Decentralized Access Control using Blockchain Technology for Application in Smart Farming

Normaizeerah Mohd Noor[1], Noor Afiza Mat Razali[2]*, Nur Atiqah Malizan[3], Muslihah Wook[5], Nor Asiakin Hasbullah[6]
Defence Science and Technology Faculty
National Defence University of Malaysia
Sungai Besi, Kuala Lumpur Malaysia.

Khairul Khalil Ishak[4]
Center of Cyber Security and Big Data
Management and Science University
Shah Alam, Selangor, Malaysia

***Abstract*—The application of the Internet of Things (IoT) plays a crucial role in the fourth industrial revolution. The sophistication of technology due to the integration of heterogenous smart devices open a new threat from various aspects. Access control is the first line of defence to ensure that IoT resources are secure by preventing illegitimate users from gaining access to these resources. However, access control mechanisms face the limitation of technology in large scale IoT deployments since they are based on a centralized architecture. Significant research concerning decentralized access control solutions for securing IoT resources using combined techniques, such as blockchain, have caught much research attention in recent years. Nevertheless, research for decentralized access control for application in smart farming domain remain as a gap. Thus, this study presented a structured literature review on 81 articles related to the field of access control in IoT and blockchain technology to understand the challenges of centralized access control in securing IoT resources. This study serves as a foundation for decentralized access control using blockchain technology and its application to ensure the IoT actuators and sensors security with the aim to be applied in smart farming. This paper was deliberated based on systematic literature review that was searched from four different database platforms between 2018 and 2021. This study mostly addresses the relevant techniques/approaches including blockchain technology, access control model, key management mechanism and the combination of all three methods. The possible impacts, gap, procedures and evaluation of the decentralized access control are highlighted along with major trends and challenges.**

***Keywords*—Blockchain; access control; smart contract; internet of thing**

I. Introduction

Smart farming is the technology enabler that support food security [1] and it has brought changes that reduce costs and minimise environmental constraints, thereby boosting production productivity [2]. Smart farming is capable in enhancing the quality and quantity of production, predicting any possible crop diseases, while optimising agricultural resources and its process. Technological advancement plays a vital role in catalysing the transformation of the smart farming [3]. Data collection using IoT devices such as actuators, sensors, drones and robots are connected to the network for real time data transmission to assist operations. However, the new norm of devices connectivity opened security and privacy risks for device-based services. Unauthorised access to the devices is among the risk. The situation can be controlled by secure mechanism for authentication in all devices or connected systems. Access control and authentication are considered to be the first lines of defence in restricting unauthorised users from gaining access to IoT resources that provide the data to the smart farming ecosystem. Authentication enables legitimate users to access resources in an authorised manner [4] supporting by access control as the main mechanism for authentication and authorisation, as well as the authority to control resources [5]. Authentication will guarantee that only authorised users are allowed to access a resource. In IoT, access control assigns different privileges to various users regarding the resources of a wide IoT network [6]. However, most existing IoT systems have adopted a conventional access control method which relies on a centralized approach. This may lead to a single point of failure or performance bottlenecks. For instance, an attacker can act as an administrator by stealing authority to illegally access resources, causing a lack of confidence and integrity in such systems. Centralized systems can also be utilised to allow device tracking or related activities, which may compromise privacy. As the number of connected devices increases, it is difficult to manage massive numbers of devices in collecting and handling data using the traditional centralized approach. As a result, IoT has created a challenge in adopting centralized management since it is unable to cope with a large-scale system due to heterogenous IoT and scalability issues [7], leading to frequent bottlenecks. Researchers have found that applying the blockchain technology can be an alternative solution to this issue. However, the adaptation of decentralized access control in smart farming requires further study to estimate the optimum level of adaptation. Based on the problem statement deliberated above, this research presents a systematic literature review (SLR) on the decentralized access control method using blockchain due to the importance of decentralized access control to manage the heterogeneity and expansion of IoT resources and their application in various domains especially in the domain of smart farming.

The contribution of this review paper is to provide extensive review of research articles to determine the existing gaps, methods and techniques in applying decentralized access control to secure IoT resources. The aim of this study is to

Corresponding Author*
FRGS/1/2021/ICT07/UPNM/02/1

understand the current state of related work to address the following research questions:

RQ1: What are the gaps in current access control systems within the IoT ecosystem which can be enhanced by applying blockchain technology?

RQ2: What methods/techniques/approaches are suitable for enhancing access control within the IoT ecosystem by applying blockchain technology?

RQ3: How the evaluation was done to determine the effectiveness of methods/techniques/approaches in previous studies.

II. Research Methodology

The research methodology adopted in this study is the structured literature review (SLR). The SLR was conducted using the following methodology as shown in Fig. 1. Four databases (ScienceDirect, IEEE, Springer and ACM) were employed. Search query was performed to obtain the relevant research articles including journals, book chapters, proceeding papers and books. This paper examines all applicable articles related to decentralized access control for IoT environment application. The method described in [8] was utilised to choose the most important articles related to this research objectives. Articles filtering was done using the six filters that are defined in Fig. 1. A total of 8567 articles were gathered using the following search strings: "Access Control", "Decentral*", "IoT" or "Internet of Thing" and "Blockchain". Then, after second filter was employed, 5964 articles published between 2018 and 2021 was selected. Next, used source types as filters to reduce the number of articles, thereby producing 2562 results. Then selected papers written in English which yielded 2560 articles. The computer science field was chosen according to the abstract of the paper, resulting in 146 articles. After thoroughly reviewing each paper, a final selection of 81 articles was made upon extensive evaluation based on this study's research questions.

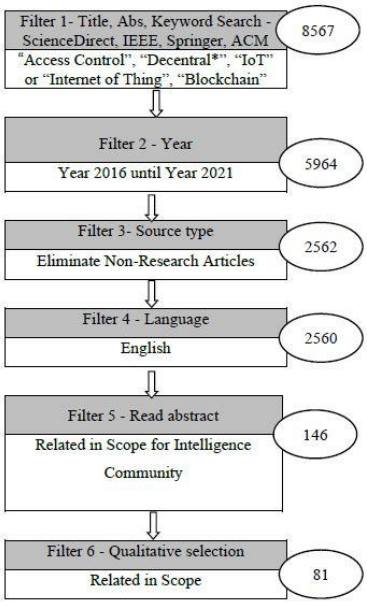

Fig. 1. Filters of the SLR Strategy.

III. Discussion

Blockchain technology adaptation has been proposed to overcome centralized access control issues. It is expected to be the first line of defence before information sharing of resources is being allowed [9]. Blockchain can also solve security and privacy issues using the decentralized feature by providing security and encryption, making it difficult for attackers since it can detect any illegal changes in its records [10]. To secure resources within an organisation, blockchain technology utilises a cryptography feature that has both a public key and private key that authenticate users who register themselves in the system. A user's personal information is applied to authenticate an individual's identity by employing unique identification, name or biometric data mapped on the user's public key and stored in the blockchain-based smart contracts. Thus, blockchain only provides access to authorised users when accessing resources by authenticating the public key [11].

A. Gaps of Existing Access Control Systems in the IoT Ecosystem

Fig. 2 presents the research articles regarding access control in IoT by various sectors to determine the gaps to better understand access control issues in the IoT ecosystem. The findings was divided into the several sectors which include smart cities, smart vehicles, smart grid, smart homes, healthcare, banking, property, industry (manufacturing and construction) and general IoT [7], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [35], [38], [39], [40], [41], [42], [43]. To answer RQ1 formulated in this study, the analysis was done to understand current access control gaps focusing on the IoT ecosystem that is determined based on the SLR outcomes. The issues were categorised into four groups based on the gaps and problem statement of the literatures: 1) common insufficient IoT access control issues, 2) blockchain combination approaches utilised in the literature, 3) cyberattack issues and 4) lack of security and privacy issues. Based on the literature, several researchers have discussed the common problems in the IoT ecosystem which are: centralized architecture, single point of failure, scalability, heterogeneity, mobility and high energy consumption. The problems are added by the nature of IoT actuators and sensors that are resource-constraints with bandwidth limitations for communication and unable to execute high and memory-intensive computation operations. These problems are major challenges that hinder optimum access control [7]. Researchers in [44], [45, 46], [47] proposed the development of design and standards to secure communication protocols that are capable of interfacing existing systems, collecting data generated by IoT resources and exchanging data to solve trust issues among devices.

Currently, most existing solutions for IoT access control have been developed based on conventional access control architectures, mechanisms, models and policies that mainly rely on single server and third-party entities, leading to high possibility in serious information breach. Failure to ensure the effectiveness of access control may lead to access of information by restricted third party [48]. Thus, conventional access control are inadequate for addressing dynamic and

diverse access control requirements for future IoT ecosystems with new emerging capabilities and application [13] that lead to various security risk including exposure to cyberattack [14]. Common cyberattacks comprise of reuse attacks, DDOS attacks [49] and poisoning attacks. These attacks can cause various drawbacks by exploiting and hijacking the system to retrieve sensitive data. In [50], it was found that attackers can capture, steal or duplicate data to perform illegal activities. In [51], the discussion was done regarding single trusted entities that have become more challenging since these centralized security companies may be biased; permitting illegal or transitive requests while denying legal requests. Attackers can destroy, change or misuse sensitive data and sell it for monetary benefits, leading to data disclosure of user security [31] and lack of data integrity.

Various schemes and cryptographic algorithms were proposed to solve security related issues of IoT by researchers [52], [53, 54]. The proposed methods include a hybrid cryptographic algorithm technique capable of substituting conventional cryptographic algorithms. The same level of security can be simultaneously maintained, leading to additional cost and time for completing encryption and decryption processes [44, 47]. However, these techniques are not feasible since the IoT environment has resource constraints such as high computational power and energy consumption of IoT actuators and sensors. The cryptographic method that involve massive data encryption in IoT actuators and sensors that required higher energy consumption also is not possible to be implemented [55].

To eliminate the gap caused by conventional access control, researchers proposed that the combination of access control and blockchain technology in the IoT ecosystem to resolve issues related to the centralized mechanism. However, IoT network transactions that exceed the capabilities of IoT actuators and sensors, can cause further problems. The complexity of blockchain solutions using the consensus algorithm is beyond the capabilities of IoT actuators and sensors, resulting in constraints in computing and processing and limited bandwidth. Researchers also suggested the consideration of a lightweight key management solution with robust and low resource designs. Based on the deliberations in this section, this study presents a summary of the existing gaps mentioned in previous research in Table I.

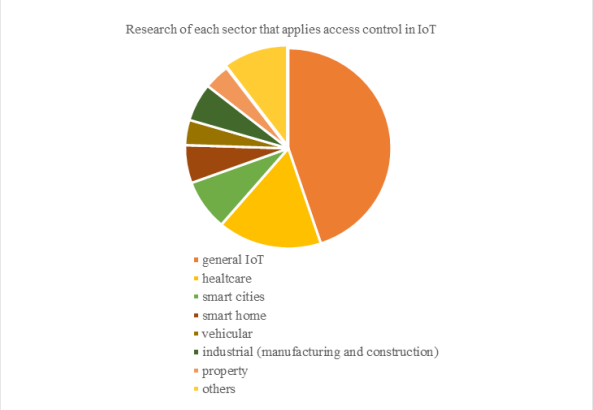

Fig. 2. Access Control Application in IoT for Each Sector.

TABLE I. GAPS IN EXISTING ACCESS CONTROL SOLUTIONS

Current Gaps	Literature Articles
Conventional access control (in centralized architecture) causing single point of failure IoT characteristic related issues (heterogeneity, scalability, mobility, limited power resources, memory size, computational capacity	[7], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [44], [46], [48], [51], [53], [55], [23], [24], [25], [26], [27]
IoT actuators and sensors unable to store large transactions	[23],
Lack of trust and fairness in nodes	[48], [17], [20], [23], [28], [29], [30]
Information leak due to un-restricted access control	[14], [15]
IoT low performance for conventional access control	[31]
Privacy leak risk	[29]
Lack of strong encryption enforcement	[47], [32]
Lack of standardised communication protocol	[47]
Malicious attacks and cyberattacks (including identity spoofing, message eavesdropping, message tampering, content poisoning, physical and cloning attacks)	[11], [45], [46], [14], [49], [50], [20], [25], [33], [34]
Lack of authentication mechanism	[45], [52], [50], [19], [22], [27], [34], [36] ,[37], [35]
Resource constrained IoT actuators and sensors	[51]
Security weaknesses and vulnerabilities	[46], [49], [55], [33], [38], [39], [56]
Access control founded on blockchain technology related issues in IoT environment: higher cost, increased transaction delays and scalability	[53], [40], [41]
Complexity of consensus algorithm beyond the capabilities of IoT actuators and sensors	[53]
Lack of access control mechanism efficient for the IoT environment	[38]
Centralized client server structure and management schemes less efficient for IoT environment	[25], [32] ,[33], [42], [43] [42]
High costs in guarding security by combining multiple security technologies	[46]
Traditional fog/cloud computing issues	[57]
Low efficiency in centralized operating environment	[54]
Insufficient conventional storage	[55]
Lack of communication control in data flow	[13]

From the SLR, it can be concluded that to enhance the access control framework in IoT ecosystems, it is crucial to further investigate the following mechanism: access control, trust, elimination of third parties, authentication, privacy and security. The trade-off between the decentralised access control supporting technologies with computing and processing power are vital to be further researched to find the optimum solution.

B. Techni[58]Ques and Approaches for Existing Decentralised Access Control in IoT

To employ decentralized access control in the IoT ecosystem, researchers have recently applied various techniques to solve the issues presented when addressing RQ1, which are: trust, communication, third party entities, privacy and security problems. Next, evaluated articles were discussed to address RQ2. Based on the literature review, all research papers have presented the use of either blockchain technology, access control models, key management or the combination of all three approaches to efficiently manage access control for IoT resources. The results revealed that only 10 papers used blockchain technology as a strategy for the decentralized access control, while another 10 applied the access control model by adopting the blockchain technology. A total of 12 papers had combined blockchain technology and key management, while three papers combined all three techniques (blockchain technology, access control model and key management techniques). Other techniques were also discussed in these papers, such as IOTA and tangle technology. IOTA is a protocol for securing data communication between IoT actuators and sensors with lightweight quantum resistant cryptocurrency devices. Tangle is an open-source distributed ledger similar to the blockchain technology [21]. Fig. 3 provides a summary of the reviewed papers in this study according to the type of decentralized access control approaches used.

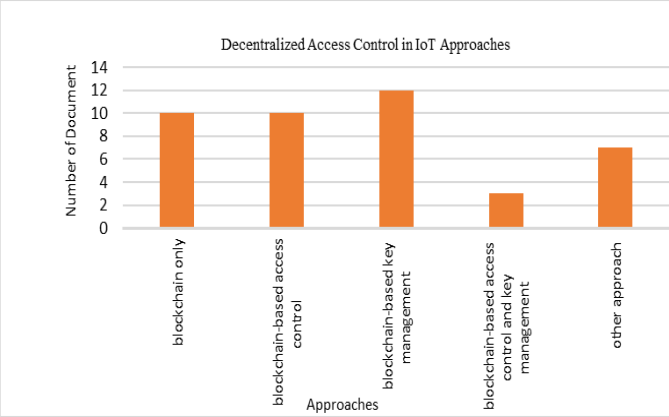

Fig. 3. Type of Decentralized Access Control Approaches in IoTication in IoT for Each Sector.

1) Blockchain technology application in decentralized access control in IoT actuators and sensors: From the literature review, 10 articles were found to have utilised blockchain technology as an approach for decentralized access control in IoT ecosystems. Blockchain is more suitable for decentralized access control due to its immutability and distributed ledgers. It can also handle access control without relying on third parties. Table II presents a summary of blockchain technology employed in decentralized access control including the objectives and techniques used. According to [59], blockchain can be categorised into two groups of access control: 1) global access control and 2) local access control. In global access control, blockchain operates as a distributed ledger and also employs smart contracts to perform global access control tasks including authentication, authorisation, and key management according to the access control policy. Nguyen et al. proposed a framework for establishing a trustworthy access control mechanism on a mobile cloud platform utilising smart contracts [15]. This study applied blockchain to develop decentralized interplanetary file system (IPFS) on a mobile cloud platform by granting access permissions to each individual medical user to access resources in the environment. The authors further employed IPFS smart contracts to strengthen the security of decentralized cloud storage and data sharing control for better user access management. In the industry domain, Xiong et al. proposed a secure and fair coordinated recognition scheme for multiple IoT actuators and sensors using peer-to-peer edge device cooperation [29]. The study further suggested that using smart contracts can be beneficial in the interaction mechanism of trusted nodes by verifying the node. Among the verification mechanisms, the public key is used to authenticate the digital signature for each node in the environment.

In the second group of local access control, the blockchain is utilised as a distributed ledger that stores access control and verification rules, while the local storage maintains authentication and authorisation. Most researchers focus on the local access control which only stores in blockchain server and uses hash techniques to authenticate and authorise the user and device in the IoT ecosystem. The authors in [50,55] and [35] recommended a lightweight authentication by using lightweight cryptographic key to improve security in IoT actuators and sensors, such as the Merkle-Tree, Streebog Lightweight Hashing Algorithm and Hash-locks. Narayanan et al. proposed the Streebog Lightweight Hashing Algorithm hash generation for faster data encryption. The SALSA20 algorithm was also deemed suitable for the IoT environment in [55] since it can minimise the time consumption. The authors in [50] and [60] used the token mechanism as the access control strategy to authenticate each IoT resource and user. Generally, token consists of unique credentials such as addresses, IDs as well as public and private keys. The research claimed that this approach can reduce computational overhead, time costs for blockchain and enhance efficient access control in the IoT environment. The authors further proposed the combination of public and private blockchain for decentralized authorisation in IoT actuators and sensors. It was claimed that the combination approach can reduce the delay of transaction requests and the amount of data the client requires to send to cloud.

2) Blockchain based access control: From the SLR, nine articles were found to adopt an access control model implanted with blockchain technology to provide more fine-grained access control using smart contracts in the IoT ecosystem. Researchers mainly used the distributed attribute-based access control (ABAC) model, capability-based access control (CBAC) model, delegation model, XAML policies and access control list (ACL) model as the proposed approaches for decentralized access control strategy in determining access control of a particular IoT device service through blockchain

and smart contracts. Table III presents the common access control models that were adopted in previous research and their function.

TABLE II. BLOCKCHAIN TECHNOLOGY APPROACH IN DECENTRALIZED ACCESS CONTROL

Authors	Application Objectives	Techniques
[29]	To propose multiple IoT actuators and sensors cooperation driven by secure and fair coordinated recognition scheme using peer-to-peer edge devices	Blockchain, smart contract, YOLO algorithm
[14]	To propose a robust blockchain-based lightweight distributed architecture by leveraging high speed network infrastructure to disburse the computing platform	Blockchain, smart contract, hashing, symmetric encryption, digital signature
[4]	To propose a blockchain based high-efficiency access control framework by leveraging token technology	Blockchain, smart contract, access token, IPFS
[9]	To propose an architecture utilizing blockchain technology in IoT-based environments for healthcare	Blockchain, Hyperledger, chaincode, IPFS
[50]	To propose a blockchain-based authentication mechanism for IoT actuators and sensors	Blockchain, smart contract, Ethereum, token, digital signature algorithm (ECDSA)
[55]	To propose the application of blockchain in enabling secure data sharing among authorised users and devices in the cloud-IoT environment	Blockchain, Streebog lightweight hashing algorithm, SALSA20
[61]	To propose a secure data sharing and access control scheme for users to control the right and privacy of their digital footprint	blockchain, smart contract
[35]	To propose a secure and lightweight Blockchain based IoT authentication scheme	Blockchain, merkle-tree, sequence numbers (SN)
[43]	To propose a novel model for decentralized authorisation by considering limitation of constrained of IoT actuators and sensors	Two blockchain (public and private) Hyperledger, smart contract, Hashed Time-Lock Contracts (HTLCs)
[15]	To propose trustworthy access control mechanism with the application of smart contract on a mobile cloud platform	Blockchain, smart contract, IPFS

TABLE III. ACCESS CONTROL MODEL

Access control model	Functions
ABAC [34]	Attribute-based access control, or ABAC, uses real identities as a set of attributes representing access control policies in a fine-grained method.
RBAC [62]	Role-based Access Control, or RBAC, adopts "roles" as a method to assign permissions. Users are assigned associated role prior to the permission assignment.
ACL	Users of a specific resource will be directly assigned permission in Access control lists (ACLs).

Hossein et al. stored and retrieved data sharing of healthcare records with user-centric and fully distributed architecture of access control, removing trusted third parties in the system [51]. The authors employed different chains of access control policies to ensure that the access policies for the owners of the data are not tampered with, and access to patient data is restricted. The architecture proposes the utilisation of Cluster Head (CH) and Proof-of-Authority (PoA) consensus algorithm to increase the blockchain network throughput and improve system performance and scalability. This approach can reduce the time delay and decrease the number of nodes stored in a single transaction since only miners of each cluster will be kept. However, due to the decreasing number of miners, the risk of malicious activities can increase. In [19], a delegation model approach was employed by adopting blockchain technology for access control in the IoT ecosystem environment setting. The authors proposed an authorisation and delegation model for IoT-cloud based on blockchain technology by deploying smart contracts. The study outcomes indicate that the suggested approach has limitations. The delegation deletion module was not successful since gas requirements exceed the gas limit of the network and further research is required.

Although some limitations do exist, the uniqueness of blockchain technology has attracted technology providers and researchers. One unique feature is the smart contract which can self-execute certain programming conditions and eliminate the need for a trusted entity in the system [63]. Most studies implemented smart contracts to authenticate ownership or to function as a mechanism for controlling token access stored in blockchain. If IoT actuators and sensors are successfully authenticated and validated, devices can access the entire system based on pre-determined access level. Technically, when all authentications are automatically triggered by smart contracts, credibility and impartiality of authentication are theoretically guaranteed. For instance, [64] proposed a trust-based access control framework for decentralized IoT network by applying smart contract to enable decentralization. The authors deployed the ABAC mechanism to manage and limit resources accessed by any party under decided conditions based on the access policy that was set with pre-determined attributes. Access policy enforce smart contracts by assessing the incoming authorisation request to access resources based on context. The context was pre-set with the rulesets according to the specific Boolean attribute in the access policy. Successful authorisation will be followed by a process in generating an access token by smart

contracts. The token can be used to access the resources without repeating the authorisation process for the next access multiple times. This approach provides scalability and at the same time acting as a defender towards Sybil attacks and newcomer attacks that apply attribute registration mechanism way of attack. A similar approach was adopted in [17] by implementing smart contract that functioned as a smart policy to the access control policy. During the execution, a smart policy is created by the resource owner and stored on a blockchain after a proper transaction being transacted.

Meanwhile, in [65], blockchain and decentralized identifier (DID) techniques were used to manage identity and access control for IoT device authentication. This paper deliberated that, based on the proposed mechanism that the capability tokens play a vital component when a particular IoT device service is requesting to obtain the authorisation, the device owner must claim their ownership via the ownership management module to obtain authorisation using the capability token. This approach was determined as lightweight due to three smart contracts applied within the core components: DID registry, device ownership credential registry and device capability credential registry. However, related services need to be present to invoke the functions of these contracts. On the other hand, the work in [66] presented a mechanism where two entities were introduced to handle the delegation process which are labelled as delegator and the delegatee. The entity that executes the role in transferring the access right is called the delegator. The delegator plays a role as the entity that will perform the transfer of the access right, while delegate play a role as the receiving entity. The proposed approach commonly deploys delegation through smart contracts to eliminate the need for a central, trusted, third-party authority. Table IV presents a summary of access control models that adopt blockchain technology in decentralized access control, including the objectives and techniques used are discussed.

3) Blockchain-based key management for decentralized access control: From the SLR, 13 articles were found to use the distributed key management in the effort to strengthen IoT access control by applying blockchain to resolve privacy and security issues. Table V presents a summary of blockchain-based key management approaches including the objectives and techniques used for decentralized access control. The combination of distributed key management and blockchain technology is to provide secure authentication and trust communication between device/node in the network layer. The authors in [28] claimed that the use of public key infrastructure (PKI) has vulnerabilities, such as high computational complexity, and requires intermediate certificate authority (CA) to accomplish certificate verification key. Thus, the authors proposed key management in blockchain operated by security access managers (SAMs). SAM plays a crucial role as CA, which is responsible for storing and verifying entire blockchain transactions. Based on SLR, the researchers suggested the adoption of various types of cryptography algorithm techniques including digital signature, endow key trust, symmetric encryption algorithm, session key, Elliptic Curve Cryptography (ECC), Aggregate signature scheme, Broadcast Encryption (BE) and Multi-Receivers Encryption (MRE) embedded with blockchain. These techniques aim to enhance the access control required for verifying the identity of resources by authenticating and authorising the IoT device and user before entering the system or communicating with other entities in the decentralized nature. For instance, Hammi et al. utilised a bubble of trust in the blockchain environment to provide secure communication to each trusted member device [46]. In this approach, two types of bubbles are present: the master bubble which acts as a certification authority, and the follower bubbles. To authenticate these bubbles, the authors used ECC to generate private/public key-pair since it is known as a lightweight key and is suitable for restricted devices. Smart contract is also applied to verify the uniqueness of the follower's identifier, checking the validity of the follower's ticket using the public key of the master bubble. If one condition is not satisfied, the object cannot be associated to the bubble. If successfully authenticated, the tickets are no longer needed to register new identification and make ACL for users in the system. Shi et al. proposed a blockchain-based access control scheme for privacy preserving in distributed IoT, which formalizes the distributed architecture in IoT and the traditional centralized access control model [25]. The authors utilised domain management server (DMS) to define information and permission of data on blockchain. They used the key-pair of DMS to sign and encrypt data permission on blockchain and employed the symmetric encryption algorithm to encrypt data. Although the data on blockchain is transparent to all nodes, it still reasonably protects the user's privacy.

4) Blockchain-based access control model and key management: Based on SLR, 3 articles were found to use distributed key management and access control model that adopted blockchain technology. Various access control models were proposed as access control strategies: RBAC, ABAC, Attribute-Based Signatures (ABS), Anonymous Attribute-Based Encryption (ABE) and Outsourced Attribute-Based Signature (OABS). Double authentication preventing signature (DAPS), Aggregate Signature Scheme, Endow Key Trust, Symmetric Encryption Algorithm and Digital Signature act as the key management for authenticating IoT actuators and sensors. Both techniques were applied together with blockchain technology for enhancing decentralized access control to secure IoT resources as well as improve security and privacy issues in the IoT ecosystem. This combination technique further increased scalability and feasibility of the proposed solution compared to existing solutions.

TABLE IV. BLOCKCHAIN-BASED ACCESS CONTROL APPROACH IN DECENTRALIZED ACCESS CONTROL

Authors	Objective	Detailed Techniques
[22]	To propose a blockchain technology combined with Zero knowledge Token-Based Access Control (BZBAC)	Blockchain, Ethereum, smart contracts, off-chain computation, on-chain, Zero knowledge Token-Based Access Control model
[64]	Trust-based access control framework was developed to support the implementation of decentralized IoT network with smart contracts as the main component	Blockchain, ABAC, smart contract, Trust and Reputation System (TRS)
[51]	To propose a novel access control architecture based on blockchain for storing and retrieving healthcare records	Blockchain, access control policy, cluster head (CH), proof-of-authority (POA) consensus algorithm
[31]	To propose a blockchain-based access control system by embedding ABAC and smart contract on the Hyperledger fabric platform	Blockchain, ABAC policy, smart contracts, Hyperledger fabric
[19]	To propose authentication and delegation mechanisms by using smart contracts and the Stack4Things framework. The mechanism is to support the migration to the decentralized environments	Blockchain, delegation mechanism, RBAC, smart contracts, universally unique identifier (UUID)
[39].	To propose "PrivySharing," a framework developed based on blockchain aimed to provide secure and privacy-preserving data sharing	Blockchain, smart contracts, ACL rules
[38]	To propose a framework for access control embedded with blockchain technology to enhance privacy policy dedicated for Decentralized Online Social Networks (DOSN)s.	Blockchain, smart contract, ACL rules
[65]	To propose a decentralized capability for IoT access control by implementing blockchain technology with smart contract as the core component	Blockchain, smart contracts, capability based IoT access control, Decentralized Identifier (DiD)
[17]	To present an implementation reference of manipulating XACML policies in a case where Solidity language was used to write a smart contract and deployed on Ethereum platform	Blockchain, smart contracts, XAML policies

Lei et al. proposed a blockchain-based security architecture for improving security and privacy of named data networking (NDN)-based vehicular edge computing (VEC) network. The ABAC mechanism was adjusted into the decentralized architecture; therefore, access control decisions do not have to rely on a centralized policy decision point. The proposed ABAC applies a set of attributes to represent the resource and the subject requesting the resource [34]. This work also suggested a blockchain-based solution that uses the endow key trust instead of the root key for verifying the authenticity of the key across the user trust domain. Other than that, the symmetric encryption algorithm is also applied to encrypt the content with a symmetric data key and used in access control by controlling the distribution of data key that can only be obtained by an authorised user. Kamboj et al. proposed the RBAC model using blockchain to assign a role in the organisation and management of interactions between users and resources [11]. The role checks and verifies credentials of roles by using smart contracts and digital signature algorithm for signing the transaction and for the generation of public and private keys. Table VI presents a summary of blockchain-based access control and key management approaches, including the objectives and techniques used for decentralized access control.

TABLE V. BLOCKCHAIN-BASED KEY MANAGEMENT APPROACH IN DECENTRALIZED ACCESS CONTROL

Author	Techniques
[40]	Access Control Header (ACH), Cryptographic, multi-layer BC, smart access control
[53]	Blockchain, identity-based signature, hash function, Verifier Control Centre (VCC), Certification Authority (CA)
[25]	Blockchain, symmetric encryption algorithm (SEA), Asymmetric Encryption Scheme (shared key), Management Server (DMS) (Storage)
[44]	blockchain, smart contracts, hybrid cryptosystem with lightweight cryptographic functions (Key Generation Centre (KGC), AES, ECDSA and One-Way Hash Function), angular distance (AD)
[7]	Blockchain, Elliptic Curve Digital Signature Algorithm (ECDSA), Algorithm (Public Key & Private Key), Smart Contract
[48]	blockchain, smart contracts, Elliptic Curve Cryptography (ECC)
[18]	Blockchain, Elliptic curve digital signature algorithm (ECDSA), one-way hash function, session key
[57]	Blockchain, Ethereum, smart contracts, Distributed, Self-Sovereign Identity, fog device authentication mechanism
[33]	Blockchain, cryptographic algorithm- public key, private key and secret key
[42]	Blockchain, Diffie–Hellman, public/private key pair, Session key, Trust Network Framework (TNC), ECDSA
[28]	Blockchain, smart contract, key management schemes, security access managers (SAMs)
[37]	Smart contracts, blockchain broadcast encryption (BE), certificateless multi-receivers encryption (CL-MRE) and Permission Data Hash Table (PDHT)
[46]	blockchain, smart contracts, Public Key Infrastructure (PKI), bubble trust (secure virtual zones), Elliptic Curve Digital Signature Algorithm (ECDSA), ticket

TABLE VI. BLOCKCHAIN-BASED ACCESS CONTROL MODEL AND KEY MANAGEMENT APPROACH IN DECENTRALIZED ACCESS CONTROL

Author	Objective	Detailed Techniques
[11]	Developing a role-based access control method using blockchain technology to manage user-role in the organisation	Blockchain, Ethereum smart contract, RBAC, public key infrastructures (PKIs), elliptic curve digital signature algorithm (ECDSA), digital signature, Keccak-256 cryptographic hash function
[34]	Developing novel security architecture using blockchain technology concept for application in NDN-based VEC networks to address security and privacy challenges	Blockchain, delegate consensus algorithm, access policy key management mechanism (endow key trust, symmetric encryption algorithm), ABAC
[49]	Privacy preserving IoT software update protocol by applying blockchain technology	Blockchain, smart contracts, double authentication preventing signature (DAPS), outsourced attribute-based signature (OABS)

5) Blockchain with other approaches: Based on SLR, seven articles were found to employ different approaches to the proposed decentralized access control in the IoT ecosystem. The approaches include Transitive Access Checking and Enforcement (TACE) mechanism which adopts blockchain, blockchain-based access control model, physical unclonable function (PUF), blockchain-based game theory and blockchain-based cross chain technology. Only two articles did not include blockchain adoption. Table VII presents a summary of blockchain combined with other approaches, including the objectives and techniques used for decentralized access control.

TABLE VII. BLOCKCHAIN COMBINED WITH OTHER TECHNIQUES IN DECENTRALIZED ACCESS CONTROL

Author	Detailed Techniques
[47]	Blockchain, smart contracts, Role-Based Access Control, hybrid PUF
[20]	Blockchain, evolutionary combination rule (ECR), smart contracts, game theory
[45]	Blockchain, PUF, smart contracts, Diffie-Hellman key, Chinese Remainder Theorem (CRT), Hash Function
[54]	Blockchain (main chain-consortium), byzantine fault tolerance (RIBFT) algorithm, smart contracts, cross chain technology
[21]	Tangle (store policies), ABAC policy, Decision Point (PDP)
[67]	Blockchain, TACE, Cross-Domain Access Control
[36]	MAM, Tangle, One-Time Signatures (OTS), Merkle Signature Schemes (MSS)

From this review, 39 articles were found to utilise blockchain technology for decentralized access control in IoT ecosystems. Only two articles used IOTA technology similar to blockchain technology. Most research used the ownership concept in the access control model. From SLR extraction, noticed that access control deploys smart contracts to create ownership of resources. The owner will register itself and its resources into smart contracts. After successful registration, smart contracts will generate the credential/token to authenticate the resource owner. The owner can access their resources any time using the credential/token. The deployment of smart contract occurs when two parties agree to the agreement made through coding and can then execute in an autonomous manner. Smart contract is built based on the role or attributes assigned by the authorizing admin who enrolled the smart contract. After deploying smart contract, the user/owner can use their credentials to access the entire network with permission. In a smart contract, several functions are present to operate based on the needs of a contract. Researchers used function add, update, delete and remove to operate in smart contracts. However, the negotiation process for the terms and conditions of smart contracts is unclear.

Access policy is also employed in smart contracts for access control in the IoT ecosystem by creating different levels of user authorisations to access resources. This access policy will be stored in the blockchain server to make it easier for users to invoke their access policy. Authentication and authorisation are also needed in access control for the IoT network. Several techniques that can be used to authenticate and authorise, such as BE, CL-MRE, PDHT, ECDSA and ECC. According SLR, the researchers used public key, private key and secret key to encrypt data for submitting or exchanging data to trusted entities in the IoT network. Several research also used key management to secure communication between device to device (D2D) and device to IoT network. As a result, it is guarded from malicious attacks such as eavesdropping, DDOS and hijacking. From all mentioned techniques, smart contract, authentication & authorisation and key management are the vital components in enhancing the decentralized access control in the IoT ecosystem. However, some techniques are not suitable due to the time delay of transactions and increased overhead. Thus, the trade-off between the techniques and transactions performance must be researched to find the optimum level. Table VIII presents the output of techniques used.

TABLE VIII. OUTPUT OF TECHNIQUES USED IN EXISTING SOLUTION

Author	Techniques	Output
[29]	Blockchain + smart contract	Better fairness and robustness Increased start-up delay
[11]	Ethereum blockchain + new RBAC + PKI + ECDSA	Less execution cost Less running time compared to the RBAC-SC
[47]	Blockchain + access control model + PUF	Cost-effective device in authentication Scalability Computational efficiency of IoT device
[61]	Blockchain + smart contract	Increased feasibility and effectiveness
[4]	Blockchain + smart contract + access token + IPFS	Secure and has low gas cost
[9]	Blockchain + Hyperledger + chaincode + IPFS.	Reduced mining costs and increased throughput
[50]	Blockchain + smart contract ECDSA	More effective in communication overhead compared to previous approach Less time for communication between IoT actuators and sensors with blockchain
[55]	Blockchain, Streebog Lightweight Hashing Algorithm, SALSA20	Better performance Suitable for a large-scale environment Lower time consumption due to spark environment High-level security
[18]	Blockchain + ECDSA + One-way hash function + session key	Low communication cost and access control phases than all existing schemes More computation time than some existing schemes
[20]	Blockchain + game theory	Compared to the environment without the protection shows effectiveness in latency overhead
[33]	Blockchain + public key, private key, secret key	Lower computation cost
[34]	Blockchain + delegate consensus algorithm + key management mechanism + ABAC	NDN: higher throughput in network architecture Time delay: increases total time to verify a transaction signature Increased overhead: encryption and decryption
[42]	Blockchain + public/private key pair + session key + TNC	Longer time to invoke smart contracts Provide stronger mechanism for verification of IoT actuators and sensors that adopt blockchain technology
[43]	Two blockchain (public and private) + Hyperledger + smart contract + HTLC	Decreased overall transaction delay
[15]	Blockchain, smart contract, IPFS	Flexibility in different platforms Availability of data in dynamic real time Decentralized IPFS to solve the single point of failure
[46]	Blockchain + PKI + bubble trust + ECDSA	Less energy and computation consumption
[36]	IOTA + MAM	Less time delay
[37]	Blockchain + BE + CL-MRE + PDHT	Smart contracts increased time cost

IV. EXISTING FRAMEWORKS FOR DECENTRALIZED ACCESS CONTROL USING BLOCKCHAIN

Developments in the field of decentralized access control in the IoT ecosystem have attracted various research efforts, resulting in several framework developments based on various objectives and goals. By taking into consideration that authentication and access control are important security aspects, especially with the increase in devices that generate content, various access control solutions have been proposed throughout the literature. In this SLR, found nine existing frameworks for decentralized access control in the IoT ecosystem. The findings are classified into three groups based on framework objectives. Table IX shows the objective regarding existing frameworks.

From the extraction of this SLR, four frameworks were found to develop an access control that focuses on communication control between various entities such as IoT device, gateway, cloud and users [4], [68], [69], [47]. To accomplish the objective of the proposed framework, researchers have adopted blockchain technology to design control communication between various entities by validating data flows before attempting to communicate with other entities. With the capability of blockchain in enhancing reliable communication between entities by utilising it distributed ledger with the hashing function and smart contracts, the authors in [69] designed intra-blockchain interactions within smart contracts. The authors also designed inter-blockchain communication from one node to other nodes and resources in the IoT network. The development of the framework was inspired by the microservice architecture that was build based on 3 proportions: right side, top right side and top left. The core part of this framework is the top right side which utilises 3 smart contracts for IoT systems. The 3 smart contracts have two functionalities: 1) contract level of communication between IoT actuators and sensors, and 2) contract to access data-sources and 3) interoperability of heterogeneous IoT smart contracts. In another approach, the authors in [4] developed access control in various entities and communication control frameworks for cloud-enabled IoT. This framework has three layers: the register model layer, blockchain-based token requesting mechanism layer and requesting data with token used to control the access of users in the system's layers. The authors also deployed pre-defined smart access policies to register resources by the upload mechanism using unique ID. After successful registration, the user must request a token for verifying authority and accessing resources.

In this SLR, two frameworks that focused on authentication and authorisation of user and device, as discussed in [24] and [28] was found. Ma et al. proposed a lightweight, scalable and adaptive key management scheme for the IoT system [28]. In this work, the authors deployed a key management mechanism performed in SAM. The mechanism that was proposed was utilised to record and verify transactions and administrating the key management information. The reason behind the proposed mechanisms is to enable a low-latency key management function for user equipment in the same deployment domain.

Several studies have discussed the constraints regarding devices installed in IoT applications, posing challenges in terms of reliability, cost delay and security. In this SLR, three frameworks that focused on security and privacy enhancements in IoT [70], [71], [72] were found. In the framework proposed in [71], the authors suggested a datagram transport-layer security (DTLS) protocol. The framework was designed with the aim to ensure secure communication that can be realized between three layers: the 1) data producer layer, 2) hybrid computing paradigm layer and 3) data consumer layer. To further strengthen the proposed framework, the authors also included three cryptography mechanisms in the form of algorithms to give higher protection towards system level privacy and security. The proposed combination of blockchain technology and DDSS framework was tested in the decentralized transparent healthcare management system. This framework can be utilised in the application of healthcare domain using a public ledger for each medical record and critical event to provide traceability as well. In addition, in this study, smart contracts usage was applied in automating event-based activities without medical professionals' interference. Meanwhile, in the framework discussed in [73], blockchain technology proposed to be applied in a data-sharing model for intelligent community by utilising the centralized model for access control. The model presented in three modules. In the first module, user authentication and identity management are addressed using enhancement multi-factor authentication model which relies on trusted third parties to manage user authentication. The authors chose not to use blockchain technology in their user authentication module so as to shorten the authentication process and preserve the system's security. However, this approach may lead to various problems in future due to the nature of centralized management. Thus, the gap must be addressed in future work to provide the improvement.

From the literature review analysis, from the observation that the proposed frameworks can be divided into three to five layers based on the physical layer, network layer and application layer concepts. These layers consist of several services and applications in different levels. The first layer is the physical layer, also known as the sensing layer. This layer consists of the IoT device and sensors responsible for collecting and processing data to send to the second layer. Before the IoT actuators and sensors being allowed to enter the network and raw data is transmitted, the access control mechanism will be the first line of defence that guarantee that only eligible actuators and devices will be allowed to access. After the devices clear the access control, then, lightweight key management approach is used to encrypt raw data. The second layer consists of gateway or network paths that are required to transmit IoT data. Any device or user that enters the network must be authorised. Some approaches use simple cryptographic, such as public key, to authorise. Other designs are based on PUF as the key generated for uniquely authenticating IoT actuators and sensors. The third layer is the blockchain layer which performs the transaction validation. This layer uses smart contracts as a core layer that only performs on legitimate devices for accessing resources in the system. Other researchers used a fourth layer as an application layer which can be executed on cloud or local environments. This layer allows users to access resources by using the internet. To obtain authorisation, users require a valid token or credentials to gain network access.

TABLE IX. BLOCKCHAIN COMBINED WITH OTHER TECHNIQUES IN DECENTRALIZED ACCESS CONTROL

Author	Objectives of the Proposed Framework
[4]	To develop access control in various entities and communication control frameworks for cloud-enabled IoT in terms of data flow from one end to another in CE-IoT services/applications
[47]	To secure data communication and sharing in IoT networks using generated cryptographic keys by providing authenticated device using PUFs and blockchain technology
[71]	To improve the system's security capabilities in classic cloud-centric blockchain-based H-CPS
[70]	To secure and create tamper-resistant massive IoT transactions by improving scalability and the performance of massive IoT networks by utilising blockchain-based secure micro-services in Virtualised Network Functions
[68]	To generate reliable communication IoT eco-systems with reliable information integration between users by validating nodes based on inter-operable structures
[72]	To improve the transaction delay among IoT applications by using blockchain based in SDN architecture
[15]	To allow authorised entities (such as healthcare providers) to effectively retrieve EHRs on cloud, while preventing unauthorised access to EHRs resources
[24]	To enable secure and transparent collaborations for connected IoT actuators and sensors trust-based automation to recognise, authenticate and access control of devices in the perception layer
[28]	To achieve a lightweight, scalable, adaptive key management scheme and authorisation assignment mode by verifying the access query transaction based on logical topology in the IoT system
[69]	To enhance access control traditional development model with features that primarily support intra-blockchain interactions within smart contracts as well as enable inter-blockchain communication to other nodes and resources in the IoT network

V. EVALUATION FOR DECENTRALIZED ACCESS CONTROL USING BLOCKCHAIN

How the evaluation was done to determine the effectiveness of methods/techniques/approaches in previous studies, is addressed in RQ3. Each reviewed study had been evaluated based on their proposed techniques, approaches and frameworks as the baseline for future investigations. This evaluation was accomplished during the experimental phase. Validation was conducted using pre-determined parameters and by comparing existing baseline models. These parameters and models have been used by numerous research works that reported satisfactory results and were then later examined and enhanced by others. To answer RQ3, this section lists the

datasets, parameters and tools (hardware/software) used to evaluate the performance of the proposed approach.

A. Dataset for Evaluation

For every proposal deliberated in the literature, experiments were done to validate the proposals. For the validation, most datasets used in access control experiments generated by nodes. Most nodes are used in the research to simulate the experiment scenario [7,15,31,44,51]. Data were generated by IoT actuators and sensors, such as raspberry pi system [7] sensors, collected from laptops and mobile phones to form a dataset. In [71] and [74], available datasets or open data are employed to conduct experiments. For instance, Guruprakash & Koppu used Kaggle which contains temperature readings from IoT actuators and sensors installed inside and outside anonymous buildings [74]. This dataset was analysed to validate the proposed system functionalities and capabilities [74].

B. Parameters for Performance Evaluation

Based on the literature, experiments have been accomplished to evaluate the different performances of the proposed approaches according to various parameters. The parameters frequently depend on the objective of the study and the goal of the experiments. The evaluation in blockchain technology can be categorised into two groups based on the evaluation goals, as follows:

1) Parameter based on performance of blockchain technology: The evaluation of blockchain performance metrics and parameters consist of transaction throughput, transaction latency, network latency, block size, computational cost, block validation, storage overhead, transaction delay and time delay [7], [9], [51], [15,25,54], [74], [75], [76]. Network latency is the total time taken for a transaction to be executed in the blockchain network. To evaluate these parameters, Table X displays the measuring units based on the parameters used: milliseconds (ms), second (s), minutes (m), joules (j), ethers, bytes, transaction (Tx), transaction per second (TPS), transaction per minutes (TPM). Based on the study of [15], the time taken is usually higher when the mechanism involved with user authentication is based on smart contracts that consume more time to process user requests, as compared to the non-authenticated scheme. The computation cost based on the time of deploying and invoking a smart contract increases [52]. The storage cost is normally based on the size of the stored data [74]. Transaction throughput is defined as the number of validated transactions per second. According to Zaabar et al., the throughput is separated into two sub-categories: the read throughput and the transaction throughput [9]. The read throughput is defined as the total number of reading operations performed across the blockchain network within the given timeslot, while the transaction throughput is the number of successful transactions performed in the blockchain network within the given timeslot.

2) Parameter based on performance of access control in blockchain technology: The evaluation of the performance access control in blockchain were proposed by allowing authorised entities to effectively retrieve the database and prevent unauthorised access from resources. To verify and authenticate the authorised transactions and un-authenticate unauthorised transactions, several existing solutions consisting of many operations must be accomplished. The authors in [44] highlighted that to execute these operations, the system may consume more energy. For the evaluation of the authentication process, researchers utilised parameters such as energy consumption [44], time taken for encryption and time taken for decryption [52]. To evaluate energy consumption, researchers chose parameters such as cost, time (ms) and energy (j). Regarding the time taken for encryption and decryption, [55] defined the encryption time as the amount of time consumed to convert plaintext into ciphertext, which generally depends on data size and the key size used for encryption. The decryption time was defined as the amount of time taken by the algorithm to convert ciphertext into original data. Storage and communication costs are also parameters in access control. The measuring unit of both parameters is bytes [44].

TABLE X. PARAMETERS AND VARIABLES

Parameter	Variables (unit)
Access Control	
Energy consumption [44]	Cost, time (ms), energy (j)
Time taken for encryption and decryption [55]	Time(ms), data size (bytes)
Storage cost [44]	Cost, size of data key (bytes)
Communication cost [44]	Cost, size of data key (bytes)
Blockchain	
Transaction throughput [77]	Response time (m) and TPM (size of transaction)
Transaction latency	Time (ms) and invoking a transaction (Tx)
Network latency [78],[15]	Time (ms),
Block validation [74]	Processing time (s), number of blocks
Computational cost[79]	Time (s), cost, ethers
Storage overhead [44],[80]	Size of key (bytes), time(s)

3) Tools for evaluation: This section provides an overview of the technologies and tools adapted by the articles reviewed in this study. Researchers implemented their proposed solutions by setting up the experimental environment to serve as the underlying functions as well as to efficiently evaluate the proposed solutions or mechanisms and frameworks. The details of the setups are divided into two categories, as follows:

a) Hardware: From the extensive review of the selected literature, the commonly used hardware for conducting experiments included desktop pc, laptop, mobile phone, raspberry pi, memory and hard disk. The researchers mainly used large storage and equipment that are compatible with their experiments. The desktop pc and laptops were commonly

employed as the simulation platform and blockchain server to run the experiments. Memory ranging from 8 to 16 GB RAM [44] are necessary [81][34]. Raspberry pi can be used as lightweight IoT actuators and sensors, further acting as IoT nodes. The interaction between IoT nodes were developed using C++ language and the JsonRPC library for communication [7].

b) Software: Most studies, as in [59] and [75], chose a private blockchain (such as Ethereum) to develop their blockchain network and conduct experiments. Based on [50], Ethereum is the commonly used platform for building decentralized apps (dApps). It provides a secure way to perform transactions using the elliptic curves cryptography protocol. Ganache is also used to test the decentralized application without an actual set-up of the Ethereum network. Ganache is defined as a blockchain emulator, also known as a personal Ethereum client or node [7]. Several studies have deployed a blockchain network built on Hyperledger fabric to execute experiments, such as in [9,54]. Node.js is also used as an Ethereum network [81]. Many studies further developed an experiment in the virtual environment to build a blockchain network that can be deployed in Ethereum Virtual Machine (EVM), such as in [64]. Some researchers applied a simulator or emulator environment to conduct their experiments. A simulator, such as OMNeT++ [28], can create an environment similar to the original which can configure real devices. An emulator, such as Common Open Research Emulator (CORE) [72], can be used to duplicate all hardware and software features in real devices.

In terms of the programming language, most studies used the python language to create a prototype interface since it is considered to be a dynamic and scalable language across multiple platforms [50]. Web3.py library is frequently employed to enable users to interact with Ethereum clients and request functions written in smart contracts. Solidity programming language is also applied to write smart contracts [7], [10], [27], [62]. These smart contracts were implemented for testing, debugging and then deployment, either in Ethereum Virtual Machine (EVM) [11], Truffle [7], Testnet [62] or Remix IDE [56], before implementing them in the blockchain platform. Ropsten [11,55], Rinkebey and Koven are Ethereum tools for testing and development purposes. Researchers have noted that benchmarking is important to measure the performance of the blockchain application [9]. The most commonly used benchmarking for the Hyperledger network is Hyperledger Caliper. The use of several appropriate protocols play a crucial role in an experiment. Common communication protocols used are IPV6 and 6LoWPAN [53].

VI. Conclusions and Future Works

IoT actuators and sensors are capable to further improve the efficiency of smart farming. However, the security of the IoT actuators and sensors depending on the access control that act as the first line of defence via authentication and authorization. This paper presented the background of decentralized access control in this study. Based on extensive literature review, most commonly applied techniques to authenticate and authorise users or devices in IoT networks are summarized as key management schemes including the asymmetric cryptographic algorithm, the symmetric cryptographic algorithm, session key, secret key, PKI (including hashing algorithms), Symmetric Encryption, Digital Signature, Elliptic Curve Cryptography (ECC) and Elliptic Curve Digital Signature Algorithm (ECDSA) based on blockchain technology. This approach is vital for securing access control and communication between D2D, user to device and device to network.

Meanwhile, the access control models - RBAC and ABAC, are frequently used to assign a user to a role in the system according to their attribute, credentials or authority to access resources. This approach can be commonly utilised as a strategy for designing various smart contracts for fine grained access control. In the smart contract operation, all information associated with a particular role or attribute will be stored on blockchain. This makes it more transparent and available for other users to access resources with the owner's permission. By deploying the access control strategy in blockchain in the form of smart contracts, the computation overhead of IoT actuators and sensors will be reduced, therefore, the framework can apply lightweight IoT actuators and sensors existed ecosystem.

Based on reviewed articles in this SLR study; tokens were incorporated into the strategy for subjects to obtain access rights by applying the token which can improve access efficiency. Other techniques are also used to make the system more scalable. Researchers commonly use off chain and on chain with other storages called IPFS. The assessment of all proposed techniques was accomplished by establishing the necessary steps to setup the evaluation. The literatures also reported that most research have developed an experimental environment on the Ethereum platform. Some experiments were executed in the virtual environment due to the requirements and needs for large storage and high CPU or laptop processors. The CPU or laptops are used as the main components in an experiment to simulate the blockchain server, or act as a gateway to collect data from IoT actuators and sensors. The core of the development system is smart contracts, which are developed using Solidity programming language. Regarding experiments, datasets were collected using IoT actuators and sensors according to pre-defined parameters for specific experiment designs. Evaluation was then performed to examine the proposed system based on established parameters. The parameters were also used as a baseline comparison with other relevant works and for validating the proposed system.

Among the gaps identified in the current access control data in the IoT ecosystem are: lack of mechanism and standardised protocol of access control and communication protocol, decentralized access control, authentication, privacy and security. From the finding that the mechanism in authorisation and authentication is not fully adapted in a decentralized manner. It remains in the same phase and requires a trusted entity in the validation process. Based on this study, most of the proposed solutions which influence decentralized access control in the IoT ecosystem include a lightweight distributed key management solution, a robust

design in smart contracts, efficient consensus approach and decentralized access control.

This study concludes that the decentralized access control is a relevant topic for researchers to explore and investigate. The combination of access control approaches that adopt blockchain technology can be a possible mechanism for enhancing decentralized access control in the IoT ecosystem. In addition, the access policy based on ABAC and RBAC model can be used to achieve flexibility and dynamic access control using smart contracts. Smart contracts can be used as an automation decision and authorization to eliminate centralized server into decentralized server. The use of multiple layers also plays a crucial role in reducing the scalability of IoT systems, speeding up the process of requesting transactions and reducing time delays. Thus, it is suitable for application in large scale IoT systems that manage big data processing.

Smart farming also relies on the IoT technology and smart systems to collect real-time data and provide observations in management operations on the farm, including pre- and post-harvest. For optimum access control decentralization in smart farming, Ethereum platform that include public and private blockchains can be utilised.

For future studies, in regard to the application of decentralized access control in smart farming, researchers should explore and investigate the enhancement of smart contracts design for access control since smart contracts play a vital role in blockchain. They were designed with the aim to perform event-based automation activities without human interference based on pre-defined contracts. Nevertheless, smart contracts can be the loophole for blockchain technology, which is another gap that must be addressed to further enhance decentralized access control in IoT, especially for the application in smart farming. Thus, the design and mechanism for applying the smart contracts concept in blockchain technology must be further examined to achieve an optimum design. This can be validated through simulations until the establishment of contracts is complete. This is crucial to further secure and strengthen a resource from unwanted threats, including smart contract-related scams and illegal activities.

ACKNOWLEDGMENT

The authors would like to acknowledge National Defence University of Malaysia (UPNM) and Ministry of Higher Education Malaysia (MOHE) for the approved fund which makes this research viable and effective. This research is supported by Fundamental Research Grant FRGS/1/2021/ICT07/UPNM/02/1.

REFERENCES

[1] Mat Lazim R, Mat Nawi N, Masroon M H, Abdullah N and Che Mohammad Iskandar M 2020 Adoption of IR4.0 into Agricultural Sector in Malaysia: Potential and Challenges Adv. Agric. Food Res. J. 1 1–14.

[2] Triantafyllou A, Tsouros D C, Sarigiannidis P and Bibi S 2019 An architecture model for smart farming Proc. - 15th Annu. Int. Conf. Distrib. Comput. Sens. Syst. DCOSS 2019 385–92.

[3] Marinchenko T 2020 Digitalization Of Agricultural Sector: Outlook In Russia.

[4] Chai B, Yan B, Yu J and Wang G 2021 BHE-AC: a blockchain-based high-efficiency access control framework for Internet of Things Pers. Ubiquitous Comput.

[5] Matrazali N, Noor N, Hasbullah N, Chen L, Ishak K and Nordin N 2021 A Conceptual Model: Securing Resources Through a Decentralized Access Control Using Blockchain Technology for Smart Farming pp 399–410.

[6] Hou J, Qu L and Shi W 2019 A survey on internet of things security from data perspectives Comput. Networks 148 295–306.

[7] Khalid U, Asim M, Baker T, Hung P C K, Tariq M A and Rafferty L 2020 A decentralized lightweight blockchain-based authentication mechanism for IoT systems Cluster Comput. 23 2067–87.

[8] Razali N A M, Malizan N A, Hasbullah N A, Wook M, Zainuddin N M, Ishak K K, Ramli S and Sukardi S 2021 Opinion mining for national security: techniques, domain applications, challenges and research opportunities J. Big Data 8 150.

[9] Zaabar B, Cheikhrouhou O, Jamil F, Ammi M and Abid M 2021 HealthBlock : A secure blockchain-based healthcare data management system Comput. Networks 200 108500.

[10] Zhang Y, He D and Choo K K R 2018 BaDS: Blockchain-based architecture for data sharing with ABS and CP-ABE in IoT Wirel. Commun. Mob. Comput. 2018.

[11] Kamboj P, Khare S and Pal S 2021 User authentication using Blockchain based smart contract in role-based access control Peer-to-Peer Netw. Appl. 14 2961–76.

[12] Rabehaja T, Pal S and Hitchens M 2019 Design and implementation of a secure and flexible access-right delegation for resource constrained environments Futur. Gener. Comput. Syst. 99 593–608.

[13] Bhatt S and Sandhu R 2020 ABAC-CC: Attribute-based access control and communication control for internet of things Proc. ACM Symp. Access Control Model. Technol. SACMAT 203–12.

[14] Deebak B D and AL-Turjman F 2022 A robust and distributed architecture for 5G-enabled networks in the smart blockchain era Comput. Commun. 181 293–308.

[15] Nguyen D C, Pathirana P N, Ding M and Seneviratne A 2019 Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems IEEE Access 7 66792–806.

[16] Liu Y, Lu Q, Chen S, Qu Q, O'Connor H, Raymond Choo K K and Zhang H 2020 Capability-based IoT access control using blockchain Digit. Commun. Networks 7 463–9.

[17] Di Francesco Maesa D, Mori P and Ricci L 2019 A blockchain based approach for the definition of auditable Access Control systems Comput. Secur. 84 93–119.

[18] Bera B, Chattaraj D and Kumar A 2020 Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment ☆ Comput. Commun. 153 229–49.

[19] Tapas N, Longo F, Merlino G and Puliafito A 2020 Experimenting with smart contracts for access control and delegation in IoT Futur. Gener. Comput. Syst. 111 324–38.

[20] Esposito C, Tamburis O, Su X and Choi C 2020 Robust Decentralised Trust Management for the Internet of Things by Using Game Theory Inf. Process. Manag. 57 102308.

[21] Shafeeq S, Alam M and Khan A 2019 Privacy aware decentralized access control system Futur. Gener. Comput. Syst. 101 420–33.

[22] Song L, Ju X, Zhu Z and Li M 2021 An access control model for the Internet of Things based on zero-knowledge token and blockchain Eurasip J. Wirel. Commun. Netw. 2021.

[23] Pal S, Rabehaja T, Hitchens M, Varadharajan V, Member S and Hill A 2019 On the Design of a Flexible Delegation Model for the Internet of Things Using Blockchain IEEE Trans. Ind. Informatics PP 1.

[24] Tang B, Kang H, Fan J, Li Q and Sandhu R 2019 IoT passport: A blockchain-based trust framework for collaborative internet-of-things Proc. ACM Symp. Access Control Model. Technol. SACMAT 83–92.

[25] Shi N, Tan L, Yang C, He C, Xu J, Lu Y and Xu H 2021 BacS: A blockchain-based access control scheme in distributed internet of things Peer-to-Peer Netw. Appl. 14 2585–99.

[26] Elahi M M, Rahman M M and Islam M M 2022 An efficient authentication scheme for secured service provisioning in edge-enabled vehicular cloud networks towards sustainable smart cities Sustain. Cities Soc. 76 103384.

[27] Alshahrani M and Traore I 2019 Secure mutual authentication and automated access control for IoT smart home using cumulative Keyed-hash chain J. Inf. Secur. Appl. 45 156–75.

[28] Ma M, Shi G and Li F 2019 Privacy-Oriented Blockchain-Based Distributed Key Management Architecture for Hierarchical Access Control in the IoT Scenario IEEE Access 7 34045–59.

[29] Xiong F, Xu C, Ren W, Zheng R, Gong P and Ren Y 2022 A blockchain-based edge collaborative detection scheme for construction internet of things Autom. Constr. 134 104066.

[30] Ali I, ul Hussen Khan R J, Noshad Z, Javaid A, Zahid M and Javaid N 2020 Secure Service Provisioning Scheme for Lightweight Clients with Incentive Mechanism Based on Blockchain vol 96 (Springer International Publishing).

[31] Liu H, Han D and Li D 2020 Fabric-iot: A Blockchain-Based Access Control System in IoT IEEE Access 8 18207–18.

[32] Alam M, Emmanuel N, Khan T, Khan A and Javaid N 2018 Secure policy execution using reusable garbled circuit in the cloud Futur. Gener. Comput. Syst. 87 488–501.

[33] Bonnah E and Shiguang J 2020 DecChain : A decentralized security approach in Edge Computing based Futur. Gener. Comput. Syst. 113 363–79.

[34] Lei K, Fang J, Zhang Q, Lou J, Du M, Huang J, Wang J and Xu K 2020 Blockchain-Based Cache Poisoning Security Protection and Privacy-Aware Access Control in NDN Vehicular Edge Computing Networks J. Grid Comput. 18 593–613.

[35] Hong S 2020 P2P networking based internet of things (IoT) sensor node authentication by Blockchain Peer-to-Peer Netw. Appl. 13 579–89.

[36] Brogan J, Baskaran I and Ramachandran N 2018 Authenticating Health Activity Data Using Distributed Ledger Technologies Comput. Struct. Biotechnol. J. 16 257–66.

[37] Lin C, He D, Huang X, Choo K K R and Vasilakos A V. 2018 BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0 J. Netw. Comput. Appl. 116 42–52.

[38] Ur Rahman M, Guidi B and Baiardi F 2020 Blockchain-based access control management for Decentralized Online Social Networks J. Parallel Distrib. Comput. 144 41–54.

[39] Makhdoom I, Zhou I, Abolhasan M, Lipman J and Ni W 2020 PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities Comput. Secur. 88 101653.

[40] Paul R, Ghosh N, Sau S, Chakrabarti A and Mohapatra P 2021 Blockchain based secure smart city architecture using low resource IoTs Comput. Networks 196.

[41] Alcaraz C, Rubio J E and Lopez J 2020 Blockchain-assisted access for federated Smart Grid domains: Coupling and features J. Parallel Distrib. Comput. 144 124–35.

[42] Zhang J, Wang Z, Shang L, Lu D and Ma J 2020 BTNC: A blockchain based trusted network connection protocol in IoT J. Parallel Distrib. Comput. 143 1–16.

[43] Siris V A, Dimopoulos D, Fotiou N, Voulgaris S and Polyzos G C 2020 Decentralized authorization in constrained IoT environments exploiting interledger mechanisms ☆ Comput. Commun. 152 243–51.

[44] Vishwakarma L and Das D 2021 SCAB - IoTA: Secure communication and authentication for IoT applications using blockchain J. Parallel Distrib. Comput. 154 94–105.

[45] Suresh A, Hamza R, Hassan A, Jiang N and Yan H 2020 Computers & Security Efficient privacy-preserving authentication protocol using PUFs with blockchain smart contracts Comput. Secur. 97 101958.

[46] Hammi M T, Hammi B, Bellot P and Serhrouchni A 2018 Bubbles of Trust: A decentralized blockchain-based authentication system for IoT Comput. Secur. 78 126–42.

[47] Satamraju K P and Malarkodi B 2021 A decentralized framework for device authentication and data security in the next generation internet of medical things Comput. Commun. 180 146–60.

[48] Huang J C, Shu M H, Hsu B M and Hu C M 2020 Service architecture of IoT terminal connection based on blockchain identity authentication system Comput. Commun. 160 411–22.

[49] Zhao Y, Liu Y, Tian A, Yu Y and Du X 2019 Blockchain based privacy-preserving software updates with proof-of-delivery for Internet of Things J. Parallel Distrib. Comput. 132 141–9.

[50] Hameed K, Garg S, Amin M B and Kang B 2021 A formally verified blockchain-based decentralised authentication scheme for the internet of things vol 77 (Springer US).

[51] Mohammad Hossein K, Esmaeili M E, Dargahi T, Khonsari A and Conti M 2021 BCHealth: A Novel Blockchain-based Privacy-Preserving Architecture for IoT Healthcare Applications Comput. Commun. 180 31–47.

[52] Zhang Y, Deng R H, Han G and Zheng D 2018 Secure smart health with privacy-aware aggregate authentication and access control in Internet of Things J. Netw. Comput. Appl. 123 89–100.

[53] Fotohi R and Shams Aliee F 2021 Securing communication between things using blockchain technology based on authentication and SHA-256 to improving scalability in large-scale IoT Comput. Networks 197 108331.

[54] Guo S, Wang F, Zhang N, Qi F and Qiu X 2020 Master-slave chain based trusted cross-domain authentication mechanism in IoT J. Netw. Comput. Appl. 172 102812.

[55] Narayanan U, Paul V and Joseph S 2021 Decentralized blockchain based authentication for secure data sharing in Cloud-IoT: DeBlock-Sec J. Ambient Intell. Humaniz. Comput.

[56] Panda S S, Jena D, Mohanta B K, Ramasubbareddy S, Daneshmand M and Gandomi A H 2021 Authentication and Key Management in Distributed IoT Using Blockchain Technology IEEE Internet Things J. 8 12947–54.

[57] Patwary A A, Fu A, Kumar S and Kumar R 2020 FogAuthChain : A secure location-based authentication scheme in fog computing environments using Blockchain Comput. Commun. 162 212–24.

[58] Jaikla T, Vorakulpipat C, Rattanalerdnusorn E and Hai H D 2019 A secure network architecture for heterogeneous IoT devices using role-based access control 2019 27th Int. Conf. Software, Telecommun. Comput. Networks, SoftCOM 2019.

[59] Mistry I, Tanwar S, Tyagi S and Kumar N 2020 Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges Mech. Syst. Signal Process. 135 106382.

[60] Song L, Zhu Z, Li M, Ma L and Ju X 2021 A Novel Access Control for Internet of Things Based on Blockchain Smart Contract IEEE Adv. Inf. Technol. Electron. Autom. Control Conf. 2021 111–7.

[61] Chiu W Y, Meng W and Jensen C D 2021 My data, my control: A secure data sharing and access scheme over blockchain J. Inf. Secur. Appl. 63 103020.

[62] Cruz J P, Kaji Y and Yanai N 2018 RBAC-SC: Role-based access control using smart contract IEEE Access 6 12240–51.

[63] Wan Muhamad W N, Matrazali N, Ishak K, Hasbullah N, Zainudin N, Ramli S, Wook M, Ishak Z and MSaad N 2019 Enhance Multi-factor Authentication Model for Intelligence Community Access to Critical Surveillance Data pp 560–9.

[64] Putra G D, Dedeoglu V, Kanhere S S, Jurdak R and Ignjatovic A 2021 Trust-Based Blockchain Authorization for IoT IEEE Trans. Netw. Serv. Manag. 18 1646–58.

[65] Liu Y, Lu Q, Chen S, Qu Q, O'Connor H, Raymond Choo K K and Zhang H 2020 Capability-based IoT access control using blockchain Digit. Commun. Networks 0–6.

[66] Pal S, Rabehaja T, Hitchens M, Varadharajan V and Hill A 2020 On the Design of a Flexible Delegation Model for the Internet of Things Using Blockchain IEEE Trans. Ind. Informatics 16 3521–30.

[67] Ali G, Ahmad N, Cao Y, Ali Q E, Azim F and Cruickshank H 2019 BCON: Blockchain based access CONtrol across multiple conflict of interest domains J. Netw. Comput. Appl. 147 102440.

[68] Abou-Nassar E M, Iliyasu A M, El-Kafrawy P M, Song O Y, Bashir A K and El-Latif A A A 2020 DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems IEEE Access 8 111223–38.

[69] Taherkordi A and Herrmann P 2018 Pervasive Smart Contracts for Blockchains in IoT Systems 6–11.

[70] Hakiri A and Dezfouli B 2021 Towards a Blockchain-SDN Architecture for Secure and Trustworthy 5G Massive IoT Networks SDN-NFV Sec 2021 - Proc. 2021 ACM Int. Work. Softw. Defin. Networks Netw. Funct. Virtualization Secur. co-located with CODAYSPY 2021 11–8.

[71] Egala B S, Pradhan A K, Badarla V and Mohanty S P 2021 Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things with Effective Access Control IEEE Internet Things J. 8 11717–31.

[72] Sanwar Hosen A S M, Singh S, Sharma P K, Ghosh U, Wang J, Ra I H and Cho G H 2020 Blockchain-Based Transaction Validation Protocol for a Secure Distributed IoT Network IEEE Access 8 117266–77.

[73] Razali N A M, Muhamad W N W, Ishak K K, Saad N J A M, Wook M and Ramli S 2021 Secure Blockchain-Based Data-Sharing Model and Adoption among Intelligence Communities IAENG Int. J. Comput. Sci. 48.

[74] Guruprakash J and Koppu S 2020 EC-ElGamal and Genetic Algorithm-Based Enhancement for Lightweight Scalable Blockchain in IoT Domain IEEE Access 8 141269–81.

[75] Xu L, Chen L, Gao Z, Fan X and Shi W 2020 DL-DP: Improving the security of industrial IoT with decentralized ledger defined perimeter BSCI 2020 - Proc. 2nd ACM Int. Symp. Blockchain Secur. Crit. Infrastructure, Co-located with AsiaCCS 2020 53–62.

[76] Syed T A, Siddique M S, Nadeem A, Alzahrani A, Jan S and Khattak M A K 2020 A Novel Blockchain-Based Framework for Vehicle Life Cycle Tracking: An End-to-End Solution IEEE Access 8 111042–63.

[77] Pajooh H H, Rashid M, Alam F and Demidenko S 2021 Hyperledger fabric blockchain for securing the edge internet of things Sensors (Switzerland) 21 1–29.

[78] Serrano W 2021 The Blockchain Random Neural Network for cybersecure IoT and 5G infrastructure in Smart Cities J. Netw. Comput. Appl. 175 102909.

[79] Tan L, Shi N, Yu K, Aloqaily M and Jararweh Y 2021 A Blockchain-empowered Access Control Framework for Smart Devices in Green Internet of Things ACM Trans. Internet Technol. 21.

[80] Pyoung C K and Baek S J 2020 Blockchain of Finite-Lifetime Blocks with Applications to Edge-Based IoTa IEEE Internet Things J. 7 2102–16.

[81] Ali G, Ahmad N, Cao Y U E, Khan S, Cruickshank H, Qazi E A L I and Ali A 2020 xDBAuth: Blockchain Based Cross Domain Authentication and Authorization Framework for Internet of Things 8.