AC	Spatial-temporal AC [53]	Requestor's role in organization with space, time constraints	Limits possible attacks
Time-formed AC	Time-formed AC [54]	One-way hash chain to partition into two dimensions	Efficiently exploitable in resource limited networks
Geographic-formed AC	Geo-fencing [56]	Geo-fencing system to localize users for AC	Low power consumption and time to obtain content
Behavior-formed AC	BEAM [6]	Analyzes network behavior to dynamically grant permissions	No performance analysis presented

D. A Recap of Access Control Approaches

4.1 Formed upon Granularity

4.1.1 Fine grained

Fine-grained AC deals with defining more precise and detailed AC permissions for users or entities. Fine grained AC provides more security than coarse grained AC despite its higher complexity. As a case in point, in [57], a fine-grained AC technique for NDN providing confidentiality and mobility and support potential receivers.

4.1.2 Coarse grained

Coarse grained AC involves defining broader AC permissions that are applicable to groups of users or roles rather than individual users. This approach is simple and easy to manage and effective when high-level AC is sufficient. Driven by simplicity in implementation, a coarse-grained AC scheme exploiting broadcast encryption and multi-user searchable encryption to provide security under conditions when untrusted server colludes with adversaries has been exploited in a hybrid cloud [58].

4.2 Formed upon Control Architecture

4.2.1 Distributed

In distributed AC, AC decision making power is shifted to nodes within a network where each node is responsible for managing its own access policies and permissions. This technique is scalable, however, complex to implement and audit. As a case in point, in [10], a fine-grained distributed AC using attribute-formed encryption is exploited in a wireless sensor network to provide AC for sensor data and has been effective versus user collusion and sensor compromisation.

4.2.2 Hierarchical

In hierarchical AC, there exist multiple AC layers where lower-level AC is more distributed and fine-grained while higher levels are more coarse-grained and centralized. In this approach, lower layers can inherit high level AC policies from the upper layers. DKMS is a dispersed key administration scheme for hierarchical AC for team communications in a multimedia network where each service group keeps a server that manages key tree and supply session keys for the users in the group [11].

4.2.3 Centralized

Conventional AC methods among others discretionary AC, mandatory AC, role-formed AC, etc. are centralized meaning that AC rights are managed by an AC server. This centralized authority defines, enforce, and monitor AC policies [59]. This approach is simple and auditable, however, suffers from fundamental weak spot and have poor scalability. As a case in point, a centralized AC framework for a millimeter wave broadband system that also manages device-to-device communication minimizes delay and maximizes system throughput consisting of a data flow coordination approach and a time planning algorithm to achieve centralized AC [60].

4.3 Formed upon Authentication method

Authentication is put to use for verify the identity of end-users with a view to offer them appropriate access levels to resources. There are two approaches to authentication as single factor and multi-factor.

4.3.1 Single factor

In single factor authentication, a single factor such as a password or a personal identification number is put to use for verify the users. Even though this technique is simple, its security is poor as revealing of the single factor can result in unauthorized access. Recently single factor authentication using fingerprint biometric data and validated data is encrypted and accessed using attribute structure and upon verification of cipher text using elliptic curve cryptography, it is shared among owner and user to improve authentication in the cloud [61].

4.3.2 Multi-factor

In multi-factor authentication, multiple factors such as something that user know (password, PIN), smart cards, tokens, biometric factors of the user, etc. are harnessed in combination to grant access. In [9], multi-factor authentication using all "something you have", "something you know", and "something you are" have been demonstrated for a wireless network by using one time password token, password, and user photo, respectively.

4.4 Formed upon Location

4.4.1 Host-formed

In host-formed AC, AC is provided to resources such as files, directories, etc. or services at individual hosts rather than network [62]. This is a high granular AC technique. A fine-grained host-formed AC for data flows in SDN has been posited by transferring agent functionality from network to host level where high-level AC policies that can discriminate using users and program info associated with network flows [63].

4.4.2 Network-formed

Network formed AC operates at the network level and is coarse grained while AC policies defined which network traffic is allowed or denied. These systems aid network firewalls and intrusion detection and prevention systems for AC. In [64], tickets are put to use for offer network admission for well-mannered nodes in a MANET where a ticket certification is implemented using multiple node consensus and preventing single node monopoly by multiple nodes monitoring a given node to certify or revoke its ticket.

4.5 Formed on Access control nature

4.5.1 Static

Static AC refers to an approach which the AC rights are predefined and assigned to assets formed on the discretions of the asset proprietor. Typical example is a static discretionary AC scheme where the access proprietor defines the access permissions and remain constant until the owner changes them. In [7], AC contracts are put to use for implement static access rights validation alongside other contracts to track misbehavior of users.

4.5.2 Dynamic

In dynamic AC, dynamic parameters among others user attributes, resource attributes, real-time conditions, etc. for determining access to resources. This approach is adaptive and resource driven unlike static approach which is owner-centric [65]. As a case in point, a dynamic AC scheme formed on zero trust security paradigm where user trusts and portraits created dynamically according to real-time user behavior has been feasible in [66] to accomplish high resolution and dynamic AC.

Table 2 highlights a brief of contemporary literature on different AC approaches.

Table 2. A brief of contemporary literature on different AC approaches.

AC approach	**Contemporary literature**	**Methods**	**Performance**
Fine-grained	FGAC-NDN [57]	Fine-grained AC supporting mobility	Provable security with DBDH assumption
Coarse-grained	CGAC-HC [58]	Broadcast encryption and multiple end-user searchable encryption	Secure scheme for unauthorized and internal adversaries
Distributed	FDAC [10]	Attribute-formed encryption	Effective against user collusion and sensor compromisation
Hierarchical	DKMS [11]	Distributed key management--server managing key tree	Low storage and communication overhead
Centralized	Centralized-D2D [60]	Data flow management and a scheduling algorithm	Minimize delay and maximize throughput
Single-factor	SSS-EC [61]	Encrypted fingerprint biometric data using ECC	Improved authentication for AC
Multi-factor	User authentication [9]	multi-factor authentication using "have, no, are"	No performance analysis presented
Host-formed	Flow-formed AC [63]	High level AC policies related with network flows	Each host capable of creating more than 25 new flows/second
Network-formed	URSA [64]	Tickets put to use for offer network admission for well-mannered nodes	Effectively implements AC
Static	Smart contracts [7]	AC contracts implement static access rights	Low execution time, cost, overhead
Dynamic	DAC-ZT [66]	Formed upon behavior, user trusts, portraits created dynamically	No performance analysis presented

E. A Recap of Blockchain Framework

An arrangement of inter-connected blocks or transfers/transactions entails the ledger recognized as blockchain.

5.1 Formation

Each separate block inherent to a sequential blockchain, which entails a header piece and data piece is associated to its antecedent block (apart from the starting block) exploiting the antecedent block's hashed representation, and the transfers/transactions inherent to a data piece are systematized into a Merkle tree form [13].

Multi-directional blockchain entails an arrangement of inter-connected transfers/transactions where one transfer/transaction possibly ratify various further transfers/transactions that generated beforehand. These transfers/transactions have missing header pieces and data pieces, accordingly Merkle trees are unavailable [14].

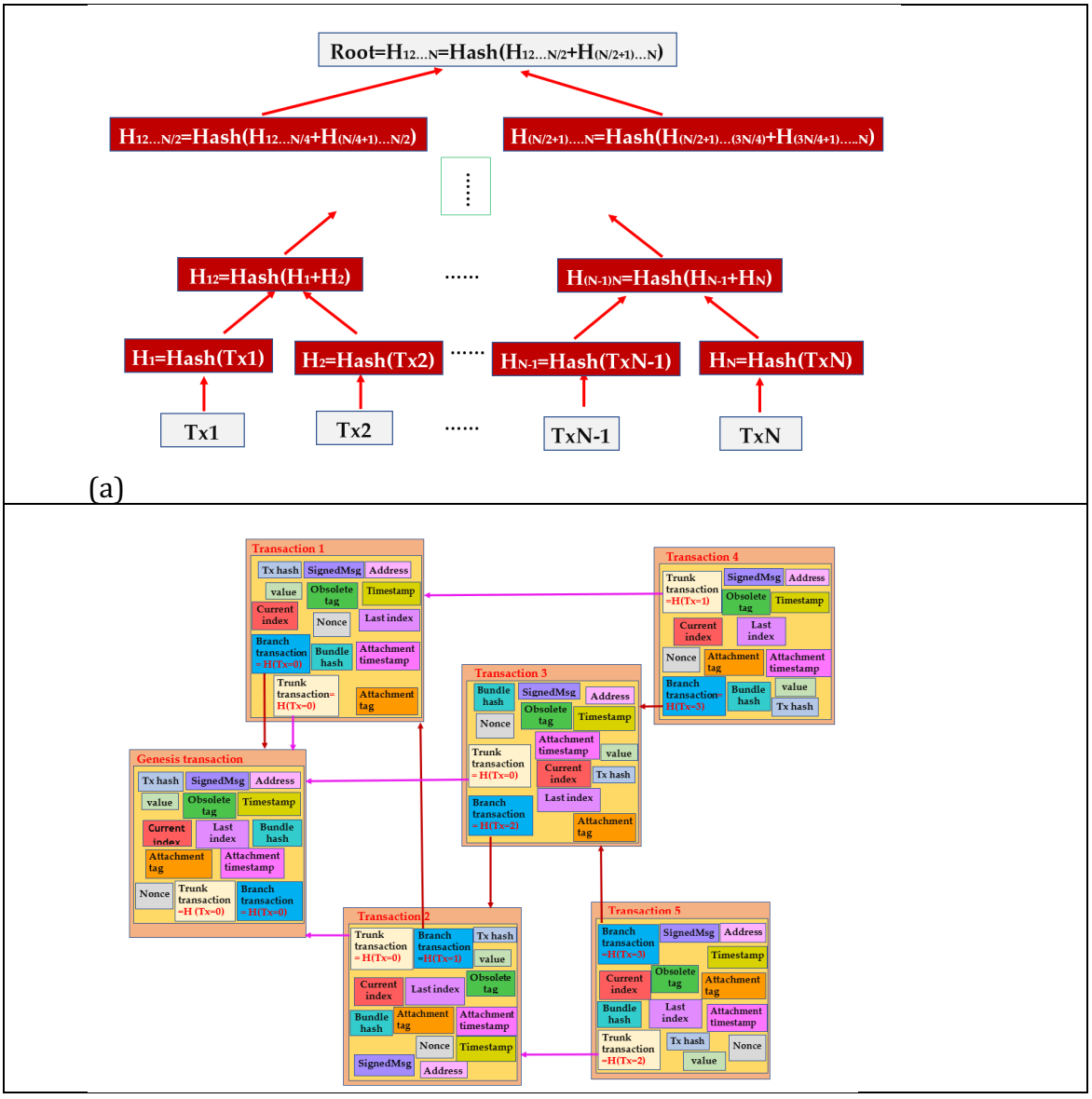
Merkle tree structure of a sequential blockchain and architecture of multi-directional blockchain are graphically highlighted in Figure 4.

5.2 Transactions

A client can set in motion a blockchain transaction/transfer, which is thereafter transferred to all equals lying the network and hidden exploiting the sender's cryptographic secret. A consensus method will set in motion once each client exploits the open key to approve the transaction/transfer [67]. Block contributors continuously engage in consensus/common accord by incorporating the transaction/transfer encased by a block, which is thereafter transferred around the blockchain network and collaborated by each client in the chain of blocks network succeeding block approval.

5.3 Cryptography

To defend the trustworthiness of transfers/transactions in blockchain, a hash process is exploited to issue consistent magnitude hashed representations with limited conflations [15].



(b)

Figure 4. Merkle tree and architecture of multi-directional blockchain. (a) Merkle tree. (b) Multi-directional blockchain (IOTA).

Exploiting a virtual signature, unbalanced key encryption maintaining secret and open keys is exploited to approve transfers/transactions. With the intention of amplify the seclusion of transactions, it's also conceivable be exploited to obfuscate blockchain transfers/transactions [68].

Verifications preserving privacy are exploited to approve transfers'/transactions' accuracy keeping secret the personally identifiable information of transfers/transactions, amplifying seclusion and halting the transferring of secret knowledge [69].

Advanced cryptography exploits potent cryptographic mechanisms that are safeguard from breaches from quantum information systems, including enhanced Ed448, Kyber, etc. [16].

5.4 Consensus/Common accord

Blockchain consensus exploits widespread common accord to contribute and approve recently created blocks, defending the trustworthiness of the ledger.

Involved in vote-formed common accord, details are relayed and gained amidst the equals as they combine efforts to approve blocks. The top choice vote-formed common accord mechanism exploits byzantine fault-resilience common accord, amidst which a manager incorporates transfers/transactions encased by a block, transfers it, and clients retransfer it to approve the block gained with the help of the parent is matching [17]. Once each client got matching replicates of a recently created block with the help of surpassing the double third threshold of the network's clients, the block can be incorporated to the chain of blocks.

Proof-formed common accord requires clients to issue compelling corroboration in light of why they can be appreciated for incorporating a recently created block to the chain of blocks. The most preferred proof-formed common accord mechanism is identified as proof-of-work obliging a client to expend energy by settling a formidable conundrum with the intention of defends its trustworthiness [67]. Alternatively, there exist efficient consensus approaches among others proof-of-stake that considers nodes stake instead of computations.

F. Blockchain-formed AC in Networking

6.1 Proposition

Founded on this scholarly exploration, blockchain formed AC proposition is realized using one of the four methods given in sequence.

- C1 -- Blockchain as an AC manager - In these schemes blockchain is exploited as an AC manager that administrates devices, access information, data, authentication keys, AC policies, authentication, and authorization.
- C2 -- AC using SCs or blockchain itself - Smart contracts/blockchain itself are put to use for verify access privileges, auditing, authentication, generation and revocation of keys, automatic AC, etc.
- C3 -- AC with the aid of securely stored tokens, encrypted data, etc. (AC related data) in blockchain - In this approach, blockchain is exploited in both encryption-formed AC for securely storing encrypted content or in

encryption-independent schemes to securely store tokens, attributes, digital signatures, certificates, etc. to aid in the operation of AC.

- C4 -- Blockchain-formed transactions (data sharing) while AC is realized using a conventional technique - Blockchain has been exploited to perform transactions securely (securely store data) preventing repudiation, falsification, and mutation in the operation of AC by another approach (using a conventional AC technique) which aids in improving the general security aspect of the AC.

The proposition of AC in networking exploiting blockchain is graphically highlighted in Figure 5.

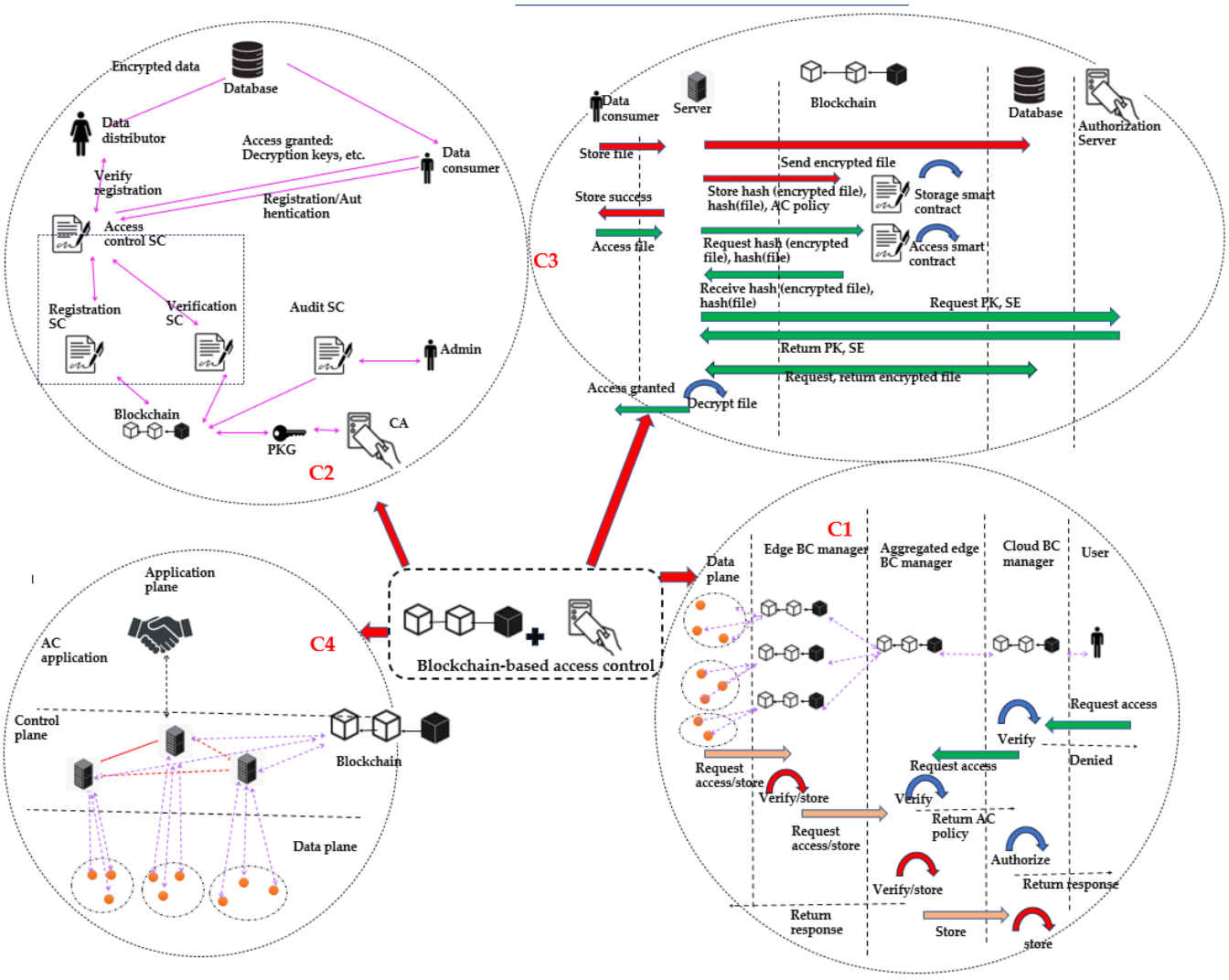


Figure 5. Proposition of blockchain-formed AC.

6.2 Review regarding Blockchain-formed AC in Networking

6.2.1 Blockchain formed Distributed Generic AC

BaCs is a Ethereum private blockchain-formed distributed AC scheme designed for IoT networks that uses the address of account of the nodes to gain admission to management server having processes for authorization and its

revocation, AC and auditing alongside a symmetric key encryption to ensure privacy [70]. Another work implements a blockchain AC manager that implements authentication, authorization, and privacy for sensitive-medical with a view to provide access to stakeholders in an automatic and decentralized manner [19]. Alternatively, a clustering architecture of blockchain managers at edge, aggregated edge, and consortium levels contains a hierarchy of blockchains to provide authentication and authorization for the end-users to gain admission and utilization of resources at different levels in a scalable manner using SCs in IoT networks [23]. Smart contracts exploited on blockchain have been utilized for providing AC, authentication, authorization while registering users and to track subject/object negligence in an IoT network which has resulted in a low-cost utilization [71]. AuthPrivacyChain is a privacy protecting blockchain in a cloud environment having a customized blockchain-formed AC mechanism where authorization related transactions provided by the user are ciphered and reserved in the blockchain which uses the address of the blockchain node as the identity [72]. In mobile communication networks, a decentralized AC scheme exploiting blockchain and SCs stores subscription data securely (using threshold secret sharing) in the blockchain while automatically verifying access privileges using SCs having an authentication scheme that uses tokens for authentication [22]. BACC is a novel approach to secure cloud storage servers using blockchain and SCs to implement AC where 4 SCs: AC policy, auditing, lookup contract, and contract look up carry out automatic AC where the cloud servers only reserve the ciphered data while split deciphering key is reserved in the master node of the blockchain network [24].

6.2.2 Blockchain and Broadcast Encryption formed

A generic system for AC using Ethereum blockchain, SCs for automatic AC, and special secret key-driven broadcast encryption in which ciphered authentication information for accessing data conditionally present within the blockchain while the conditional access to encrypted data is available in an off-chain approach has been effective in an Internet of Things (IoT) network [25]. Using cloud computing and blockchain technology, a secure medical information service framework ensures confidentiality by leveraging an identity-driven hierarchical broadcast encryption-formed AC where encrypted data are reserved in the blockchain with an incentive mechanism to maintain the system [73]. In a clinical blockchain-formed broadcast encrypted data sharing network, a dynamic and expandable AC framework which leverages broadcast encryption where keys utilized for encrypting low sensitivity medical data can be deduced from those put to use for encrypt high sensitivity data different from the conventional approach of updating permission lists [74].

6.2.3 Blockchain and Public Key Infrastructure formed

BBACS is a blockchain-formed AC scheme in medical networks that can bypass gateway for authorization exploiting public key infrastructure for encryption and authorization cutting down network cost with a view to store electronic medical records where the blockchain itself implements AC [75]. By using specification languages to state service requirements and using public key infrastructure to develop trust using AC with the aid of certificates, a generic trusted framework for IoT networks using blockchain has been posited in [76]. For

preserving data integrity, authenticity, and AC in an IoT network, a blockchain formed public key management scheme making utilization of the non-centralized and non-modifiable blockchain features that leverages SCs generating, distribution, and revocation of public keys preventing sole point of collapse in conventional public key infrastructure has been posited in [20]. DBACP-IoTSG is a blockchain-formed framework designed for smart grids where there is a leader selection process for achieving consensus using Practical Byzantine Fault Tolerance (PBFT) for entering transactions to the blockchain where transactions are encrypted using elliptic curve cryptography by one service provider to be decrypted by another for achieving authentication while having a key establishment process for newly added nodes [77].

6.2.4 Blockchain and Attribute formed Encryption formed

VO-PH-MAABE is a framework designed for internet of medical things that uses blockchain to store validation parameters that are put to use for verify outsourced decryption results and to develop trust between multiple authorities and use SCs to calculate keys for attributes in attribute-formed encryption for electronic health record AC [78]. Attribute formed encryption and single-key cryptography are jointly exploited to provide high resolution AC IoT data with the aid of SCs in which blockchain is put to use for support distributed storage for data hash values, AC policies, etc. [79]. Similarly, a ciphertext policy attribute-formed encryption encrypts a token containing access permissions to resources and uploaded to a multi-directional IOTA tangle to be decrypted by authorized users effectively implementing high-resolution and scalable AC [80]. BACC-SDN is a scheme that has been posited to secure the SDN paradigm where AC between the controllers and applications are realized using attribute-formed encryption while that between controllers and switches are implemented using a custom AC mechanism while all the transactions amidst the controllers, network apps, and forwarding devices are entered and maintained securely in the blockchain using PBFT consensus mechanism [81].

6.2.5 Blockchain and Identity formed Encryption formed

BIDAC is a framework that has been posited for AC in IoT networks that uses identity-formed encryption algorithm and blockchain for authorization and data sharing, respectively where SCs are put to use to automatically provide identity-formed AC by taking private keys [82]. Similarly, identity-formed encryption has been exploited in a blockchain-formed framework designed to store sensitive medical data where SCs implement the AC formed upon identity [83]. A consortium blockchain-formed decentralized AC scheme for the smart grid using identity-formed fused encryption and signcryption alongside a customized consensus approach for selecting a private key generator of the power system as a solution to problem of key escrow of unfaithful parties [84].

6.2.6 Blockchain and Proxy re-encryption-formed AC

In healthcare networks, a blockchain framework has been exploited to store electronic health data of patients that uses a smart card approach for authentication exploiting privacy-preserving proofs and provide admission to service offerors using proxy re-encryption [27]. Blockchain is exploited for non-centralized data exchanging and acting as a trusted authority for AC in cloud ecosystems where IoT data proprietors externalize information to cloud exploiting

identity-formed encryption where proxy re-encryption provides AC and an edge unit will act as a proxy server catering to computationally intense tasks [85]. In SDN, blockchain and proxy re-encryption have been utilized to solve fundamental weak spot in SDN and to provide authorization for the devices to engage in secure communication where SCs are leveraged to efficiently search and update blockchain records with AC related information such as re-encryption keys [86].

6.2.7 Blockchain and Signature-formed AC

In vehicle-to-vehicle networks, a framework for management and decentralized sharing of vehicles' dashcam videos has been posited by exploiting blockchain to prevent falsification and by exploiting multiple-signature formed AC achieved using segmentation and reserving video data stemming from GPS [87]. For IoT-formed healthcare applications to access sensitive medical data, a private blockchain is utilized for sharing private hospital data where an elliptic curve cryptographic signature-formed novel AC mechanism which attempts to solve an elliptic curve discrete logarithmic problem and hash function is utilized that has been proven to be resistant to security attacks preserving anonymity and untraceability [88].

6.2.8 Blockchain and Certificate-formed AC

BACS-IoD is a blockchain-formed AC scheme for internet of drones networks among flying drones and between drones and a ground server station where data gathered by server stations are reserved to the blockchain exploiting ripple protocol common accord algorithm in which AC is formed on certificates provided by control room with a view to achieve authentication [89].

6.2.9 Blockchain and Attribute formed AC

A blockchain-formed and attribute formed AC system for IoT networks has been posited to prevent from convoluted admission coordination and deficiency of reliability, by using blockchain to store attribute distribution preventing data tampering [90]. Similarly, another framework known as ZAIB exploits blockchain for anonymous registration and store activity logs in an immutable manner, uses zero trust architecture and attribute-formed AC to provide AC for communication considering behavior of devices and environmental parameters in IoT with the aid of SCs [91]. In a Hyperledger fabric blockchain, sensitive medical data is stored securely and in a privacy reserving mode in blockchain by exploiting searchable cryptography and k-anonymity where the attribute formed AC is implemented by exploiting SCs to offer access to users with proper attributes [92].

6.2.10 Blockchain-formed Discretionary AC

For healthcare networks, Bell–LaPadula model is utilized to implement by using SCs for discretionary AC with a view to manage existing mandatory AC permissions allocated to different roles where Hyperledger fabric blockchain transactions and peers are categorized into different security and clearance levels to improve the scalability [93].

6.2.11 Blockchain-formed Mandatory AC

A private hierarchical blockchain is exploited to protect each tier of the IoT network having a lightweight consensus approach reducing traffic overhead exploits mandatory AC where only blockchain managers are able to mutate the AC policy with a view to supply a hierarchical security for the IoT network [21].

6.2.12 Blockchain and Role-formed AC

In a federated data sharing system, multidimensional authorization of users using colored coins and role-formed AC exploited using self-executing SCs in Hyperledger fabric blockchain [94]. A non-centralized high-resolution role-formed AC is implemented in an IoT network by grouping user devices formed on the gateway exploiting SCs for each gateway triggered by blockchain transactions where access rights are stored in a key-value database [95].

6.2.13 Blockchain and Capability formed

IoT-CCAC is a capability-formed AC scheme for consortium IoT networks in which blockchain is exploited as a secure decentralized database with a view to get rid of shortcomings of traditional centralized AC and having a high scalability [96]. Moreover, DCACI is another decentralized capability-formed AC scheme built using multi-directional IOTA tangle using its masked authentication messaging system for ensuring the integrity of capability tokens for granting, updating, delegating, and revoking AC [26]. Furthermore, recently SCs on Ethereum blockchain have been utilized for managing capability tokens allocated to subjects and processed one token per action allowing fine-grained capability delegation having consistency among delegated information in IoT networks [97].

6.2.14 Blockchain and Organizational-formed

FairAccess is an organizational-formed AC scheme formed on blockchain that defines AC regulations contained within blockchain transactions for pseudonymous and privacy protecting authorization management where the blockchain acts as an AC manager [98].

6.2.15 Blockchain and Time-formed

Blockchain has been exploited to store educational assets in an immutable manner of the metaverse as a management framework and for AC where asset owners can control the duration of the access using time-formed AC [99]. A security scheme for IoT formed upon blockchain exploits AC where users have to pay a fee to owners of devices to get access for device storage for a specific time in which access is denied when the time expires where blockchain serves as a manager managing devices, access information, and data [100].

G. Review Assessment

7.1 Assessment of solo proposals

Table 3 highlights the assessment of solo blockchain-formed AC frameworks in minute detail in connection with AC technique, BC related parameters, AC approach, network parameters, and year of proposal.

Table 3. Assessment of Blockchain-formed AC frameworks.

AC technique	Methodology	BC proposition	Blockchain formation	Blockchain consensus	Blockchain classification	AC approach	Network formation	Network classification	Performance	Year pro.
Generic	BaCs [70]	C3	Sequential	PoW	Private	Fine grained, decentralized, single-factor, host-formed, dynamic	Decentralized	IoT	Secure AC with privacy protection	2021
	AC-manager [19]	C1	Sequential	Generic	Generic	Fine grained, decentralized, single-factor, host-formed, dynamic	Generic	Healthcare	AC without trusted third party	2021
	Multi-chain [23]	C1	Sequential	PBFT	Permissioned	Fine grained, hierarchical, single-factor, host-formed, dynamic	Generic	IoT	Scalable, trustworthy, low latency	2022
	Smart-AC [71]	C2	Sequential	PoW	Public	Fine grained, decentralized, single-factor, host-formed,	Generic	IoT	Cost effective solution	2021

						dynamic				
	AuthPrivacyChain [72]	C3	Sequential	Generic	Generic	Fine grained, decentralized, single-factor, host-formed, dynamic	Generic	Cloud	Prevent hackers from access	2020
	Subscription [22]	C2	Sequential	PBFT	Private	Fine grained, decentralized, single-factor, host-formed, dynamic	Generic	Mobile	High security with acceptable overhead	2021
	BACC [24]	C2	Sequential	PoW	Public	Fine grained, decentralized, single-factor, host-formed, dynamic	Generic	Cloud	Depend on network architecture, block GR	2020
Broadcast encryption	Symmetric [25]	C2	Sequential	PoW	Public	Fine grained, decentralized, single-factor, host-formed, dynamic	Generic	IoT	Low key management overhead	2023
	MIS [73]	C3	Sequential	PoStorage	Generic	Fine grained, hierarchical, single-factor, host-formed, dynamic	Generic	Medical	Safe and effective access control	2018
	Clinical [74]	C3	Sequential	PoW	Pubic	Fine grained, decentralized, single-factor, host-formed, dynamic	Generic	Medical	Strict access and privacy control	2020
Public key infrastructure	BBACS [75]	C2	Sequential	Generic	Generic	Fine grained, decentralized, single-factor, host-formed, dynamic	Generic	Medical	Low time cost and throughput	2018
	Trust-PKI [76]	C2	Sequential	PBFT	Permissioned	Fine grained, hierarchical, multi-factor, host-formed, dynamic	Generic	IoT	Time completion vary verifying requirements	2022
	SC-PKI [20]	C2	Sequential	Generic	Generic	Fine grained, decentralized, single-factor, host-formed, dynamic	Generic	IoT	Enhances security, avoid sole point of collapse	2022
	DBACP-IoTSG [77]	C2	Sequential	PBFT	Private	Fine grained, decentralized, single-factor, host-formed, dynamic	Decentralized	IoT-SG	Resistive against security attacks	2020
Attribute-based encryption	VO-PH-MAABE [78]	C3	Sequential	PoW	Private	Fine grained, semi-decentralized, multi-factor, host-formed, dynamic	Generic	IoMT	Privacy preserving, low computational cost	2022
	Attribute [79]	C3	Sequential	PBFT	Consortium	Fine grained, decentralized, single-factor, host-formed, dynamic	Generic	IoT	Protect security and privacy of data	2021
	IOTA [80]	C3	Multi-directional	Generic	Public	Fine grained, decentralized, multi-factor, host-formed, dynamic	Generic	IoT	Execution time is proportional to attributes	2021
	BACC-SDN [81]	C4	Sequential	PBFT	Generic	Fine grained, hierarchical, single-factor, host-formed, dynamic	Centralized	SDN	AC preventing sole point of collapse	2020
Identity-based encryption	BIDAC [82]	C2	Sequential	Generic	Generic	Fine grained, decentralized, single-factor, host-formed, dynamic	Generic	IoT	Can resist passive, active, physical attacks	2021
	SC-IBE [83]	C2	Sequential	Generic	Generic	Fine grained, decentralized, single-factor, host-formed, dynamic	Centralized	IoMT	Better performance with respect to others	2022
	SG-AC [84]	C2	Sequential	Custom PoS	Consortium	Fine grained, decentralized, single-factor, host-formed, dynamic	Generic	Smart grid	Low computation and communication cost	2019
Proxy re-encryption	Smart card [27]	C2	Sequential	PoW	Public	Fine grained, decentralized, multi-factor, host-formed, dynamic	Generic	Healthcare	Feasible solution consuming less time	2020
	PR-IoT [85]	C2	Sequential	PBFT	Consortium	Fine grained, decentralized, single-factor, host-formed, dynamic	Generic	IoT	Ensure data confidentiality and integrity	2021
	SC-PRE [86]	C2	Sequential	PBFT	Consortium	Fine grained, decentralized, single-factor, host-formed, dynamic	Centralized	SDN-IoT	High efficiency and security	2020
Signature-based	Dash-cam [87]	C2	Sequential	Raft	Private	Fine grained, decentralized, multi-factor, host-formed,	Decentralized	V2V	Less than 100ms latency for AC	2022

						dynamic				
	Signature-IoT [88]	C2	Sequential	PBFT	Private	Fine grained, decentralized, single-factor, host-formed, dynamic	Centralized	IoT-hospital	Low communication and computation overhead	2020
Certificate-based	BACS-IoD [89]	C4	Sequential	RPCA	Private	Fine grained, decentralized, single-factor, host-formed, dynamic	centralized	IoD-UAV	More functional attributes, better security	2020
Attribute-based	Attribute-IoT [90]	C2	Sequential	PBFT	Consortium	Fine grained, decentralized, single-factor, host-formed, dynamic	Generic	IoT	High efficiency, resistive against attacks	2019
	ZAIB [91]	C2	Sequential	PBFT	Consortium	Fine grained, decentralized, single-factor, host-formed, dynamic	Generic	IoT	Fulfils requirements of active defence	2023
	MDS [92]	C2	Sequential	PBFT	Consortium	Fine grained, decentralized, single-factor, host-formed, dynamic	Generic	Medical	Scalable and feasible access control	2021
Discretionary	Bell-LaPadula [93]	C2	Sequential	PBFT	Consortium	Fine grained, decentralized, single-factor, host-formed, dynamic	Generic	Medical	Low transaction execution, validation time	2021
Mandatory	MAC [21]	C1	Hierarchical	Custom	Private	Fine grained, hierarchical, single-factor, host-formed, static	Hierarchical	IoT	Secure communication in IoT nodes, fog, cloud	2021
Role-based	FDS-RB [94]	C2	Sequential	PBFT	Consortium	Fine grained, decentralized, single-factor, host-formed, static	Decentralized	FDS	Feasible and efficient solution	2020
	Role-IoT [95]	C2	Sequential	DPoS	Private	Fine grained, decentralized, single-factor, host-formed, static	Generic	IoT	Execution time is less than 1ms	2019
Capability-based	IoT-CCAC [96]	C4	Sequential	Tendermint	Consortium	Fine grained, decentralized, single-factor, host-formed, dynamic	Hierarchical	IoT	Secure, effective, and scalable AC	2021
	DCACI [26]	C3	Multi-directional	Generic	Public	Fine grained, decentralized, single-factor, host-formed, dynamic	Generic	IoT	Highly scalable access control	2019
	Cap-SC [97]	C3	Sequential	PoW	Private	Fine-grained, decentralized, single-factor, host-formed, dynamic	Generic	IoT	Lower gas consumption, privacy than BlendCAC	2020
Organizational-based	FairAccess [98]	C1	Sequential	PoW	Public	Fine-grained, decentralized, single-factor, host-formed, dynamic	Centralized	IoT-Organizational	Throughput of 7 transactions/s	2016
Time-based	EAM-AC [99]	C2	Sequential	PoS	Public	Fine-grained, decentralized, single-factor, host-formed, dynamic	Generic	Metaverse	Cost effective and resistant to attacks	2023
	Time-IoT [100]	C1	Sequential	PoAuthentication	Private	Fine-grained, decentralized, single-factor, host-formed, dynamic	Generic	IoT	Higher flexibility in access control	2020

7.2 Overall Assessment

Figure 6 highlights the visualization of the spreading of blockchain-formed AC in regard to BC proposition, BC-formed elements, AC approach, network variety, and publication trend.

Figure 6. Overall assessment (a) BC-formed AC proposition (b) BC variety (c) BC consensus (d) BC-formed AC approach (e) Network variety (f) Published year

Relying on Figure 6a, highest percentage (52.5%) of blockchain concept is held by C2 (AC using SCs or blockchain itself) in succession to C3 (22.5%), C1 (12.5%), C4 (7.5%). Next, relying on Figure 6b, 92.5% of BC-formed AC frameworks harness sequential blockchain, while only 5% harness multi-directional blockchain, and 2.5% only harness hierarchical blockchain. Moreover, when assessing the consensus approach harnessed in BC-formed AC frameworks, as highlighted in Figure 6c, it is apparent that PBFT is the foremost frequently harnessed consensus having a percentage of 35% in succession to PoW with 22.5%, 20% by generic consensus, and other consensus such as PoAuthentication, PoStake, Raft, PoStorage, and rest with least harnessing percentages. When assessing the blockchain-formed AC approaches reviewed in this context, 100% of them are fine-grained and host-formed, 85% are decentralized, 12.5% are

hierarchical, 2.5% are semi-decentralized, 87.5% have single-factor authentication, 12.5% have multi-factor authentication, 92.5% are dynamic, and 7.5% are static, relying on Figure 6d. Moreover, relying on Figure 6e, IoT is the foremost frequently (45%) used network type for BC-formed AC, in succession to by medical (12.5%), healthcare (5%), cloud (5%), IoMT (5%), and rest by other network types highlighted in Figure 6e. Finally, blockchain formed AC concept has been inaugurated by 2016, and since then there has been a surge of frameworks until 2020, and remained constant in 2021, and then there is a diminishing trend of research interest ever since 2021 up to present (2023).

H. Discussion

8.1 Chances

8.1.1 Enable dynamic AC

Dynamic AC exploits real-time conditions and time-varying parameters for AC unlike static AC which is owner-centric. Blockchains can facilitate dynamic AC by securely transferring dynamic AC parameters. As a case in point, blockchain-formed dynamic AC is feasible when AC is implemented for different sensitivity levels of data shared using blockchain. Furthermore, in blockchains, AC policies can be updated dynamically through consensus approaches where participants can collectively agree to changes in access permissions so that SCs can be updated accordingly.

8.1.2 Facilitate management of AC

Blockchain can act as a manger to perform various administration processes related to AC. AC manager is responsible for defining processes for authorization and revocation, authentications and AC, and auditing tasks. Blockchain formed AC management is decentralized and attempts to provide AC to stakeholders in a privacy preserving manner. Moreover, these managers can operate in different levels of a network such as network edge, aggregated edge, core, etc. having a hierarchy of blockchains with a view to provide AC in different levels. Furthermore, blockchains can act as a secure key management framework generating, distributing, and revoking keys for providing AC.

8.1.3 Automatic AC

Blockchain can implement automatic AC using SCs. Smart contracts are self-executing upon reaching specified conditions, so that AC policies can be specified as conditions to provide AC to users upon satisfying those conditions. They can be exploited to offer AC, authentication, and authorization in an automatic fashion. Moreover, blockchain formed customized AC techniques can store authorization related transactions in the blockchain by encrypting them to protect privacy with a view to provide AC. Smart contracts can verify the access privileges and provide authentication using different techniques.

8.1.4 Alignment with conventional AC

Blockchains go hand in hand with existing AC techniques. They are highly compatible with existing AC techniques by themselves implementing an AC technique using SCs, managing the aggregate AC process, or aiding in AC by secure data or AC parameter sharing. As a case in point, they are compatible with public-key infrastructure formed encryption and authorization by storing encrypted data in the blockchain to be decrypted by authorized personnel providing robust

authentication. Blockchains can store all transactions securely while a conventional AC technique can implement AC.

8.1.5 Preserving data and parameters for AC

Blockchains can securely store data and parameters that are required for AC by blockchain itself or using a conventional AC mechanism. Either way, blockchain ensures the purity of the data and parameters elevating the trustworthiness of the subsequent AC process. As a case in point, in encryption formed AC, blockchains can safely store the credentials such as private (secret) key with a view to provide AC to a resource. Another example is securely storing encrypted data encrypted using an encryption-formed AC technique in the blockchain. Furthermore, blockchains can store validation parameters to verify decryption results, data hash values, etc. in attribute formed encryption.

8.2 Difficulties

8.2.1 Performance supremacy of conventional AC

Conventional AC techniques among others encryption-formed and encryption-independent techniques that do not exploit blockchain can perform AC with lesser usage of network resources than when blockchain is integrated for AC. This is true in both blockchain aided AC and pure blockchain formed AC. The reason for that is blockchains use peer-to-peer communication and energy draining consensus strategies in block creation, propagation, and validation in the operation of achieving AC. Even though there are green consensus approaches and scalable blockchain platforms with parallel computation complexity, it is daunting to totally remove the performance degradation that can occur due to integration of blockchain in AC.

8.2.2 Reluctance to transfer from centralized AC

Access control techniques towards the beginning of the networking were mostly centralized in nature where AC policies are defined by a centralized authority. As a case in point, in mandatory AC, policies are predefined by a centralized authority and users' access to resources is determined by comparing policies with resources of users. However, blockchain-formed AC is typically decentralized in nature, where access to resources is provided in a decentralized approach without involvement of a trusted third party (public blockchain). Therefore, conventional networks exploiting centralized AC may be reluctant to transfer into blockchain-formed non-centralized AC systems.

8.2.3 AC susceptibilities of blockchain

Smart contracts can be exploited to implement automatic AC using blockchain. However, they are vulnerable in case the SC code contains flaws leading to unauthorized access and perform malicious actions in the network. In blockchain aided identity formed encryption for AC, if private keys are not properly managed, there can be a security vulnerability where malicious users can mimic as legitimate users. Moreover, blockchain formed AC systems can be subjected to insider attacks where authorized users with high privileges can manipulate transactions.

8.2.4 Difficulty in auditing AC

Even though blockchain transactions are transparent making transactions auditable, auditing AC to check whether AC functions properly without mis-behavior can be challenging. This is challenging as blockchain transactions are

pseudonymous containing pseudo cryptographic addresses rather than real addresses. Moreover, SCs can be complex to be analyzed by the auditors, as they may have been written using different programming languages and can be difficult to identify AC susceptibilities. Furthermore, the decentralized nature of blockchains can further intensify the difficulty in auditing AC, as there may not be any centralized authority to manage AC policies. Finally, auditing AC in blockchain-formed systems can demand specialized auditing tools that may not be readily available.

8.2.5 Difficulty in integrating on-chain AC policies with off-chain data storage

Typically, large content of data is not reserved in blockchain and is reserved in off-chain information reserves. In blockchain-formed AC systems, AC regulations and AC related entities (tokens, attributes, ciphered data, etc.) are reserved in blockchain to accomplish AC. Off-chain structures can contain various forms of data represented in various formats. Moreover, SC formed AC can function well withing the blockchain network, however, can be difficult to be integrated with external systems. Therefore, providing AC to off-chain storage from on-chain AC policies and entities can be challenging in light of the low interoperability that exists among on-chain and off-chain platforms as cross-chain communication is still an emerging field in research.

I. Conclusion, Recommended Actions, and Prospective Directions

This assessment paper first offered a recap of AC strategies such as encryption-formed AC, encryption independent AC, and AC models and then displayed AC approaches formed on granularity, control architecture, authentication method, location, and nature. Subsequent to supplying a recap of blockchain network, blockchain-formed AC was assessed by segmenting under AC technique. Founded on this scholarly assessment, we realized 4 methods in which blockchain is utilized for AC in networking: blockchain as an AC coordinator, AC using SCs, blockchain for secure storage of AC related parameters among others tokens, attributes etc. for AC, and securing data using blockchain for subsequent AC. Then, we minutely assessed blockchain-formed AC by categorizing assessed works related to above 4 methods of proposition, AC techniques, AC strategies, blockchain related elements, network elements etc. Finally, we explored the chances and difficulties of blockchain-formed AC.

This work inspects how contemporary blockchain-formed AC has been exploited in networking. Founded from the minute assessment, one can readily recognize the flows and discontinuities in blockchain-formed AC to recognize the areas where blockchain can be exploited for AC. Moreover, this inspection bestows recommended actions for overcoming the difficulties recognized for integrating blockchain for AC as a guideline for other researchers to develop their forthcoming research.

Built upon the recognized difficulties, subsequent recommended actions can be posited for blockchain-formed AC.

- For reducing the performance gap that exists between blockchain-formed AC and conventional AC in terms of latency, energy extraction, etc., several approaches can be exploited. First, energy conserving consensus

approaches among others green proof-of-work, green PBFT, etc. Next, multi-directional blockchain can be exploited instead of conventional blockchain to provide a scalable solution having parallel transaction computation capabilities.

- For meeting the challenge of reluctance to directly transfer from centralized AC to fully decentralized AC using blockchain, a hybrid centralized and distributed AC can be exploited having both centralized and distributed AC features. Specifically, instead of public blockchain, a consortium or a private blockchain could be exploited where the AC can be implemented in partially centralized mode where an organization may have some level of centralized authority.
- Several strategies can be exploited to counter-attack known AC vulnerabilities of blockchain. First, SCs have to be thoroughly verified before exploiting for AC to detect any vulnerability and correct them. Next, AC related parameters have to be protected either by using blockchain or another secondary mechanism to prevent them from exposing to third parties. In fact, blockchain has been exploited to store AC related parameters securely thanks to its privacy protecting and immutable features. The impact of insider attacks can be minimized by implementing a zero-trust architecture where users are assumed untrusted until proven trusted and by providing minimum privileges for a given user or role.
- Following strategies can be exploited to tackle difficulties in auditing in blockchain-formed AC: When malicious activity is detected from a pseudonymous address in a blockchain, such users can be blacklisted and removed from the blockchain. Human expertise can be improved by training sessions to analyze the SCs vulnerabilities. A partial centralized authority for AC can be implemented by using a consortium/private blockchain with a view to provide AC policies that can be audited later removing the auditing difficulties in totally decentralized pubic blockchain.
- For overcoming the difficulties in integrating on-chain AC policies with off-chain data storage, diverse approaches can be exploited. One can use oracles to maintain an effective communication between the blockchain and off-chain storage allowing SCs to access off-chain data. Moreover, cross chain validators and off-chain data proofs can be exploited to ensure that data accessed from off-chain is authentic.

Blockchains can facilitate providing dynamic AC with high automation and improved security reducing the potential for AC attacks. Future research may concentrate more techniques for further developing and standardizing providing AC for off-chain storage from on-chain AC. Specifically, forthcoming research can assess more on reducing known AC vulnerabilities of blockchain.

J. References

[1] D. Boneh, C. Gentry, and B. Waters, “Collusion resistant broadcast encryption with short ciphertexts and private keys,” in Annual international cryptology conference, pp. 258-275, Aug. 2005

[2] Y. Yang, "Broadcast encryption based non-interactive key distribution in MANETs," Journal of Computer and System Sciences, vol. 80, no. 3, pp.533-545, 2014
[3] S. Malani, J. Srinivas, A.K. Das, K. Srinathan, and Jo, M., "Certificate-based anonymous device access control scheme for IoT environment," IEEE Internet of Things Journal, vol. 6, no. 6, pp.9762-9773, 2019
[4] S.V. Belim, and S.Y. Belim, "Implementation of mandatory access control in distributed systems," Automatic Control and Computer Sciences, vol. 52, pp.1124-1126, 2018
[5] P.A.D.S.N. Wijesekara, K.L.K. Sudheera, G.G.N. Sandamali, and P.H.J. Chong, "An Optimization Framework for Data Collection in Software Defined Vehicular Networks," Sensors, vol. 23, no. 3, pp. 1600, 2023
[6] B. Toshniwal, K.D. Joshi, P. Shrivastava, and K. Kataoka, "BEAM: Behavior-based access control mechanism for SDN applications," in 2019 28th ICCCN, pp. 1-2, Jul. 2019
[7] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," IEEE Internet of Things Journal, vol. 6, no. 2, pp.1594-1605, 2018
[8] P.A.D.S.N. Wijesekara, K.L.K. Sudheera, G.G.N. Sandamali, and P.H.J. Chong, "Data Gathering Optimization in Hybrid Software Defined Vehicular Networks," in 20th Academic Sessions, p. 59, Jun. 2023
[9] D.T. Manurung, "Designing of user authentication based on multi-factor authentication on wireless networks," Jour of Adv Research in Dynamical & Control Systems, vol. 12, no. 1, pp. 201-209, 2020
[10] S. Yu, K. Ren, and W. Lou, "FDAC: Toward fine-grained distributed data access control in wireless sensor networks," IEEE transactions on parallel and distributed systems, vol. 22, no. 4, pp.673-686, 2010
[11] R. Li, J. Li, and H.H. Chen, "DKMS: distributed hierarchical access control for multimedia networks," International Journal of Security and Networks, vol. 2, no. 1-2, pp.3-10, 2007
[12] P.A.D.S.N. Wijesekara, and S. Gunawardena, "A Review of Blockchain Technology in Knowledge-Defined Networking, Its Application, Benefits, and Challenges," Network, vol. 3, no. 3, pp. 343-421, 2023
[13] M. Yu, S. Sahraei, S. Li, S. Avestimehr, S. Kannan, and P. Viswanath, "Coded merkle tree: Solving data availability attacks in blockchains," in International Conference on Financial Cryptography and Data Security, pp. 114-134, Feb. 2020
[14] S. Ko, K. Lee, H. Cho, Y. Hwang, and H. Jang, "Asynchronous federated learning with directed acyclic graph-based blockchain in edge computing: Overview, design, and challenges," Expert Systems with Applications, vol. 223, p.119896, 2023
[15] L.A. Ajao, J. Agajo, E.A. Adedokun, and L. Karngong, "Crypto hash algorithm-based blockchain technology for managing decentralized ledger database in oil and gas industry," J, vol. 2, no. 3, pp.300-325, 2019
[16] E.O. Kiktenko, N.O. Pozhar, M.N. Anufriev, A.S. Trushechkin, R.R. Yunusov, Y.V. Kurochkin, A.I. Lvovsky, and A.K. Fedorov, "Quantum-secured blockchain," Quantum Science and Technology, vol. 3, no. 3, p.035004, 2018

[17] S.M.H. Bamakan, A. Motavali, and A.B. Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," Expert Systems with Applications, vol. 154, p.113385, 2020
[18] P.A.D.S.N. Wijesekara, and S. Gunawardena, "A Comprehensive Survey on Knowledge-Defined Networking," Telecom, vol. 4, no. 3, pp. 477-596, 2023
[19] U. Chelladurai, and S. Pandian, "A novel Blockchain-based Access Control Manager to Electronic Health Records (EHRs)," Blockchain for Smart Cities, pp. 233-244, 2021
[20] P. Bai, S. Kumar, and U. Dohare, "Smart Contract Assisted Public Key Infrastructure for Internet of Things," in IEMIS 2022, vol. 3, pp. 215-229, Sep. 2022
[21] S. Algarni, F. Eassa, K. Almarhabi, A. Almalaise, E. Albassam, K. Alsubhi, and M. Yamin, "Blockchain-based secured access control in an IoT system," Applied Sciences, vol. 11, no. 4, p.1772, 2021
[22] K. Xue, X. Luo, H. Tian, J. Hong, D.S. Wei, and J. Li, "A blockchain based user subscription data management and access control scheme in mobile communication networks," IEEE Transactions on Vehicular Technology, vol. 71, no. 3, pp.3108-3120.
[23] A.I. Abdi, F.E. Eassa, K. Jambi, K. Almarhabi, M. Khemakhem, A. Basuhail, and M. Yamin, "Hierarchical blockchain-based multi-chaincode access control for securing IoT systems," Electronics, vol. 11, no. 5, p.711, 2022
[24] N. Sohrabi, X. Yi, Z. Tari, and I. Khalil, "BACC: Blockchain-based access control for cloud data," in Australasian Computer Science Week Multiconference, pp. 1-10, Feb. 2020
[25] M.J. Mihaljević, M. Knežević, D. Urošević, L. Wang, and S. Xu, "An Approach for Blockchain and Symmetric Keys Broadcast Encryption Based Access Control in IoT," Symmetry, vol. 15, no. 2, p.299, 2023
[26] S.K. Pinjala, and K.M. Sivalingam, "DCACI: A decentralized lightweight capability based access control framework using IOTA for Internet of Things," in 2019 IEEE 5th WF-IoT, pp. 13-18, Apr. 2019
[27] B. Sharma, R. Halder, and J. Singh, "Blockchain-based interoperable healthcare using zero-knowledge proofs and proxy re-encryption," in 2020 COMSNETS, pp. 1-6, Jan. 2020
[28] I. Riabi, H.K.B. Ayed, and L.A. Saidane, "A survey on Blockchain based access control for Internet of Things," in 2019 15th IWCMC, pp. 502-507, Jun. 2019
[29] S. Namane, and I. Ben Dhaou, "Blockchain-based access control techniques for iot applications," Electronics, vol. 11, no. 14, p.2225, 2022
[30] P. Patil, M. Sangeetha, and V. Bhaskar, "Blockchain for IoT access control, security and privacy: a review," Wireless Personal Communications, vol. 117, pp.1815-1834, 2021
[31] M. Sookhak, M.R. Jabbarpour, N.S. Safa, and F.R. Yu, "Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues," Journal of Network and Computer Applications, vol. 178, p.102950, 2021
[32] S. Rouhani, and R. Deters, "Blockchain based access control systems: State of the art and challenges," in IEEE/WIC/ACM International Conference on Web Intelligence, pp. 423-428, Oct. 2019

[33] F. Ghaffari, E. Bertin, J. Hatin, and N. Crespi, "Authentication and access control based on distributed ledger technology: A survey," in 2020 2nd Conference on BRAINS, pp. 79-86, Sep. 2020

[34] P.A.D.S.N. Wijesekara, "A study in University of Ruhuna for investigating prevalence, risk factors and remedies for psychiatric illnesses among students," Scientific Reports, vol. 12, no. 1, pp. 12763, 2022

[35] P.A.D.S.N. Wijesekara, and Y.K. Wang, "A Mathematical Epidemiological Model (SEQIJRDS) to Recommend Public Health Interventions Related to COVID-19 in Sri Lanka," COVID, vol. 2, no. 6, pp. 793-826, 2022

[36] Y. Wang, M. Xu, Z. Feng, Q. Li, and Q. Li, "Session-based access control in information-centric networks: Design and analyses," in 2014 IEEE 33rd IPCCC, pp. 1-8, Dec. 2014

[37] Q. Wang, W. Li, and Z. Qin, "Proxy re-encryption in access control framework of information-centric networks," IEEE Access, vol. 7, pp.48417-48429, 2019

[38] T. Chen, K. Lei, and K. Xu, "An encryption and probability based access control model for named data networking," in 2014 IEEE 33rd IPCCC, pp. 1-8, Dec. 2014.

[39] Y. Yu, J. Shi, H. Li, Y. Li, X. Du, and M. Guizani, "Key-policy attribute-based encryption with keyword search in virtualized environments," IEEE Journal on Selected Areas in Communications, vol. 38, no. 6, pp.1242-1251, 2020

[40] K. Sowjanya, and M. Dasgupta, "A ciphertext-policy Attribute based encryption scheme for wireless body area networks based on ECC," Journal of Information Security and Applications, vol. 54, p.102559, 2020

[41] H. Yan, Y. Wang, C. Jia, J. Li, Y. Xiang, and W. Pedrycz, "IoT-FBAC: Function-based access control scheme using identity-based encryption in IoT," Future Generation Computer Systems, vol. 95, pp. 344-353, 2019

[42] T.H. Yuen, Y. Zhang, S.M. Yiu, and J.K. Liu, "Identity-based encryption with post-challenge auxiliary inputs for secure cloud applications and sensor network," in Computer Security-ESORICS 2014, pp. 130-147, Sep. 2014

[43] C. Seneviratne, P.A.D.S.N. Wijesekara, and H. Leung, "Performance analysis of distributed estimation for data fusion using a statistical approach in smart grid noisy wireless sensor networks," Sensors, vol. 20, no. 2, pp. 567, 2020

[44] A. Seleznyov, M.O. Ahmed, and S. Hailes, "ADAM: An agent-based middleware architecture for distributed access control," in Twenty-Second International Multi-Conference on Applied Informatics: Artificial Intelligence and Applications, pp. 200-205, Jan. 2004

[45] J. Kuriharay, E. Uzun, and C.A. Wood, "An encryption-based access control framework for content-centric networking," in 2015 IFIP networking, pp. 1-9, May. 2015

[46] Y. Tao, and Y. Zhu, "An interest-based access control scheme via edge verification in Named Data Networking," International Journal of Communication Systems, vol. 35, no. 10, p.e5169, 2022

[47] K. Xue, P. He, X. Zhang, Q. Xia, D.S. Wei, H. Yue, and F. Wu, "A secure, efficient, and accountable edge-based access control framework for information centric networks," IEEE/ACM Transactions on Networking, vol. 27, no. 3, pp.1220-1233, 2019

[48] Q. Wang, and H. Jin, "Data leakage mitigation for discretionary access control in collaboration clouds," in 16th ACM symposium on Access control models and technologies, pp. 103-112, Jun. 2011

[49] P.A.D.S.N. Wijesekara, K.L.K. Sudheera, G.G.N. Sandamali, and P.H.J. Chong, "Machine Learning Based Link Stability Prediction for Routing in Software Defined Vehicular Networks," in 20th Academic Sessions, p. 60, Jun. 2023

[50] M. Kalinin, V. Krundyshev, E. Rezedinova, and P. Zegzhda, "Role-based access control for vehicular adhoc networks," in 2018 IEEE International BlackSeaCom, pp. 1-5, Jun. 2018

[51] Y. Liu, B. Zhao, Y. An, and J. Guo, "DACAS: integration of attribute-based access control for northbound interface security in SDN," World Wide Web, vol. 26, pp.2143–2173, 2023

[52] R. Xu, Y. Chen, E. Blasch, and G. Chen, "A federated capability-based access control mechanism for internet of things (iots)," in Sensors and Systems for Space Applications XI, vol. 10641, pp. 291-307, May. 2018

[53] C. Belbergui, N. Elkamoun, and R. Hilal, "Spatial and Temporal Organization Based Access Control for Wireless Network as a Component of Security Requirements," Wireless Personal Communications, vol. 97, pp.4587-4619, 2017

[54] B. Wang, W. Li, and N.N. Xiong, "Time-based access control for multi-attribute data in internet of things," Mobile Networks and Applications, vol. 26, pp.797-807, 2021

[55] P.A.D.S.N. Wijesekara, and S. Gunawardena, "A Machine Learning-Aided Network Contention-Aware Link Lifetime- and Delay-Based Hybrid Routing Framework for Software-Defined Vehicular Networks," Telecom, vol. 4, no. 3, pp. 393-458, 2023

[56] G. Yamanaka, T. Nishio, M. Morikura, K. Yamamoto, Y. Maki, S.I. Eitoku, and T. Indo, "Geo-fencing in wireless LANs with camera for location-based access control," in 2019 16th IEEE Annual CCNC, pp. 1-4, Jan. 2019

[57] Y.F. Tseng, C.I. Fan, and C.Y. Wu, "FGAC-NDN: Fine-grained access control for named data networks," IEEE Transactions on Network and Service Management, vol. 16, no. 1, pp.143-152, 2018

[58] Z. Liu, Z. Wang, X. Cheng, C. Jia, and K. Yuan, "Multi-user searchable encryption with coarser-grained access control in hybrid cloud," in 2013 Fourth International Conference on EIDWT, pp. 249-255, Sep. 2013

[59] H.M.D.P.M. Herath, W.A.S.A. Weraniyagoda, R.T.M. Rajapaksha, P.A.D.S.N. Wijesekara, K.L.K. Sudheera, & P.H.J. Chong, "Automatic Assessment of Aphasic Speech Sensed by Audio Sensors for Classification into Aphasia Severity Levels to Recommend Speech Therapies," Sensors, vol. 22, no. 18, pp. 6966, 2022

[60] D. Panno, and S. Riolo, "A new centralized access control scheme for D2D-enabled mmWave networks," IEEE Access, vol. 7, pp.80697-80716, 2019

[61] M.N. Sharphathy, and V. Sumalatha, "SSS-EC: Cryptographic based Single-Factor Authentication for Fingerprint Data with Machine Learning Technique," in 2023 2nd ICECAA, pp. 308-315, Jul. 2023.

[62] P.A.D.S.N. Wijesekara, W.M.A.K. Sangeeth, H.S.C. Perera, and N.D. Jayasundere, "Underwater Acoustic Digital Communication Channel for an UROV," in 5th Annual Research Symposium (ARS2018), p. E17, Jan. 2018

[63] C.R. Taylor, D.C. MacFarland, D.R. Smestad, and C.A. Shue, "Contextual, flow-based access control with scalable host-based SDN techniques," in IEEE INFOCOM 2016, pp. 1-9, Apr. 2016

[64] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "URSA: ubiquitous and robust access control for mobile ad hoc networks," IEEE/ACM transactions on networking, vol. 12, no. 6, pp.1049-1063, 2004

[65] P.A.D.S.N. Wijesekara, "Deep 3D Dynamic Object Detection towards Successful and Safe Navigation for Full Autonomous Driving," Open Transportation Journal, vol. 16, no. 1, pp. e187444782208191, 2022

[66] Q. Yao, Q. Wang, X. Zhang, and J. Fei, "Dynamic access control and authorization system based on zero-trust architecture," in 2020 1st International CCRIS, pp. 123-127, Oct. 2020

[67] M. Milutinovic, W. He, H. Wu, and M. Kanwal, "Proof of luck: An efficient blockchain consensus protocol," in 1st Workshop on System Software for Trusted Execution, pp. 1-6, Dec. 2016

[68] M. Turkanović, and B. Podgorelec, "Signing blockchain transactions using qualified certificates," IEEE Internet Computing, vol. 24, no. 6, pp.37-43, 2020

[69] T. Miyamae, F. Kozakura, M. Nakamura, and M. Morinaga, "ZGridBC: Zero-Knowledge Proof Based Scalable and Privacy-Enhanced Blockchain Platform for Electricity Tracking," IEICE TRANSACTIONS on Information and Systems, vol. 106, no. 7, pp.1219-1229, 2023

[70] N. Shi, L. Tan, C. Yang, C. He, J. Xu, Y. Lu, and H. Xu, "BacS: A blockchain-based access control scheme in distributed internet of things," Peer-to-peer networking and applications, vol. 14, pp.2585-2599, 2021

[71] P. Chinnasamy, B. Vinodhini, V. Praveena, C. Vinothini, and B.B. Sujitha, "Blockchain based access control and data sharing systems for smart devices," in Journal of Physics: Conference Series, vol. 1767, no. 1, p. 012056.

[72] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu, "AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud," IEEE Access, vol. 8, pp.70604-70615, 2020

[73] Y. Du, J. Liu, Z. Guan, and H. Feng, "A medical information service platform based on distributed cloud and blockchain," in 2018 IEEE SmartCloud, pp. 34-39, Sep. 2018

[74] H. Jin, C. Xu, Y. Luo, and P. Li, "Blockchain-based secure and privacy-preserving clinical data sharing and integration," in ICA3PP 2020, pp. 93-109, Oct. 2020

[75] X. Zhang, S. Poslad, and Z. Ma, "Block-based access control for blockchain-based electronic medical records (EMRs) query in eHealth," in 2018 IEEE GLOBECOM, pp. 1-7, Dec. 2018

[76] W. Viriyasitavat, L.D. Xu, A. Sapsomboon, G. Dhiman, and D. Hoonsopon, "Building trust of Blockchain-based Internet-of-Thing services using public key infrastructure," Enterprise Information Systems, vol. 16, no. 12, p.2037162, 2022

[77] B. Bera, S. Saha, A.K. Das, and A.V. Vasilakos, "Designing blockchain-based access control protocol in IoT-enabled smart-grid system," IEEE Internet of Things Journal, vol. 8, no. 7, pp.5744-5761, 2020

[78] X. Yang, and C. Zhang, "Blockchain-based multiple authorities attribute-based encryption for EHR access control scheme," Applied Sciences, vol. 12, no. 21, p.10812, 2022

[79] X. Lu, S. Fu, C. Jiang, and P. Lio, "A fine-grained IoT data access control scheme combining attribute-based encryption and blockchain," Security and Communication Networks, vol. 2021, pp.1-13, 2021

[80] Y. Zhang, R. Nakanishi, M. Sasabe, and S. Kasahara, "Combining IOTA and attribute-based encryption for access control in the Internet of Things," Sensors, vol. 21, no. 15, p.5053, 2021

[81] D. Chattaraj, S. Saha, B. Bera, and A.K. Das, "On the design of blockchain-based access control scheme for software defined networks," in IEEE INFOCOM 2020, pp. 237-242, Jul. 2020

[82] Y. Ji, X. Xiao, F. Wu, F. Chen, and S. Liu, "BIDAC: Blockchain-Enabled Identity-Based Data Access Control in IoT," in IEEE/WIC/ACM International Conference on WI-IAT, pp. 400-405, Dec. 2021

[83] P. Sharma, N.R. Moparthi, S. Namasudra, V. Shanmuganathan, and C.H. Hsu, "Blockchain-based IoT architecture to secure healthcare system using identity-based encryption," Expert Systems, vol. 39, no. 10, p.e12915.

[84] Y. Zhou, Y. Guan, Z. Zhang, and F. Li, "A blockchain-based access control scheme for smart grids," in 2019 International Conference on NaNA, pp. 368-373, Oct. 2019

[85] K.O.B.O. Agyekum, Q. Xia, E.B. Sifah, C.N.A. Cobblah, H. Xia, and J. Gao, "A proxy re-encryption approach to secure data sharing in the internet of things based on blockchain," IEEE Systems Journal, vol. 16, no. 1, pp.1685-1696, 2021

[86] Y. Gao, Y. Chen, H. Lin, and J.J. Rodrigues, "Blockchain based secure IoT data sharing framework for SDN-enabled smart communities," in IEEE INFOCOM 2020, pp. 514-519, Jul. 2020

[87] D. Na, and S. Park, "Blockchain-Based Dashcam Video Management Method for Data Sharing and Integrity in V2V Network," IEEE Access, vol. 10, pp.3307-3319, 2022

[88] S. Saha, A.K. Sutrala, A.K. Das, N. Kumar, & J.J. Rodrigues, "On the design of blockchain-based access control protocol for IoT-enabled healthcare applications," in ICC 2020, pp. 1-6, Jun. 2020

[89] B. Bera, D. Chattaraj, and A.K. Das, "Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment," Computer Communications, vol. 153, pp.229-249, 2020

[90] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," IEEE Access, vol. 7, pp.38431-38441, 2019

[91] S.M. Awan, M.A. Azad, J. Arshad, U. Waheed, and T. Sharif, "A Blockchain-Inspired Attribute-Based Zero-Trust Access Control Model for IoT," Information, vol. 14, no. 2, p.129, 2023.

[92] Y. Chen, L. Meng, H. Zhou, and G. Xue, "A blockchain-based medical data sharing mechanism with attribute-based access control and privacy protection," Wireless Communications and Mobile Computing, vol. 2021, pp.1-12, 2021

[93] R. Kumar, and R. Tripathi, "Scalable and secure access control policy for healthcare system using blockchain and enhanced Bell–LaPadula model,"

Journal of Ambient Intelligence and Humanized Computing, vol. 12, pp.2321-2338, 2021

[94] Y. Ding, L. Feng, Y. Qin, C. Huang, P. Dong, L. Gao, and Y. Tan, "Blockchain-based access control mechanism of federated data sharing system," in 2020 IEEE ISPA/BDCloud/SocialCom/SustainCom, pp. 277-284, Dec. 2020

[95] S. Sun, S. Chen, R. Du, W. Li, and D. Qi, "Blockchain based fine-grained and scalable access control for iot security and privacy," in 2019 IEEE Fourth International Conference on DSC, pp. 598-603, Jun. 2019

[96] M.A. Bouras, B. Xia, A.O. Abuassba, H. Ning, and Q. Lu, "IoT-CCAC: a blockchain-based consortium capability access control approach for IoT," PeerJ Computer Science, vol. 7, p.e455, 2021

[97] Y. Nakamura, Y. Zhang, M. Sasabe, and S. Kasahara, "Exploiting smart contracts for capability-based access control in the internet of things," Sensors, vol. 20, no. 6, p.1793, 2020

[98] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "FairAccess: a new Blockchain-based access control framework for the Internet of Things," Security and communication networks, vol. 9, no. 18, pp.5943-5964, 2016

[99] M. HOCAOĞLU, A BLOCKCHAIN-BASED EDUCATIONAL ASSETS MANAGEMENT AND ACCESS CONTROL MODEL FOR THE METAVERSE, Doctoral dissertation, Karabuk University, Turkey, 2023

[100] T.H. Thanh, T.D. Nguyen, and H. Tan, "A Blockchain-Based Access Control Solution for IoT: Array," Journal of Science and Technology on Information and Communications, vol. 1, no. 3, pp.15-23, 2020