INTERNATIONAL JOURNAL OF RESEARCH AND INNOVATION IN APPLIED SCIENCE (IJRIAS)
ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

Comprehensive Investigation of Blockchain-Based Access Control on the Internet of Things

Joshua Iranwose Ugbesia and Fortune Ordiah

Derby, United Kingdom

DOI: https://doi.org/10.51584/IJRIAS.2026.11070182

Received: 02 August 2026; Accepted: 07 August 2026; Published: 19 August 2026

ABSTRACT

Blockchain technology offers a potential solution for enhancing access control mechanisms in Internet of Things (IoT) environments. Conventional access control solutions face difficulties in terms of scalability, security, and interoperability, especially when dealing with the extensive and varied nature of IoT networks. The decentralised, irreversible, and transparent ledger system of blockchain provides a robust framework for tackling these challenges. This paper examines the incorporation of blockchain technology into IoT systems for the purpose of access control, with a specific emphasis on recent advancements and methodologies. We examined the benefits, which encompass enhanced security, reduced vulnerability to system failures, and improved openness. In addition, we analysed challenges such as scalability, processing overhead, and privacy concerns. This paper conducts a comprehensive analysis and evaluation of the current status of blockchain-based access control on the Internet of Things (IoT). Its purpose is to provide researchers with a thorough understanding of the topic, including various approaches, models, standards, platforms, and potential applications for implementing blockchain-based access control in IoT. Out of the total of 207 papers, a subset of 72 were chosen for additional study, by applying the inclusion and exclusion criteria. The selected papers were evaluated and summarized to highlight their respective strengths and weaknesses. Moreover, the study examined the suitability and occurrences of using blockchain technology for access control in IoT devices. In the end, the discussion included challenges, potential areas for research, and an explanation of how blockchain technology can be used for access management on the IoT.

INTRODUCTION

Enforcing restrictions on the availability of resources and information within computer networks is a crucial element of cybersecurity known as access control. Access permissions are established through the process of authorisation, which considers the responsibilities or attributes of users, while authentication verifies the identities of users. Accountability guarantees the tracing of user action. Access control systems such as firewalls and encryption are implemented to prevent unauthorised access and enforce security regulations. The three primary objectives of this system are to uphold confidentiality, minimise data breaches, and mitigate insider dangers. Access controls facilitate compliance with standards such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation). (S. De Capitani di Vimercati, et al., 2008).

Blockchain technology is a decentralised ledger system that has the potential to revolutionise access control applications. It records transactions across a distributed network to provide immutability, security, and transparency. Blockchain empowers consumers to have authority over their digital identities by facilitating decentralised identity management through access control. Smart contracts are self-executing programs deployed on a blockchain to enhance accountability and transparency by automating access rights according to preset criteria. Token-based access control enables the safe issuance, transfer, and revocation of access entitlements. Immutable logs recorded on blockchains provide an unalterable record of access events, ensuring accountability and compliance. Privacy-preserving access control systems provide secure protection of private information. Access control applications on blockchain also have the potential to revolutionise security, privacy, and efficiency by providing a robust framework for managing digital identities and access privileges (Yang Lu, 2019). Furthermore, this study aims to investigate the potential of blockchain technology in transforming access control protocols in the IoT space.

Conventional access control mechanisms involve the techniques and frameworks employed to oversee and govern the accessibility of resources, including information, networks, and physical areas. These systems frequently rely on manual procedures and the employment of middlemen or intermediaries to allow or deny access to those who are permitted. Access control techniques that use manual procedures necessitate human interaction for functions like access management, authorisation, and user authentication. Due to human error or malevolent intent, this manual method can be difficult, prone to mistakes, and vulnerable to security flaws.

Addressing the issues around blockchain-based access control in the IoT's are critical to protecting the availability, confidentiality, and integrity of IoT data as well as guaranteeing adherence to legal requirements and industry standards. By utilising blockchain technology to improve access control within IoT ecosystems, enterprises may reduce security risks, safeguard user privacy, and realise the full potential of IoT innovation across various industries and applications. For tackling the particular needs and difficulties of blockchain-based access control in IoT's, current theories, solutions, and methods for IoT access control may not be sufficient or appropriate. Businesses can overcome these constraints and realise the whole possibilities of a secure, compatible, and robust access control in IoT systems by capitalising on the decentralised, transparent, and scalable characteristics of blockchain technology. Due to the decentralised, immutable, and transparent nature, blockchain technology has emerged as a possible solution to these problems. The main goals of this study is to examine current access control systems and identify the problems within, assess how blockchain technology can change this situation with regards to IoT, quantify the difficulties in putting blockchain-based solutions into practice, and provide possible suggestions for development (Sara Rouhani, 2019).

This research provides a systematic literature review of blockchain-based access control models, in order to achieve these aims we need these objectives as follows.

- Investigate the state-of-the art studies related to current access control systems.
- Identify the approaches and models used to implement blockchain-based access control in IoT.
- Clarify how blockchain technology can be implemented with access control standards, frameworks, and protocols.
- Analyse the possible uses and scenarios for implementing blockchain technology in access control mechanisms.
- Identify the challenges, newest development and potential path for blockchain-based access control

METHODOLOGY

Research Methods

Research methods are the foundation of scientific works. This method employs systematic processes for asking questions, collecting data, examining findings, and drawing inferences. They cover a range of methods for gathering and analysing data, guaranteeing its authenticity, dependability, and ethical behaviours. There are several types of research methods. These are but not limited to quantitative, qualitative and mixed methods, but for the sake of our systematic literature review, we will focus on the qualitative research methodology.

Qualitative Research Method:

This kind of research approach focuses on understanding the significance and personal experiences of individuals; in this type of study, we thoroughly examine complicated incident, situations, and social interactions in order to collect rich and detailed data about people's attitudes, sentiments, and actions. Focus groups, participant observation, and interviews are examples of qualitative research methodologies.

- Interview: this is a one-on-one discussion with people or individuals in order to get their opinions and ideas on a given subject.
- Focus groups: entail gathering a small group of people to talk about and exchange experiences and viewpoints regarding a particular topic.
- Participant observation: a researcher observes and records participant behaviors and interactions by fully immersing oneself in a specific social situation or group.

With the use of these techniques, we can collect more grounded and detailed data, leading to a greater comprehension of the study issue. In the social sciences, psychology, anthropology, and other disciplines where comprehending human behaviours and experiences is crucial, qualitative research is frequently used. Rather than being provided as numerical data or statistical analysis, the results of qualitative research are often presented as narratives, themes, and patterns.

Quantitative Research Methods:

This kind of research approach entails analysing and interpreting numerical data using statistical techniques, as well as determining how frequently various kinds of access control systems are employed. Surveys, experiments, and other sources are different ways of collecting data, and these methods provide us with quantitative data that can be analysed using statistical techniques.

Research Methodology

This systematic literature review characterises, evaluates, and interprets research meeting defined criteria on blockchain-based access control published between 2009 and 2023. This systematic literature review aims to learn more about the latest developments, problems, and solutions pertaining to blockchain-based access control systems. In conducting a systematic literature review, the following are the different steps as shown in figure 1 below.

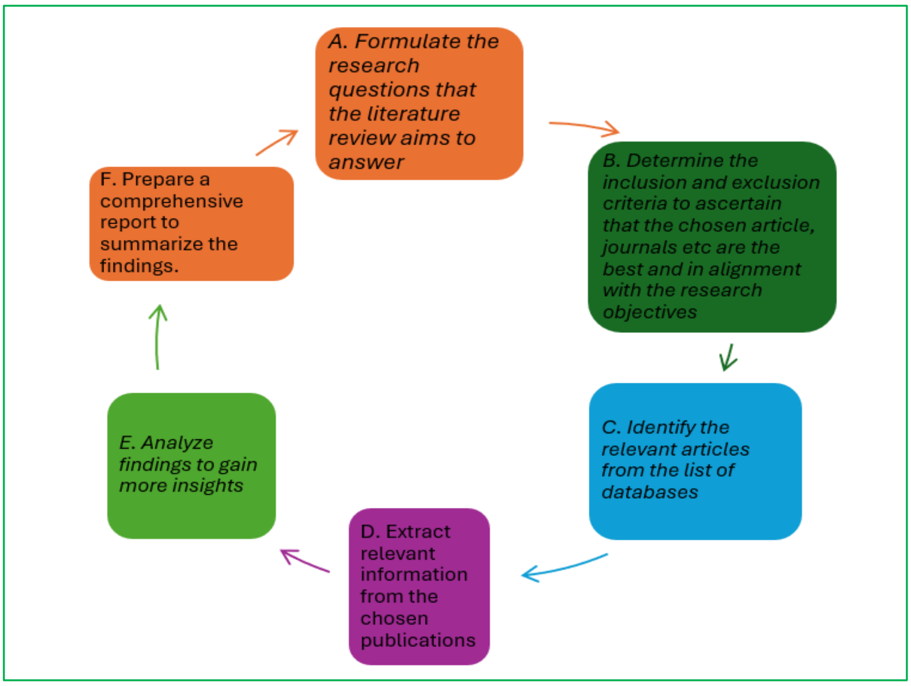

Figure 1: stages of conducting a systematic literature review

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

By conducting a thorough and methodical review of the existing literature, the study aims to advance knowledge in the field of blockchain-based access control and contribute to the understanding of researchers, practitioners, and policymakers working in the field. This methodology is a predefined set of steps and criteria to identify, select, and analyse relevant studies in a rigorous and methodical manner. It offers trustworthy and evidence-based insights on blockchain-based access control. Through the implementation of a methodical literature review approach, the research guarantees that the insights offered are grounded in an exhaustive and impartial examination of the extant literature.

Notwithstanding being employed in numerous systematic literature reviews, this methodology has certain drawbacks, such as the fact that it restricts the scope of the review or study and might not give readers all the information they want to comprehend the topic at hand.

Furthermore, only studies published between 2009 and 2023 were reviewed for this study. The search methodology restricts the number of papers that may be reviewed in the study, even though it gives readers an overview of cutting-edge studies published for all the years.

Research Questions

- RQ1: What are the state-of-the-art studies related to blockchain-based access control in IoT?
- RQ2: What are the approaches and models used to implement blockchain-based access control in IoT?
- RQ3: What are the access control standards and platforms used to implement the blockchain-based access control model in IoT?
- RQ4: What are the potential applications and use cases where the blockchain-based access control models were adopted in IoT?
- RQ5: What are the challenges and future directions in blockchain-based access control models

The Inclusion and Exclusion criteria

To choose the relevant studies, inclusion and exclusion criteria were applied. Answering the research questions and ensuring the production of a successful literature review was the main goal of these criteria.

The inclusion criteria were as follows:

- Peer-reviewed publications, proceedings from conferences, or reliable scholarly sources between 2009 and 2023.
- Theoretical models, or conceptual frameworks pertaining to blockchain-based access control.
- Articles are written in English.
- Articles that are related to research questions.

The exclusion criteria were as follows:

- Articles that are not related to the research questions.
- Research unavailable via credible sources or scholarly databases.
- Research without supporting data or original ideas from theory.
- Non-English Articles.

- Articles that have previously been included twice.

Data sources

The searches were carried out using digital libraries. The following electronic databases were utilised in this systematic literature review.

- Google Scholar
- PubMed
- Science direct (Elsevier)
- SpringerLink
- ACM Digital Library
- IEEE Xplore
- MDPI Publisher

Phases of Selection

This stage required selecting from among the 207 articles collected from various online digital libraries important and recent studies on blockchain-based access control in IoT. There were several stages to the selection of applicable literature.

- The inclusion and exclusion criteria were used to sort publications that were discovered during the search and those that were already part of the collection. Only publications published between 2009 and 2023 that addressed the subject of blockchain-based access management in IoT were included in the search parameters.
- We concentrated on removing duplicates from the seven digital libraries we used to compile our publishing collection during this phase.

With the aid of keyword searches, the relevant papers for the topic and research questions were located. The following search phrases were:

- Smart contract
- Access control
- Decentralisation
- Internet of Things (IoT)
- Blockchain
- Permissioned and Permissionless Blockchain
- Immutability

Data collection

The dataset comprises published publicly available articles hence no primary data collection was required.

Ethical approval

Ethical approval was not required. The study analyses published publicly available articles and no primary data were collected.

RESULTS

The objective of this chapter is to present the study findings in an orderly fashion that directly addresses each of the five research questions. This presentation is essential because it helps readers see how the study's conclusions relate to the original questions and whether the goals of the research have been achieved.

Result Analysis

As previously mentioned, the gathered publications were subjected to the inclusion and exclusion criteria in three stages. After a total of 207 publications were screened, 135 of them were excluded because they did not meet the inclusion criteria from stage 1 to 3 as shown in table 1 below.

We were able to gather the majority of papers relevant to blockchain-based access control in the IoT by conducting a search across seven reputable web databases. Table 1 below displays the findings of the articles gathered from each online database as well as the total number of publications following the application of the three selection steps.

Table 1: Analysis of search result

Data Source	**Stage 1**	**Stage 2**	**Stage 3**
Google Scholar	57	17	14
PubMed	23	18	15
IEEE Xplore	41	13	12
SpringerLink	31	9	4
Science Direct (Elsevier)	15	6	5
Mpdi.com	26	13	12
ACM Digital Library	14	12	10
Total	**207**	**88**	**72**

Research Included the following as shown in table 2 below:

Table 2: Citation, Publication Type and Year

S/N	**Citation**	**Publication Type**	**Year**
1.	Ghazal et al.	Journal	2020
2.	Yanru and Chen Chen et al.	Journal	2023
3.	Narouei et al.	Conference	2017

4.	Mutka et al.	Journal	2017
5.	Habib et al.	Journal	2014
6.	H. Wang et al.	Journal	2022
7.	Charalampos et al.	Journal	2022
8.	Sherish Shafeeq et al.	Journal	2019
9.	Kauser et al.	Journal	2018
10.	Batchu et al.	Journal	2022
11.	Fotiou et al.	Report	2022
12.	Vincent et al.	Report	2015
13.	Zhang et al.	Report	2014
14.	Ronghua et al.	Journal	2018
15.	Fernandez et al.	Report	2019
16.	Hao et al.	Conference	2022
17.	Xu et al.	Journal	2019
18.	Yuta et al.	Journal	2018
19.	Yining et al.	Conference	2019
20.	Karimibiuki et al.	Journal	2018
21.	Ronghua Xu et al.	Journal	2020
22.	Manar et al.	Journal	2019
23.	Faisal et al.	Conference	2021
24.	Qingfeng et al.	Journal	2009
25.	Sara Rouhani et al.	Report	2019
26.	Baobao et al.	Journal	2020
27.	Novo et al.	Journal	2018
28.	Paillisse et al.	Report	2019
29.	Dukkipati et al.	Conference	2018
30.	Osterberg et al.	Journal	2021
31.	Khan et al.	Conference	2021

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

32.	Riabi et al.	Conference	2019
33.	Teo Poh et al.	Conference	2010
34.	Oscar et al.	Conference	2017
35.	Faith et al.	Conference	2017
36.	Desperats et al.	Conference	2018
37.	R. Ghazal et al.	Journal	2020
38.	Sara Rouhani et al.	Conference	2021
39.	Sehrish Shafeeq et al.	Conference	2019
40.	Sheng ding et al	Conference	2019
41.	Yan Zhuet al.	Conference	2019
42.	Hany Atlam et al	Journal	2018
43.	Damiano di Francesco et al	Conference	2017
44	Namane et al	Journal	2022
45.	Rinki Singh et al	Report	2023
46.	S. Cirani et al	Journal	2015
47.	V. A Siris et al	Journal	2019
48.	Campbell et al.	Journal	2015
49.	C. Rupa et al.	Conference	2020
50.	R. Xu et al.	Journal	2018
51.	Sana Moin et al	Journal	2019
52.	Pajarnay Sharma et al.	Journal	2021
53.	Mehmood et al	Conference	2023
54.	Kuperberg et al.	Journal	2020
55.	Minango et al.	Conference	2023
56.	Rateb Jabbar et al.	Conference	2022
57.	Beesem Zaabar	Journal	2021
58.	Salonikas et al.	Journal	2022
59.	Chinmay Saraf et al	Journal	2018

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

60.	P.P Ray et al.	Conference	2021
61.	Shantanu Pal et al	Journal	2022
62.	Muneeb Hassan et al.	Journal	2019
63.	Malak Alamri et al	Journal	2019
64.	Abdurrashid Ibrahim Sanka et al.	Journal	2021
65.	J. Howlett et.al	Report	2016
66.	Y. Huang et al.	Journal	2019
67.	Yuanyu Zhang et. al	Journal	2018
68.	S. Aich et. al	Conference	2019
69.	Abderahman Rejeb	Journal	2019
70.	K. Azbeg et. al	Journal	2022
71.	U. Agrawal et. al	Conference	2019
72.	Bharat Bhushan et al.	Journal	2020

Result

Many researchers are investigating blockchain-based IoT access control to find better and more efficient approaches to combat this emerging threat. These researchers can review previous research that may be relevant to their study questions and use this material as a great starting point to comprehend this paradigm.

RQ1: What are the state-of-the-art studies related to blockchain-based access control?

The relevant publications about blockchain-based access control in IoT that can be used to address this research issue are listed in the table below; this table enumerates each publication's contributions.

This paper's discussion section is devoted to the examination of recovered and examined papers concerning blockchain-based access control methods for Internet of Things devices. Reviews and summaries of recent peer-reviewed publications that describe blockchain technology are provided. Every article advances our knowledge of the ways in which blockchain technology can be applied to access control in many IoT scenarios. For academics wishing to understand and apply blockchain-based access control in IoT. Table 3 below offers a thorough synopsis of the major contributions of each paper.

Table 3: Summary of Research papers

Citation	**Summary of contribution on each paper**	**Limitation**
R. Ghazal (2020)	In order to improve adaptability through semantic technologies, the study proposes an intelligent role-based access control (RBAC) model that makes use of semantic business roles for effective access management in multi-domain situations.	The suggested model's drawbacks could include difficulties in coordinating semantic roles across several domains and scalability issues with large-scale deployments.

Yanru Chen & chen et. al (2023)	Aiming to improve granularity and adaptability in access control methods, the article suggests a capability and blockchain-based access control paradigm for flexible and fine-grained access management.	comprise difficulties guaranteeing interoperability with current systems, difficulty in maintaining capabilities and blockchain integration, and scalability limitations with large-scale implementations.
Narouei et. al (2017)	The paper presents research findings and advances in the field while discussing a variety of subjects connected to access control models and technologies.	However, limitations include a lack of in-depth analysis because of the scope of subjects covered, a lack of room for in-depth investigation, and possible bias towards particular research fields or viewpoints
Mutka et al. (2018)	This work aims to improve security and privacy in access control methods by presenting a blockchain-based privacy-preserving access control framework for pervasive settings.	Difficulty in assuring compatibility with current systems or standards, complexity in implementing and managing the suggested framework, and scalability issues with blockchain technology in ubiquitous environments.
M.A Habib et al. (2014)	This work aims to improve access control security and flexibility by discussing a permission-based method for implementing Dynamic Separation of Duty (DSD) in RBAC systems.	Difficulties in implementing fine-grained access control, as well as possible performance overhead related to managing dynamic separation of duties rules in large-scale systems.
H. Wang et al. (2022)	Using blockchain technology, the study presents a distributed Attribute-Based Access Control (ABAC) scheme that aims to improve access control mechanisms by promoting transparency and decentralisation.	The distributed ABAC scheme has drawbacks that affect its applicability and efficiency in real-world deployments, such as scalability issues, blockchain integration challenges, and significant performance overhead.
Charalampos Savvaidis et. al (2022)	Using distributed techniques, this study investigates ways to improve security and scalability in Internet of Things environments by decentralising access management.	Scalability problems and the intricacy of administering decentralised access control policies in Internet of Things systems are possible obstacles.
Sehrish Shafeeq et.al (2019)	The study presents a decentralised access control system that is privacy-aware, illuminating creative ways to improve privacy protection in access control mechanisms and probably advancing the development of privacy-enhancing technologies.	Limitations include difficulties in managing privacy requirements across various access control regimes and scalability issues with decentralised systems.
Batchu S et.al (2022)	This study addresses privacy and security issues in healthcare data management by examining the use of Ethereum smart contracts for the safe exchange and storage of COVID-19 patient data.	Difficulty with handling sensitive medical data in conformity with regulations, worries about data privacy and security
N. Fotiou et. al. (2022)	This study examines how to improve security and access control methods in IoT environments by using Verifiable	The difficulty of maintaining authenticated credentials in dynamic settings and possible

	Credentials to implement a capabilities-based access control approach for IoT devices.	incompatibilities with current access control systems
Vincent Hu et.al. (2015)	This paper offers a review and analysis of access control systems, maybe with best practices, methodology, and standards for judging the security and efficacy of the systems in question.	possible narrow focus, its scant attention to new technology, and the requirement for regular upgrades to stay current in the quickly changing field of security.
Zhang et al. (2014)	In order to improve security and dependability in access control mechanisms, this paper addresses approaches for creating and evaluating attribute-based access control policies.	Among the drawbacks are the difficulty of creating and evaluating attribute-based access control policies and the scalability issues with large-scale implementations.
Ronghua Xu et.al (2020)	This paper investigates the use of blockchain technology and smart contracts to provide decentralised access control for IoT environments, mostly with the goal of resolving security and privacy issues with IoT systems.	Integrating blockchain and smart contracts with current systems, privacy, and data protection.
Ronghua Xu et al. (2018)	This paper explains a smart contract-based decentralised access control system for Internet of Things environments that aims to improve access control's flexibility and security.	Challenges in implementing and managing smart contract-enabled solutions, interoperability, and scalability using decentralised access control techniques in IoT environments.
Fernandez et. al. (2019)	It provides an overview of research on several facets of data and application security and privacy.	Inadequate breadth in covering all facets of a subject, shallowness in individual studies, and possible biases in the way the research was chosen and presented.
J. Hao et.al (2022)	This paper combines off-chain signature verification with on-chain evaluation to provide a revolutionary smart contract-based access control mechanism that improves security and efficiency.	Potential security flaws in the implementation, difficulties in handling off-chain and on-chain components
Xu et.al. (2019)	In order to potentially solve security and privacy concerns in dispersed contexts, this article explores the use of blockchain technology for access control in business blockchain systems.	Issues with data privacy and regulatory compliance, as well as difficulties incorporating blockchain technology into current business processes.
Yuta Nakamura et.al. (2018)	The goal of this study is to improve access management security and flexibility by investigating the application of capability-based access control techniques designed for Internet of Things contexts.	Interoperability problems with current access control systems, difficulties in monitoring and updating capabilities dynamically, and difficulties with capability-based access control in large-scale IoT implementations.

Yining Hu et.al. (2019)	This study aims to provide insights into the state-of-the-art, problems, and future directions in the field of blockchain-based smart contract applications for IoT applications. It does this by presenting an extensive assessment of the literature in the field.	Concerns about the overhead involved in using smart contracts on devices with limited resources.
M**.** Karimibuiki et.al**.** (2018)	This paper offers a dynamic policy-based access control mechanism designed specifically for Internet of Things (IoT) systems with the goal of improving security and flexibility in access authorisation management.	Difficulties creating and managing dynamic rules, potential overheads in putting policies into place on IoT devices with constrained resources.
Manar Abdelhamid et.al. (2019)	This study investigates the uses and ramifications of smart contracts and blockchain technology, with the possibility of addressing how they may affect different industries like supply chains, banking, and government.	Concerns about legal and regulatory frameworks and compliance, and difficulties guaranteeing security and privacy in decentralised systems.
Faisal Jamil et.al. (2021)	This paper covers a range of sensor technology topics and their uses.	Limited scope, Narrow applicability, Lack of experimental validation.
Qingfeng He et.al. (2009)	This paper presents the ReCAPS process, which is centered on evaluating access control requirements and defining policies that correlate with them.	Complexities involved in putting the ReCAPS technique into practice, also challenges in coordinating access control rules with changing system requirements,
Baobao Chaia et.al. (2020)	This paper presents a technique or system for implementing fine-grained access control using smart contracts. This strategy might try to improve security and control over who can access resources or data.	Difficulties in establishing access control policies, overhead associated with executing smart contracts on blockchain networks.
Novo et.al. (2018)	To overcome the issues of scalable access control, this study offers an architecture that combines blockchain technology with Internet of Things technologies.	Difficulties in setting up and maintaining access control systems based on blockchain technology, and problems with blockchain's scalability in IoT deployments
Paillisse et.al. (2019)	This study investigates distributed access control systems using blockchain technology. This strategy might try to solve issues with decentralisation and security in access control for different apps or networks.	Issues with distributed access control policy management and worries about blockchain transaction performance overhead in real-time communication settings.
Dukkipati et.al (2018)	This paper addresses managing access to IoT devices and data across many networks may be made more secure, autonomous, and compatible with these methods.	Implementing a decentralised blockchain-based access control framework is hard, and scaling access control policies over a large number of IoT devices may bring challenges

Osterberg et.al. (2021)	In order to secure the Internet of Things (IoT), this study presents an overview and analysis of distributed access control mechanisms for blockchain systems.	Issues with overseeing access control rules in extensive IoT installations.
Khan et.al. (2021)	The study discusses a number of topics related to smart contracts, including possible applications, technical constraints, and legal issues.	A small sample size, reliance on self-reported data, lack of previous research for comparison, and cultural context specificity.
I. Riabi et.al. (2019)	This paper suggests an access control system based on blockchain that is suited for Internet of Things settings. It aims to enhance security, openness, and decentralisation in the administration of IoT device.	limited real-world implementation, reliance on simulation data, and a lack of extensive validation
Teo Poh Kuang et.al. (2010)	Explains how to integrate role-based access control model-based security extensible access control markup language rules in collaborative healthcare settings. The goal of this integration is to improve healthcare facilities' security and access control systems.	Absence of a thorough assessment of performance and practicality in the real world, as well as a comparison with other policy integration techniques
Oscar Mortagua Pereira et.al (2017)	This article addresses the architectural and security elements of the (XACML) standard. Talks about how XACML handles security issues and access control requirements in big data, IoT, and other areas are included in this.	Problems integrating XACML with current IT infrastructures and applications, as well as scalability concerns with XACML rules in large-scale deployments.
Fatih Turkmen et.al (2017)	This paper reports on a study that uses Satisfiability Modulo Theories (SMT) to analyse XACML policies. The purpose of this study is to enhance comprehension, validation, or optimisation of the XACML-specified access control policies.	Limitations include complexities in the analysis process and potential limitations of the SMT approach in handling certain types of policy specifications.
Desperats, N.D et.al. (2022)	In order to improve XACML efficiency in high-performance or resource-constrained applications, this study presents an asynchronous method to accelerate PDP decision-making in stable contexts.	The extension ignores issues such as policy conflicts, which could have an impact on the dependability of decision-making.
Hany Atlam et.al. (2018)	This paper examines how to establish and manage access control rules in Internet of Things (IoT) systems to improve security and privacy. It also analyses the usage of XACML for building access control policies in IoT contexts.	Difficulties in managing a large number of devices and access rules, as well as challenges in scalability when implementing XACML-based access control policies.

Damiano Di Francesco Maesa et.al (2017)	The approach utilises blockchain for transparent access control policies and rights exchanges, ensuring distributed auditability and mitigating fraudulent denial of granted rights. By deploying XACML policies on the Bitcoin blockchain, it enables decentralised access control, eliminating the need for a centralised authority.	Because the study is only shown on the Bitcoin blockchain, it is not widely applicable and lacks large-scale validation
Namane et.al. (2022)	This paper looked into the specific problems that IoT networks and devices bring, and how blockchain technology may be used to improve access control in IoT environments.	Insufficient thorough testing and practical deployment of the suggested blockchain-based access control methods for IoT applications.
Rinki Singh et.al. (2023)	This study presents a comprehensive assessment of the literature on access control for blockchain-enabled IoT security against cyberattacks.	Difficulties in combining various research techniques and approaches from the chosen studies, which could affect the conclusions' generalisability and depth of analysis.
S. Cirani et.al. (2015)	This paper suggests an architecture known as IoT OAS (IoT OAuth-based Authorisation Service). The architecture makes use of OAuth, a popular authorisation mechanism, to provide safe access to Internet of Things services.	OAuth is a commonly used standard for authorisation, there may be overhead, and complications associated with its use in IoTs scenarios that should be carefully considered.
V.A Siris et.al. (2019)	The study proposes a novel method for authorisation in limited IoT scenarios that uses blockchain technology and OAuth 2.0.	IoT devices with limited resources, such as processing power and memory, may not be able to implement technologies that demand substantial computational resources.
Campbell et.al. (2015)	Proposes the usage of SAML assertions in federated identity management, cross-domain identity federation, and web browser single sign-on.	This paper's focus is on the SAML 2.0 protocol, which when extensively used does not handle all upcoming security concerns or newer technologies.
C. Rupa et.al. (2020)	This study investigates how to improve access privacy in fog computing settings for Identity as a Service (IDaaS) systems by utilising the Security Assertion Markup Language (SAML) standard.	Potential security risks or related to the integration of the SAML protocol in fog computing systems were not covered
R. Xu et.al. (2018)	The article introduces BlendCAC, a decentralised capability-based access control system for Internet of Things environments that is supported by blockchain technology. It leverages smart contracts for automated enforcement and access control policy decentralisation via blockchain technology.	Scalability, Overhead, Security risk, Interoperability, and adoption barriers
Sana Moin et.al. (2019)	This paper proposed the difficulties that distributed blockchain systems provide in	Due to the constantly changing nature of blockchain and IoT technology, this paper's

	maintaining the security and privacy of Internet of Things data.	limitations did not fully address all potential security issues and solutions.
Pajarnay Sharma et.al. (2021)	The paper investigates how to improve security in 5G-driven industrial settings by utilising machine learning and deep learning approaches. It talks about how 5G networks provide security challenges.	The study overlooked other relevant approaches in favor of concentrating on certain machine learning or deep learning methodologies.
Mehmood et.al. (2023)	This paper explores Consent Management System (CMS) that uses Hyperledger Fabric blockchain technology to protect user data security and privacy, it describes the CMS's architecture and setup, emphasising how Hyperledger Fabric guarantees safe and open consent administration.	Scalability, Complexity, Integration, Regulatory Compliance, user adoption.
Kuperberg et.al. (2020)	Kuperberg offers an extensive analysis of blockchain-based identity management systems, looking at their uses and difficulties from an ecosystem and enterprise standpoint.	The topic of blockchain-based identity management is ever-evolving, hence the article, released in 2020, might not accurately reflect the most recent developments or difficulties.
Miniango et.al. (2023)	This paper explores supply chain management proof-of-concept applications for Corda blockchain technology. They give examples of several application cases, including supplier management, product traceability, and the implementation of smart contracts.	The study's applicability to larger-scale supply chain contexts is limited by its proof-of-concept nature. Additionally, the scalability was not thoroughly evaluated in the paper.
Rateb Jabbar et.al. (2022)	This paper discusses the literature on the use of blockchain technology in intelligent transport systems (ITS), it thoroughly examines the body of research in this area, addressing a range of topics including applications, difficulties, and potential future paths.	Due to the possibility of variation based on elements like infrastructure, regulatory frameworks, and geographic location, the results and conclusions derived from this study cannot be readily applied to all ITS environments or real-world scenarios.
Beesem Zabbar et.al. (2021)	This paper suggests "HealthBlock," as a safe blockchain-based healthcare data management platform to solve security and privacy issues in the administration of healthcare data.	Since blockchain may not be the best option in every healthcare data management scenario, the research did not examine other strategies
Salonikas et.al. (2022)	This paper relies on the confluence of blockchain technology with the Internet of Things (IoT) to provide safe transport systems in smart cities.	The article focuses on specific aspects of blockchain and IoT integration, potentially ignoring larger issues and alternate approaches.
Chinmay Saraf et.al (2018)	This study gives an overview of various blockchain platforms, their architectures, consensus mechanisms, smart contract	With the rapidly growing nature of blockchain technology, the content in this article may

	capabilities, scalability, security features, and real-world use cases.	quickly become outdated, because it does not cover the most recent advancements.
P.P Ray et.al (2021)	The study aims to provide insights into how blockchain might improve interoperability, security, and transparency in healthcare IoT systems.	The study focuses on the theoretical features of blockchain technology in healthcare IoT systems, rather than digging further into actual implementation issues or real-world case studies.
Shantanu Pal et.al (2022)	This study investigates several uses of blockchain-based access management in IoT systems and discusses recent advances in this field.	This work prioritises theoretical debates above practical issues, which may result in disregarding critical implementation details and deployment challenges.
Muneeb Hassan et.al (2019)	This study investigates many elements of the integration of blockchain and IoT systems, with a focus on privacy preservation.	The report lacks empirical investigations to back up the mentioned notions and proposals, which may limit the practical applicability of the outlined methodologies.
Malak Alamri et.al (2019)	The study seeks to help researchers investigate the potential of blockchain technology in IoT applications. It examines the interaction between blockchain and IoT, concentrating on research topics, obstacles, and future perspectives.	The challenge of guaranteeing compatibility between various blockchain platforms and IoT gadgets is brought to light, potentially impeding the smooth integration and communication required for effective IoT functions.
Abdurrashid Ibrahim Sanka et.al (2021)	The study outlines potential avenues for further research, including building user-friendly interfaces, ensuring privacy preservation, boosting interoperability, increasing security measures, and establishing scalable and energy-efficient consensus processes.	Future research directions were stated; however, they may not be thorough, leaving out developing trends and technology that could influence blockchain's progress.

RQ2: What are the approaches and models used to implement blockchain-based access control in IoT?

R. Ghazal et al. (2020) argued that the traditional role-based access control (RBAC) solutions are limited in adaptability and scalability, particularly in complex multi-domain situations thereby, integrating semantic technologies and clever algorithms which can improve RBAC systems by delivering more context-aware and flexible access control decisions. M.A Habib et al (2014) argued for the relevance and feasibility of integrating dynamic separation of duty (DSD) policies within RBAC systems, others claim that traditional static separation of duty (SSD) techniques are rigid and fail to accommodate growing security requirements. A permission-based strategy to implementing DSD was proposed, claiming that it gives greater flexibility and adaptability in addressing conflicts of interest and enforcing security regulations. Both authors concentrate on access control mechanisms within information systems, specifically role-based access control (RBAC) frameworks, models to improve access control with the goal of improving security, flexibility, and scalability, and the importance of access control in managing user permissions and protecting sensitive data from unauthorised access. Narouei et al. (2017) argued capability and blockchain-based access control architecture emphasising fine-grained and flexible permissions management for increased security and scalability in decentralised systems, while on the other hand Vincent Hu et al. (2015) discuss methods for establishing and administering policy rules in policy-based access control systems, focusing on policy enforcement techniques. Narouei et al. (2017) are particularly interested in blockchain-based access control solutions, whereas Vincent Hu et al. (2015) is more concerned with policy-based systems.

Savvaidis et al. (2022) argue decentralising access control mechanisms for IoT environments, with a focus on improving security, to address issues such as single points of failure and scalability challenges also discusses specific IoT use cases and implementation scenarios. Shafeeq et al. (2019) argue for the creation of a privacy-aware decentralised access control system to ensure data privacy and security, with the goal of protecting user data while maintaining confidentiality in distributed contexts. Both studies help to advance the development of decentralised access control systems, which aim to increase security and privacy in dispersed environments. They both highlight the challenges and opportunities that come with decentralisation in access control systems. Wang et al. (2022) argue for the implementation of a distributed Attribute-Based Access Control (ABAC) scheme based on blockchain technology to improve access control in distributed systems. Wang also proposes using blockchain, possibly through smart contracts or decentralised consensus mechanisms. In contrast, Zhang et al. (2014) suggest that establishing and analysing Attribute-Based Access Control (ABAC) policies is critical for ensuring effective access control in software systems. Zhang uses formal analytical tools to specify the behavior of ABAC rules, such as formal logic, model verification, and simulation.

Yuta Nakamura et.al. (2018) argue for the applicability of capability-based access control in IoT environments, emphasising its ability to manage access rights based on device and user capabilities while also providing efficient and flexible access control for IoT devices and services. Chen et al. integrate capabilities with blockchain technology to develop a fine-grained and flexible access control model using decentralised consensus processes e.g. smart contracts, with the goal of improving security and manageability in distributed systems.

Novo et al. (2018) advocates for an architecture that blends blockchain and IoT in order to provide a scalable access control system for IoT devices, with a focus on improving security, decentralisation, and transparency. Paillisse et al (2019) advocates for distributed access control using blockchain technology, emphasising decentralisation and safe access management in communication networks and data integrity. Novo et al (2018) and Paillisse et al. (2019) both discusses the integration of blockchain technology for access control purposes, emphasising the necessity of security in access management within their proposed models while also providing insights into harnessing blockchain to improve access control systems.

IoT environments confront a number of security concerns, including unauthorised access by malicious actors and data tampering, which can jeopardise the integrity and confidentiality of critical information. Traditional access control mechanisms may be insufficient to manage these evolving dangers, rendering blockchain an attractive option due to its decentralised and secure nature. Namane et al (2022) delve into the discussion that adopting blockchain for access control in IoT scenarios can be highly effective because of the immutability nature of blockchain which assures that access rights cannot be manipulated, lowering the danger of unauthorised access.

This system adds an extra layer of protection by keeping a transparent and auditable record of access actions. Rinki Singh et al (2023) advocates for using blockchain technology into IoT access control methods because it has the potential to improve security, privacy, and reliability. This is based on blockchain technology's capacity to resist cyber threats while also maintaining data integrity, confidentiality, and availability in IoT scenarios. By incorporating blockchain technology with IoT access control methods, the system can be strengthened against cyber assaults, as the decentralised structure of blockchain makes it more difficult for hackers to change data or gain unauthorised access.

Table 4: Summary of Approaches and Models used by various Researchers

Citation	**RBAC**	**ABAC**	**Decentralised AC**	**PBAC**	**Smart contracts**	**Capability BAC**	**Federated Access control**	**LBC**
R. Ghazal et.al (2020)	✓							
Yanru Chen & Chen et.al (2023)						✓		

Narouei et.al (2017)		✓						
Mutka et.al (2018)						✓		
M.A Habib et.al (2014)	✓							
H. Wang et.al (2022)			✓	✓			✓	
Charalampos Savvaidis et.al (2022)			✓					
Sehrish Shafeeq et.al (2019)			✓					
Kauser et.al (2018)		✓						
Batchu S et.al (2022)					✓			
N. Fotiou et.al (2022)						✓		
Vincent Hu et.al (2015)		✓						
Zhang et.al (2014)				✓				
Ronghua Xu et.al (2018)			✓		✓			
Fernandez et.al (2019)		✓						
J. Hao et.al (2022)					✓			
Xu et.al (2019)			✓					
Yuta Nakamura et.al (2018)						✓		
Yining Hu et.al (2019)					✓			
M. Karimibiuki et.al (2018)				✓				
Manar Abdelhamid et.al (2019)					✓			
Faisal Jamil (2021)					✓			
Qingfeng He (2009)				✓				
Baobao Chaia et.al (2020)					✓			
Novo et.al (2018)							✓	
Paillisse et.al (2019)							✓	
Dukkipati et.al (2018)			✓					
Osterberg et.al (2021)							✓	
Khan et.al (2021)					✓			

I. Riabi et.al (2019)							✓	
Ronghua Xu et.al (2020)	✓	✓	✓				✓	
Damiano Di Francesco Maesa et.al (2017)							✓	
Namane et.al (2022)								✓
Rinki Singh et.al (2023)								✓

RBAC: Role-Based Access Control

PBAC: Policy-Based Access Control

LBC: Lightweight-Blockchain Design

Researchers have explored various models and approaches to implement blockchain-based access control in IoT. Ghazal et al. (2020) and Habib et al. (2014) proposed combining algorithms and semantic technologies for context-aware, adaptable access control judgments. Narouei et al. (2017) proposed an access control architecture combining capability and blockchain technology for detailed permission management. Vincent Hu et al. (2015) focused on policy-based access control systems. Decentralised access control mechanisms are suggested by Savvaidis et al. (2022) and Shafeeq et al. (2019) as a way to enhance security and privacy in Internet of Things environments. A distributed blockchain-based Attribute-Based Access Control (ABAC) strategy for distributed systems is proposed by Wang et al. (2022). For efficient access control in software systems, Zhang et al. (2014) stress the significance of creating and evaluating ABAC policies. The advancement of decentralised access control systems is aided by both investigations.

RQ3: What are the access control standards, frameworks and platforms used to implement the blockchain-based access control model in IoT?

The gathered and examined literature relating to access control standards and frameworks will be discussed in order to address this research topic. The contributions of each publication are presented in Table 5 below. S. Cirani et al. 2015 proposed IoT-OAS an architecture that applies open authorisation as an open protocol built on the representational state transfer (REST) web architecture that enables secure authorisation from third-party apps accessing online services in an easy and standardised manner. However, in 2019 V.A Siris et al creatively introduced open authorisation as a framework that allows limited IoT devices to have delegated authorisation. While utilising the main benefits of blockchains and smart contracts, these models consist of associating payments with authorisation grants, enforcing policies and authorisation information in smart contracts immutably, and providing resilience by executing smart contract code across all blockchain nodes. XACML was recommended by H.F. Atlam et al. as the most effective and suitable policy language for the IoT because it is platform-neutral and offers a distributed, adaptable method for interacting with various access control scenarios. For organisations to avoid fraud or permission breaches, which can lead to major data leaks or privacy violations with strong legal and financial repercussions, access control policy correctness is essential. However, Fatih Turkmen et al proposed the general framework for policy analysis using SMT (Satisfiability Modulo Theories) as the fundamental reasoning process. Not only does the application of SMT enable more in-depth policy research, but it also enhances performance. Campbell et al. (2015) emphasise the relevance and benefits of adopting the SAML 2.0 profile for safe identity management and federated authentication. They present a deeper review of SAML 2.0 and its characteristics, focusing on its employment in diverse authentication scenarios. However, Howlett et al. (2016) argue for the importance of defining specific attributes, profiles, and confirmation methods to ensure seamless integration between RADIUS and SAML protocols, thereby improving interoperability in network access control systems. They delve into technical aspects, detailing the integration of SAML with RADIUS protocols and defining additional attributes and profiles. Both publications help to understand and implement SAML in a variety of scenarios, including generic authentication (Campbell et al.)

and interaction with RADIUS protocols Howlett et al. (2016) with the aim to increase interoperability and consistency in identity management and access control systems. Xu et al. (2019) propose that capability-based access control is helpful in dealing with IoT environments that are dynamic and heterogeneous. They offer BlendCAC as a solution that uses blockchain to provide decentralised administration of access capabilities, enabling safe and granular access controls. Marwan et al. (2020) argue for the use of decentralisation and blockchain to improve the security and trustworthiness of IoT devices deployed in cloud environments. Their strategy entails integrating blockchain for secure data storage, authentication, and device connection in order to mitigate numerous security risks.

Table 5: Summary of Different Standards and Frameworks used by various Researchers

Citation	**OAuth (Open-Authorisation)**	**XACML (Xtensible access control mark-up language)**	**SAML**	**XML**
S. Cirani (2015)	✓			
Hany Atlam et.al (2018)		✓		
Fatih Turkmen et.al (2017)		✓		
V.A Siris et.al (2019)	✓			
Teo Poh Kuang et.al (2010)		✓		
Campbell et. al (2015)			✓	
J. Howlett et.al (2016)			✓	
C. Rupa et.al (2020)			✓	
R. Xu et.al (2018)				✓

Open authorisation is a protocol based on the REST web architecture; it facilitates secure authorisation by third-party applications. In 2019, Siris et al proposed a framework that utilises blockchains and smart contracts to enhance the functionality of restricted IoT devices. XACML is the chosen policy language for IoT because of its platform-neutral characteristics and versatility which was proposed by Hany Atlam et al. 2018. Fatih Turkmen and her colleagues introduced a paradigm for policy analysis that utilises Satisfiability Modulo Theories. This approach allows for thorough study and improved performance.

Y. Huang et al (2019) provides information on protecting smart contracts across the whole software development lifecycle. It goes over methods for spotting, stopping, and addressing security flaws at several phases, like design, development, testing, deployment, and maintenance. Yuanyu Zhang et al. suggests using smart contracts to enable access control in Internet of Things settings that might support the transparent and independent enforcement of access controls through the use of blockchain technology and smart contracts, lessening the need for centralised authorities and improving security and accountability. Both studies share the goal of improving IoT security through the use of smart contracts. Improving security in IoT contexts is critical given the growing number of connected devices and the potential consequences associated with vulnerabilities in these systems. By focusing on smart contracts as a security solution, researchers want to create a robust and automated strategy to mitigating security concerns in IoT environments. Chinmay Saraf, S. S. (2018) provides a comprehensive examination of various blockchain platforms, including Ethereum, Hyperledger Fabric, Corda, and others. It also discusses each platform's features, functionalities, and use cases, highlighting differences in consensus mechanisms, smart contract capabilities, scalability, privacy, and governance. By conducting a thorough examination of these blockchain platforms, the authors hope to provide insights into their strengths, weaknesses, and suitability for various applications, with a focus on Hyperledger fabric because it supports modular

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

architecture, allowing organisations to customise their blockchain networks to meet their specific needs. On the other hand, Mehmood et al (2023) argues that existing consent management systems frequently lack openness, robustness, and user control over their data. It proposes using the Hyperledger Fabric blockchain to overcome these limitations by creating a decentralised, tamper-proof, and auditable platform for maintaining user consent. The approach entails creating smart contracts to encapsulate consent agreements, putting in place access control mechanisms, and using cryptographic approaches to protect data privacy and integrity. The system's strategy attempts to increase user trust and comply with data protection standards.

According to Moin et al. (2019), combining distributed blockchain technology with IoT devices allows organisations to better secure their data and protect their consumers' privacy. This integration can aid in the development of trust among users and stakeholders in the security of IoT systems. Ensuring the security and privacy of data transmitted and stored by IoT devices is critical to protecting sensitive information from unauthorised access or modification. The marriage of blockchain technology and IoT devices provide a powerful alternative for improving data security and privacy in an increasingly linked society. This integration not only safeguards sensitive data, but it also increases trust in the dependability and integrity of IoT devices. Chinmay Saraf, S. S. (2018) offers an extensive compilation of blockchain platforms, accompanied by an overview of their features, applications, and technology. The author delves into several blockchain technologies, including Hyperledger, Corda, and Ethereum. Minango (2023) proposes that an additional source offering real-world illustrations and applications of Corda blockchain technology application in supply chain management should be considered with regard to improving transparency, traceability, and operational efficiency.

Table 6: Summary of Platforms used by various Researchers

Citation	**Smart contracts**	**Hyperledger fabric**	**Ethereum**	**Corda**
Y. Huang et al. (2019)	✓			
Chinmay Saraf et.al (2018)		✓	✓	✓
Paillisse et. al (2019)		✓		
Yuanyu Zhang et. al (2018)	✓			
Sana Moin et.al (2019)			✓	
Mehmood et.al (2023)		✓		
Kuperberg et.al (2020)				✓
Minango et.al (2023)				✓

In their study, Y. Huang et al. emphasise the significance of safeguarding smart contracts during the entire software development process. On the other hand, Yuanyu Zhang et al. proposed the utilisation of smart contracts for IoT access management, aiming to diminish centralised authority and enhance security. In his study, Chinmay Saraf (2018) analyses various blockchain systems such as Ethereum, Hyperledger Fabric, and Corda, with a specific emphasis on the modular architecture of Hyperledger Fabric. Mehmood et al (2023) suggest employing Hyperledger Fabric to establish a decentralised platform that ensures user permission, prevents tampering, and enables auditing. This is achieved through the use of smart contracts, access control mechanisms, and cryptographic methods to safeguard data privacy and integrity. The objective of these studies is to enhance the security of the Internet of Things (IoT) and foster confidence among users.

RQ4: What are the potential applications and use cases where the blockchain-based access control models were adopted in IoT?

Because of blockchain decentralised nature (which helps to eliminate single points of failure and improves the overall security and privacy of IoT networks), the usage of blockchain-based access control models in IoT applications has shown to be adaptable and successful. It has also shown potential in a variety of use cases, including smart homes, healthcare, supply chains, smart cities, transportation, to name a few. The table below analyses the applicability of blockchain-based access control in IoT's.

Zaabar et al. (2021) propose for the use of 'HealthBlock', a blockchain-based system, to improve security and privacy in healthcare data management. It employs blockchain technology to establish a decentralised and tamper-proof ledger for securely storing and exchanging healthcare data; it also includes a full description of its architecture and implementation, emphasising aspects like as encryption, access control, and data sharing protocols. Salonikias et al. 2022 offer a blockchain-based framework that works with existing healthcare systems to increase data integrity, interoperability, and security. The framework is intended to interface smoothly with existing healthcare systems used by hospitals, clinics, and other providers. This connectivity means that the blockchain-based solution may work in tandem with the existing infrastructure without requiring a whole modification. In a different light. Ray et al. (2021) highlighted the potential of blockchain technology in IoT-based healthcare to address critical challenges such as data security, interoperability, and transparency. Their paper provides a comprehensive examination of the background, consensus methods, blockchain platforms, and real-world use cases within the healthcare domain. On the other hand, Azbeg et al. (2022) propose a taxonomy study aimed at systematically organising and classifying various applications of IoT and blockchain in healthcare. Their focus is on providing a structured overview of use cases and benefits to enhance understanding and facilitate future research and development in this field. Reddy et al. (2022) address the use of blockchain for financial applications in conjunction with IoT, emphasising the possible benefits and problems of adopting this technology combination, with a focus on practical factors and technical concerns. Ahamad et al. (2022) investigates the relevance of blockchain and IoT in securing financial transactions in the bitcoin market. This study delves into specific use cases, security techniques, and regulatory factors related to bitcoin transactions. Both articles emphasised the need of data security, transparency, and trust in financial transactions powered by blockchain and IoT technology. They may, however, differ in their specific techniques, use cases, and analytical depth. Zheng et al. (2022) explore the use of blockchain for enterprise credit information exchange in supply chain finance. They emphasised blockchain's role in increasing openness, trust, and efficiency in financial transactions inside supply chain networks. Agrawal et al. (2019) study the use of blockchain in both IoT and financial applications. While they may mention supply chain finance, their paper is anticipated to provide a more comprehensive assessment of blockchain's possibilities across industries and its interaction with IoT technologies. Both articles emphasised the benefits of blockchain technology, including increased security, transparency, and decentralisation. However, variances may exist in their specific use cases, depth of analysis, and emphasis on certain applications within finance and supply chain management.

Jabbar et al. (2022) investigated how blockchain technology is implemented in transportation systems, which involve supply chain management, vehicle tracking, toll collecting, ride-sharing platforms, and safe data sharing among transportation players. Understanding these applications helps shed light on the various ways blockchain is altering the transportation sector. Jabbar et al. sought to highlight potential benefits for stakeholders. These advantages include increased data security, lower transaction costs, improved product traceability, increased logistical efficiency, and increased confidence among transportation ecosystem members. Abbas et al. (2021) investigate how technology might be used to safeguard transport systems in smart cities. Transport systems in smart cities are critical to guaranteeing efficient mobility and connection. However, these systems are vulnerable to cyber assaults, thus security is a primary responsibility. Abbas et al (2021). investigate particular application cases in which blockchain and IoT might be used to improve the security of urban transport networks, this includes scenarios like secure data sharing among vehicles, infrastructure, and traffic management systems.

Abderahman Rejeb et al. (2019) investigate the use of IoT and blockchain technology in supply chain management, focusing on how this combination improves transparency, traceability, and efficiency. This paper discusses use cases such as tracking the temperature of perishable goods during transportation and monitoring the condition of sensitive products, as well as benefits such as improved inventory management, reduced fraud and counterfeiting, increased trust among partners, and optimised logistics via data-driven decision-making. On the other hand, S. Aich et al' (2019) review focuses on the benefits of merging IoT and blockchain, specifically in supply chain management across different industries. They delve into case studies and practical applications to demonstrate how this integration can bring about positive outcomes for supply chain. One of the review's primary benefits is increased supply chain transparency here, companies can track items at every level of the supply chain using IoT sensors and blockchain technology, giving them visibility into the entire process. On the other hand, Sana Moin et al. (2019) investigates the security issues of IoT systems using distributed blockchain technology. This article examines the security requirements of IoT devices, identifies potential vulnerabilities, and suggests methods for mitigating security risks. It emphasises the importance of secure communication protocols and data encryption solutions for protecting IoT devices from cyber-attacks.

Table 7: Summary of Application and Use cases Implemented by various Researchers

Citation	**Healthcare**	**Finance**	**Transportation**	**Supply Chain**	**Smart Home/City**
Rateb Jabbar et.al (2022)			✓		
Abbas et. al (2021)			✓		
Beesem Zaabar et. al (2021)	✓				
S. Aich et. al (2019)				✓	
Sana Moin et al (2019)					✓
Salonikias et al. (2022)	✓				
P. P. Ray et. al (2021)	✓				
Abderahman Rejeb (2019)				✓	
K. Azbeg et. al (2022)	✓				
U. Agrawal et. al (2019)		✓			
Pajarnay Sharma et. al (2021)					✓

Zaabar et al. (2021) propose 'Health Block', a blockchain-based system, to enhance security and privacy in healthcare data management. The system uses a decentralised ledger for secure storage and exchange of data, while Salonikias et al. (2022) propose a blockchain-based framework that integrates with existing healthcare systems for enhanced data integrity and interoperability. Ray et al. (2021) explores the use of blockchain technology in IoT-based healthcare to tackle data security, interoperability, and transparency, while Azbeg et al. (2022) propose a taxonomy study to categorise IoT and blockchain applications, enhancing understanding and facilitating future research.

RQ5: What are the challenges and future directions in blockchain-based access control models: a table stating the challenges and future directions

Blockchain-based access control models show great promise for improving security, transparency, and decentralisation in a variety of fields. However, they confront a number of problems as well as chances for future growth. The table below highlights the challenges and future directions.

Shantanu Pal et al. (2022) analyses several options, such as smart contracts and decentralised identity management, noting the benefits and challenges. It also investigates emerging trends in blockchain technology integration with IoT devices, highlighting the significance of secure access control techniques in ensuring the integrity and privacy of IoT systems.

S. Rouhani et al. examine the problems and solutions to blockchain-based access control, such as securely integrating off-chain storage, resolving blockchain vulnerabilities, balancing transaction transparency with privacy, improving performance, and transitioning access control methods to dynamic approaches. Using trusted hardware, increasing smart contract security, hybrid centralised-decentralised solutions for privacy, optimising blockchain performance, and investigating dynamic access control integration with blockchain are all possible answers.

Muneeb Hassan et al. (2019) discusses decentralisation in Industrial IoT, Internet of Farming Things, Smart Cities, and Mobile Crowd Sensing improves performance while raising privacy concerns, necessitating lightweight blockchain protocols, encryption methods, and privacy-enhancing techniques such as anonymisation and differential privacy. Bharat Bhushan et al. (2020) investigates the integration of blockchain technology with IoT devices, emphasising the importance of safe and decentralised data management. It also discusses numerous use cases, technical considerations, and potential benefits of IoT systems, as well as addressing associated obstacles and detailing future research and development opportunities.

Malak Alamri et al. (2019) and Abdurrashid Ibrahim Sanka et al. (2021) identify numerous issues that blockchain technology faces when used on the Internet of Things (IoT). Scalability, interoperability, security, privacy, and energy efficiency are all issues that must be addressed. Both papers also identify several opportunities for improvement and development in the combination of blockchain and IoT. One critical component is improving consensus mechanisms in blockchain networks to make them more efficient and scalable. This entails determining how to obtain a consensus on the validity of transactions without using excessive computer resources. Another key direction is to improve data privacy in blockchain systems, particularly in IoT situations where data security is critical.

Table 8: Summary of Challenges and Future Trends

Citation	Challenges and Future Direction	Description of Challenges and Future Direction
Shantanu pal et al. (2022)	Challenges • Scalability • Interoperability • Security and Privacy Future Direction • Lightweight Blockchain protocol • Hybrid blockchain architecture • Advance consensus mechanism	The increasing number of IoT devices challenges blockchain networks, increasing transaction and data management burdens and performance issues. Standardisation and interoperability are crucial for seamless integration. Future studies will focus on creating efficient protocols for IoT settings, hybrid blockchain designs, and innovative consensus techniques like Proof of Work or Proof of Stake.
Bharat Bhushan et al. (2020)	Challenges • Resource constraint • Security threat • Regulatory Compliance	The constrained CPU capability, memory, and battery life of IoT devices provide difficulties in deploying blockchain protocols, making them vulnerable to security threats. Devices that have been compromised have the potential to undermine the overall integrity and security of the entire Blockchain of Things system. The continuous regulatory changes impede the worldwide

	Future Direction • Standardisation • Enhanced security measure • AI and Machine learning	deployment of BIoT (Blockchain Internet of Things) systems.
Muneeb Hassan et al. (2019)	Challenges • Latency • Security vulnerability • Privacy reservation Future Direction • Edge and Fog computing • Standardisation	Blockchain consensus algorithms can cause delays and security risks in IoT applications. Balancing transparency and privacy are complex. Edge and fog computing can reduce latency and improve performance. Standardisation and uniform protocols ensure seamless communication.
Malak Alamri et al. (2019)	Challenges • Energy consumption • Scalability Future Direction • Developing scalable solutions • Developing energy efficient solutions	Blockchain operations, like Proof of Work, consume significant energy, making IoT devices inefficient. Existing blockchain technologies like Bitcoin and Ethereum face scalability challenges due to the massive volume of transactions. Research focuses on developing scalable blockchain protocols for efficient transaction processing and energy efficiency, using consensus mechanisms like Proof of Authority and Proof of History.
Hany Atlam et. al (2018)	Challenges • Complexity of IoT environment • Dynamic nature of IoT devices • Policy management Future Direction • Context-aware access control • Decentralised access control • Enhanced security features	Efficient access control policies in IoT environments are challenging due to diverse devices and dynamic attributes. Context-aware policies, decentralised technologies like blockchain, and advanced measures like encryption and anomaly detection improve flexibility and effectiveness.

Abdurrashid Ibrahim Sanka (2021)	Challenges • Privacy and confidentiality • Complexity and usability Future Direction • Privacy enhancing techniques • User friendly application	Blockchain technology faces challenges in maintaining privacy and transparency due to its complexity and lack of user experience. To improve security and accessibility, privacy-preserving methods like zero-knowledge proofs and homomorphic encryption can be used. This can also enhance user experience and facilitate wider adoption.

CONCLUSION

This study undertook a thorough investigation of the developing field of blockchain-based access control, particularly in Internet of Things applications. Blockchain-based access control on the Internet of Things is the application of blockchain technology to manage and enforce access control policies for IoT devices and data. This method improves security, privacy, and accountability in IoT environments by utilising the decentralised and immutable features of blockchain technology. Within this system, access to specific data is determined by rules and regulations. These rules and regulations are then saved on the blockchain to guarantee transparency and resistance to tampering. Smart contracts are often used to automate access control decisions, enabling conditional access based on predefined rules. Each access request and permission change is recorded as a transaction on the blockchain, providing an auditable trail of access activities.

Traditional centralised access control systems are vulnerable to a single point of failure, such as a central server, which can compromise the whole security of the system. In contrast, blockchain-based access control in IoT operates through decentralised decision-making, eliminating the risk of a central authority compromise. Each node in the blockchain network maintains a ledger copy, ensuring redundancy and fault tolerance. Blockchain technology provides resilience against unauthorised tampering by recording access control decisions on a distributed ledger in a tamper-evident manner. Once decisions are on the blockchain, altering or deleting them without detection becomes extremely challenging thus enhancing security in IoT access control environments. Hackers would need to compromise a significant portion of the blockchain network to alter access control policies, a highly impractical and resource-intensive task. This heightened security lowers the chances of unauthorised access or data breaches in IoT environments.

Nevertheless, the implementation of blockchain-based access control in IoT is not without its obstacles. These include scalability issues due to the large number of IoT devices and the need for efficient consensus mechanisms to handle high transaction volumes. The consensus method is crucial for guaranteeing the security and integrity of the system, efficient consensus mechanisms are essential to handle the increased transaction volumes in IoT environments without compromising speed or security.

Additionally, interoperability between various blockchain platforms and IoT devices is essential for creating a cohesive and interconnected ecosystem. Lack of interoperability can lead to fragmentation, data silos, and inefficiencies in communication between devices and blockchain networks. Overcoming interoperability challenges requires standardisation efforts, development of protocols for seamless integration, and compatibility testing to ensure smooth interactions between diverse technologies in the IoT environment.

REFERENCES

1. Abbas, T.R.M.E.I.A. and El-Alfy, A.A., 2021. Convergence of blockchain and IoT for secure transportation systems in smart cities. Security and Communication Networks, 2021, Article ID 5597679. Available at: https://www.hindawi.com/journals/scn/2021/5597679/
2. Abderahman Rejeb, J.G.K. a. T, H., 2019. Leveraging the Internet of Things and blockchain technology in supply chain management. Future Internet, 11(7), p.161.

3. Abdurrashid Ibrahim Sanka, M. I. I. H. R. C. C. C., 2021. A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research. Computer Communications, Volume 169, pp. 179-201.
4. Alanda, A., 2024. Web Application Penetration Testing Using SQL.
5. Alharby, M. a. v. M. A., 2017. Blockchain-based Smart Contracts: A systematic mapping study. Available at: https://arxiv.org/abs/1710.06372 [Accessed 22 Feb 2024].
6. Dorri, A., S. S. K. R J., 2017. Blockchain for IoT security and privacy: the case study of a smart home. In: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). Kona, HI, USA, 13–17 March 2017. Piscataway, NJ: IEEE, pp.618–623.
7. Alfaw, A.H. W. E. M. S. S., 2022. Blockchain Vulnerabilities and Recent Security Challenges: a review. International Journal of Computer Applications, 25 Oct, pp. 780-786.
8. Baobao Chaia, B. Y. D. a. J. y., 2020. A Smart Contract-Based Fine-Grained Access Control for. Elsevier, Shandong Academy of Sciences, Jinan 250014, China.
9. Batchu S, P. K. H. O. M. A. A. A. H. H. J. A. T. S. P. U., 2022. Using Ethereum Smart Contracts to Store and Share COVID-19 Patient Data. Cureus, Volume 14.
10. Beesem zaabar, O. C. F. J. M. A. M. a., 2021. HealthBlock: A secure blockchain-based healthcare data management system. Computer Networks, pp. pp 1-16.
11. Bharat Bhushan, C. S. P. S. a. A. K., 2020. Unification of Blockchain and Internet of Things (BIoT): requirements working model, challenges and future directions. Wireless Networks, Volume 27, pp. pp 55-90.
12. C. Rupa, R. P. F. A.-T. a. L. M., 2020. Enhancing the Access Privacy of IDaaS System Using SAML Protocol in Fog Computing. IEEE Access, Volume Vol. 8, pp. pp. 168793-168801.
13. C. Wiraatmaja, Y. Z. M. S. a. S. K., 2021. Cost-Efficient Blockchain-Based Access Control for the Internet of Things,. Madrid, Spain, IEEE.
14. Campbell, B. M. C. a. J. M., 2015. Security Assertion Markup Language (SAML) 2.0 Profile. Internet Engineering Task Force (IETF), Issue ISSN: 2070-1721, pp. 1-15.
15. Charalampos Savvaidis, C. P. G. S. A., 2022. Decentralising Access Control for IoT Environment, Thessaloniki, Greece: IEEE.
16. Chiara Addis, M. K., 2020. General Data Protection Regulation (GDPR), Artificial Intelligence (AI) and UK Organisations: A year of implementation of GDPR. Salford, Association for Information Systems electronic library (AISeL).
17. Chinmay Saraf, S. S., 2018. Blockchain Platforms: A Compendium. Bangkok Thailand, IEEE International Conference on Innovative Research and Development (ICIRD).
18. Damiano Di Francesco Maesa, P. M. L. R., 2017. Blockchain Based Access Control. International Conference on Distributed Applications and Interoperable Systems (DAIS), 17th(1007/978-3-319-59665-5_15f), pp. 206-220.
19. Damiano Di Francesco Maesa, P. M. L. R., 2017. Blockchain Based Access Control. [Online] Available at: https://typeset.io/papers/blockchain-based-access-control-axixd50sjt[Accessed 22 Jan 2024].
20. Desprats, R. L. a. T., n.d. An Extension of XACML to Improve Performance of Decision Making Processes When Dealing with Stable Conditions.
21. Dukkipati, C. Z. Y. a. C. L., 2018. Decentralised, BlockChain Based Access Control Framework for the Heterogeneous Internet of Things. 3rd ACM Workshop on Attribute-Based Access Control..
22. Dylan Yaga, N. R. K. S. P. M., 2018. Blockchain Technology Overview. s.l.:National Institute of Standards and Technology Internal Report 8202.
23. E. Politou, F. C. E. A. a. C. P., 2021. Blockchain Mutability: Challenges and Proposed Solutions. Transactions on Emerging Topics in Computing, vol. 9(no. 4), pp. 1972-1986.
24. Ebtihal Abdulrahman, S. A. a. A. C., 2021. Blockchain-Based Access Control for the Internet of Things: A Survey. Jeddah, Saudi Arabia, Researchgate.
25. F. Rahman, C. T. a. F. N.-A., 2023. A Novel Approach to Enhance Blockchain Scalability,. 5th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Issue 10.1109/BRAINS59668.2023.10317052., pp. pp. 1-2, doi.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

26. Faisal Jamil, H. K. K. S. K.,. D.-H. K., 2021. Sensors. [Online] Available at: https://pubmed.ncbi.nlm.nih.gov/33652773/[Accessed 24 April 2024].
27. Fatih Turkmen, J. d. H. S. R. a. N. Z., 2017. Analysis of XACML Policies with SMT. Lecture notes in computer science.
28. Feilong Lin, Z. Z. Z. H. C. T. H. P. a. Z. C., 2018. A Sustainable Reward Mechanism for Block Mining in PoW-based Blockchain. Zhejiang, P. R. China, IEEE.
29. Fernández, M. M. I. a. T. B., 2019. Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy.. s.l., ACM Digital library.
30. Gaétan de Rassenfosse, K. H., 2020. Decentralising the Patent System. Social Science Research Network.
31. Gate, R., 2022. Traditional and Hybrid Access Control Models: A Detailed Survey. Security and Communication Networks , Feb, p. 3.
32. Georgios Lampropoulos, K. S. a. T. A., 2018. Internet of Things (IoT) in Industry: Contemporary Application Domains,Innovative Technologies and Intelligent Manufacturing. International Journal ofAdvances in Scientific Research and Engineering, 4(10), pp. 109-114.
33. Guy Zyskind, O. N. A. P., 2015. Decentralising Privacy: Using Blockchain to Protect. Cambridge, Massachusetts, IEEE.
34. H. Wang, Z. R. T. Z. a. Q. W., 2022. A distributed ABAC access control scheme based on blockchain. 2022 2nd International Conference on Computer Science and Blockchain (CCSB), pp. pp. 19-25.
35. Hany F. Atlam, A. A. M. O. A. G. B. W., 2018. Blockchain with Internet of Things: Benefits, Challenges, and Future Directions. I.J. Intelligent Systems and Applications., Volume 6, pp. 40-48.
36. Hany F. Atlam, M. O. A. A. A. R. J. W. G. B. W., 2018. XACML for Building Access Control Policies in Internet of Things. s.l., SCITEPRESS – Science and Technology Publications.
37. Hui Lin, Q. H. J. H. a. X. W., 2023. Blockchain-based Data Access Security Solutions. Fuzhou, China., IEEE.
38. I. Riabi, Y. D. H. K. B. A. a. K. Z., 2019. A Blockchain based access control for IoT. 15th International Wireless Communications & Mobile Computing Conference, pp. pp. 2086-2091.
39. J. Hao, C. H. W. T. Y. Z. a. S. Y., 2022. Smart Contract-Based Access Control Through Off-Chain Signature and On-Chain Evaluation. IEEE Transactions on Circuits and Systems II, vol. 69(no 4), pp. pp. 2221-2225.
40. J. Howlett, S. H. a. A. P.-M., 2016. A RADIUS Attribute, Binding, Profiles, Name Identifier Format, and Confirmation Methods for SAML. ABFAB Internet Draft, pp. 1-99.
41. J. Leng, M. Z. J. L. Z. Y. H. a. Y. B., 2022. Blockchain Security: A Survey of Techniques and Research Directions. In: n. 4. vol. 15, ed. in IEEE Transactions on Services Computing. vol. 15, no. 4, pp. 2490-2510 ed. s.l.:IEEE, pp. PP. 2490-2510.
42. JASON PAUL CRUZ, Y. K., 2015. The Bitcoin Network as Platform for Trans-Organisational Attribute. Osaka, Japan, Researchgate.
43. Jiménez, L. P., 2022. Internet of Things (IoT): A Beginner’s Guide. [Online] Available at: https://www.salvosoftware.com/what-is-iot/ [Accessed 16 April 2024].
44. João Pedro Dias, H. S. F. Â. M., 2018. A Blockchain-Based Scheme for Access Control in e-Health Scenarios. Porto: Soft Computing and Pattern Recognition.
45. Julien Polge, J. R. Y. L. T., n.d. Permissioned blockchain frameworks in the industry: A comparison. [Online]Available at: https://www.sciencedirect.com/science/article/pii/S2405959520301909 [Accessed 23 Feb 2024].
46. K. Azbeg, O. O. S. A. L. F., 2022. A Taxonomic Review of the Use of IoT and Blockchain in Healthcare. IRBM, Volume 43, pp. pp 511-519.
47. Kauser, S. R. A. K. A. a. A. T., 2018. Advances in Intelligent Systems and Computing. Volume 10, p. pp. 385–393.
48. Khalid Zaman Bijon, R. K. R. S., 2013. Constraints Specification in Attribute Based Access Control. Univ of Texas at San Antonio: s.n.
49. Khan, S. L. F. G.-G. C. B. E. a. B.-H. A., 2021. Blockchain smart contracts: Applications, challenges, and future. Peer-to-Peer Networking and Applications , pp. pp 2901-2925.

50. K, L., 2022. Wireless Communications and Mobile Computing. [Online] Available at: https://www.hindawi.com/journals/wcmc/2022/4393314/
51. Kuperberg, M., 2020. Blockchain-Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective. IEEE Transactions on Engineering Management, 67(4), pp. pp. 1008-1027.
52. Luciano, F., 2010. Ethics after the Information revolution.. s.l.:Cambridge University press.
53. M. A. Habib, N. M. M. S. M. U. A. U. A. a. C. M. N. F., 2014. Permission based implementation of Dynamic Separation of Duty (DSD) in Role based Access Control (RBAC). Gold Coast, QLD, Australia, IEEE, pp. 1-10.
54. M. Karimibiuki, E. A. K. P. a. A. I., 2018. DynPolAC: Dynamic Policy-Based Access Control for IoT Systems. 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC), pp. pp. 161-170.
55. M. Madine, K. S. R. J. Y. A.-H. J. A. a. I. Y., 2021. Application-Level Interoperability for Blockchain Networks. s.l., IEEE Access, vol. 9, pp. 87777-87791, 2021,.
56. Madakam, S. R. R. a. T. S., 2015. Internet of Things (IoT): A Literature Review. Journal of Computer and Communications , Vol.3 (No.5).
57. Madhuri B. Thorat, M. S. P., 2022. Decentralization using Blockchain as a Service.. Journal For Research in Applied Science and Engineering Technology, Issue 2321-9653.
58. Malak Alamri, N. J. a. M. H., 2019. Blockchain for Internet of Things (IoT) Research Issues Challenges & Future Directions: A Review. IJCSNS International Journal of Computer Science and Network Security, 19(5), pp. pp 244-256.
59. Manar Abdelhamid, G. H., 2019. Blockchain and Smart Contracts. 8th International Conference on Software and Information Engineering, p. Pages 91–95.
60. Manisha G. Gedam, S. K. W. K. D., 2022. An Analytical Review on Challenges and Solutions for Secure Data Access through Blockchain-Based IoT. International journal of innovations in engineering and science, 7(8), pp. 110-116.
61. Mehmood, F. K. U. a. K. S., 2023. Consent Management System Based on User Data Security and Privacy Using Hyperledger Fabric Blockchain. Proceedings of the 6th International Conference on Information Technologies and Electrical Engineering, Volume 4, pp. pp 447-454.
62. Minango, J. Z. M. P. P. W. T. C. a. R. M., 2023. Proof of Concepts of Corda Blockchain Technology Applied on the Supply Chain Area. Trends in Artificial Intelligence and Computer Engineering., Volume 2, p. pp. 619–631.
63. Miodrag J. Mihaljevi, M. K. D. U. L. W. a. S. X., 2023. An Approach for Blockchain and Symmetric Keys Broadcast Encryption Based Access Control in IoT. 15(299), p.18.
64. Mirei Yutaka, Y. Z. M. S. a. S. K., 2018. Using Ethereum Blockchain for Distributed Attribute-Based Access Control. Ikoma, Nara 630-0192, Japan., IEEE.
65. Muneeb Hassan, M. H. R. a. J. C., 2019. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. Future Generation Computer Systems, Volume 97, p. 512–529.
66. Mutka, T. L. a. M. W., 2018. A Privacy Preserving Access Control Framework Based on Blockchain for Pervasive Environments. Taormina, Italy., IEEE, pp. 57-64.
67. N. Fotiou, V. A. S. G. C. P. Y. K. a. D. L., 2022. Capabilities-based access control for IoT devices using Verifiable Credentials. 2022 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, pp. pp. 222-228.
68. Namane, S. a. B. D. I., 2022. Blockchain-Based Access Control Techniques for IoT Applications. s.l., Multidisciplinary Digital Publishing Institute.
69. Nanaan wu, L. X. L. Z., 2023. A blockchain based access control scheme with hidden policy and attributes. Future Generation Computer Systems, Issue 141, pp. 186-196.
70. Narouei, M. K. H. T. H. P. N. a. N. R., 2017. Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies. pp. 1-12.
71. Novo, O., 2018. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. IEEE Internet of Things Journal, Volume 5, pp. pp. 1184-1195.

72. Óscar Mortágua Pereira, V. S. D. D. R. a. R. L. A., 2017. The XACML Standard Addressing Architectural and Security Aspects. 2nd International Conference on Internet of Things, Big Data and Security, pp. 189-197.
73. Österberg, I. B. a. P., 2021. A Review of Distributed Access Control for Blockchain Systems Towards Securing the Internet of Things. Göteborg, Sweden, IEEE, pp. pp. 5428-5441.
74. P. P. Ray, D. D. K. S. a. N. K., 2021. Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases. in IEEE Systems Journal, Volume 15, pp. pp. 85-94.
75. Pahontu, B.-I., Arsene, D.-A. & Mocanu, M., 2020. A survey about industries that blockchain can transform. Bucharest, Romania, IEEE.
76. Paillisse, J., 2019. Distributed Access Control with Blockchain ICC 2019 - 2019 IEEE International Conference on Communications (ICC). Shangai, China, IEEE.
77. Pajarnay Sharma, S. J. S. G. a. V. C., 2021. Role of machine learning and deep learning in securing 5G-driven industrial. AdHoc Networks, Volume 7, pp. pp 1-24.
78. Pešić, S. R. M. I. M. T. M. I. O. B. D., 2019. Hyperledger Fabric Blockchain as a Service for the IoT: Proof of Concept.. s.l., SpringerLink.
79. Poet, M. S. F. a. R., 2013. Dynamic Identity Federation Using Security. Policies and research in identity management, p. pp 131–146.
80. Qingfeng He, A. I. A., 2009. Requirements-based Access Control Analysis and Policy Specification (ReCAPS). 51(6), pp. 993-1009.
81. Qingsu He, Y. X. Z. L. J. H., 2018. Trust and Privacy in Blockchain Enabled Internet of Things. International Journal of Distributed sensor network, Volume Vol. 14(11), p. 12.
82. R. Ghazal, A. K. M. N. Q. B. R. A. R. S. a. H. A., 2020. Intelligent Role-Based Access Control Model and Framework Using Semantic Business Roles in Multi-Domain Environments, Volume Vol. 8, pp. pp. 12253-12267.
83. R. Xu, Y. C. E. B. a. G. C., 2018. BlendCAC: A BLockchain-Enabled Decentralized Capability-Based Access Control for IoTs. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. pp. 1027-1034.
84. Rateb Jabbar, E. D. A. B. S. M. K. N. F., 2022. Blockchain Technology for Intelligent Transportation Systems. A Systematic Literature Review," in IEEE, Volume 10, pp. pp. 20995-21031.
85. Rinki Singh, D. K. a. D. K. S., 2023. Blockchain-enabled access control to prevent cyber attacks in IoT: Systematic literature review, New Delhi, India: s.n.
86. Ronghua Xu, Y. C. E. B., 2020. Decentralised Access Control for IoT Based on Blockchain and Smart Contract. [Online] Available at: https://typeset.io/papers/decentralized-access-control-for-iot-based-on-blockchain-and-5211x790og [Accessed 22 Jan 2024].
87. Ronghua Xu, Y. C. E. B. a. G. C., 2018. A Smart Contract Enabled Decentralised Capability-Based Access Control Mechanism for IoT. Volume 7.
88. S. Aich, S. C. M. S. H. -i. L. a. H. -C. K., 2019. A Review on Benefits of IoT Integrated Blockchain based Supply Chain Management Implementations across Different Sectors with Case Study. PyeongChang, Korea (South), IEEE.
89. S. Cirani, M. P. P. G. L. V. a. G. F., 2015. IoT OAS: An OAuth-Based Authorisation Service Architecture for Secure Services in IoT Scenarios. IEEE Sensors Journal, Volume 2, pp. 1224-1234.
90. S. De Capitani di Vimercati, S. F. P. S., 2008. Recent advances in access control. 01 Jan, pp. 1-26.
91. S. Sun, Y. L. a. G. G., 2019. A Privacy-Preserving and Robust Reputation System Based on Blockchain. Xiamen, China, IEEE.
92. Salonikias, S. K. M. M. T. a. M. I., 2022. Salonikias, S., Khair, M., Mastoras, T. and Mavridis, I.. [Online] Available at: https://www.mdpi.com/2079-9292/11/17/2652
93. Sana Moin, A. K. Z. S. K. S. E. A. M. I., 2019. Securing IoTs in distributed blockchain: Analysis, requirements and open issues. Future Generation Computer Systems, Volume 100, pp. 325-343.
94. Sanjeev Kumar Dwivedi, P. R. C. K. S. A. a. R. A., 2021. Blockchain-Based Internet of Things and Industrial IoT: A. Security and Communication Networks, 27 Aug, p. 21.
95. Sara Rouhani, R. B. R. S. C. R. D., 2021. Distributed attribute-based access control system. Saskatchewan, Saskatoon, SK, S7N5C9, Canada, Springerlink.

96. Sara Rouhani, R. D., 2019. Blockchain based access control systems: State of the art and. [Online] Available at: https://allquantor.at/blockchainbib/pdf/rouhani2019blockchain.pdf[Accessed 22 Jan 2024].
97. Sara Rouhani, R. D., 2019. Blockchain based access control systems: State of the art and challenges. [Online] Available at: https://allquantor.at/blockchainbib/pdf/rouhani2019blockchain.pdf
98. Sarmah, S. S., 2018. Understanding Blockchain Technology, Business Intelligence Architect, Alpha Clinical Systems, USA: Computer Science and Engineering.
99. Sehrish Shafeeq, M. A. A. K., 2019. Privacy aware decentralized access control system. Islamabad, Elsevier.
100. Shantanu pal, A. D. R. J., 2022. Blockchain for IoT access control: Recent trends and future research. Journal of Network and Computer Applications, 203(103371).
101. SHENG DING, J. C. C. L., 2019. A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT. Xidian University, Xi'an 710071, China, IEEE.
102.
103. Sheping Zhai, Y. Y. J. L., 2019. Research on the Application of Cryptography on the Blockchain. Journal of Physics: Conf. Series 1168, 2714(1742-6596).
104. Teo Poh Kuang, H. I. N. I. U. a. F. S., 2010. Security Extensible Access Control Markup Language Policy Integration Based on Role-Based Access Control Model in Healthcare Collaborative Environments. American Journal of Economics and Business Administration, Volume 3, pp. pp 100-111.
105. U. Agrawal, I. K. a. P. P. C., 2019. A Role of Blockchain in IoT and Financial Applications. Vellore, India, IEEE.
106. Uchi Ugobame Uchibeke, K. A. S. S. H. K. R. D., 2018. Blockchain Access Control Ecosystem for Big Data Security. 1st July, pp. pp 1373-1378.
107. V. A. Siris, D. D. N. F. S. V. a. G. C. P., 2019. OAuth 2.0 meets Blockchain for Authorisation in Constrained IoT Environments. 5th World Forum on Internet of Things (WF-IoT), Volume 3, pp. 364-367.
108. Vincent C. Hu, D. F. F. D. R. K., 2006. Assessment of Access Control Systems, Gaithersburg: National Institute of Standards and Technology Interagency Report 7316.
109. Vincent C. Hu, D. F. F. D. R. K., 2006. Assessment of Access Control Systems, Gaithersburg, MD 20899-8930 : NISTIR 7316.
110. Vincent Hu, D. F. F. D. R. K., 2015. Implementing and Managing Policy Rules in policy based access control, University of Texas at Arlington: Researchgate.
111. Xu, L. M. I. I. S. a. N. N., 2019. Blockchain-based access control for enterprise blockchain applications. International Journal of Network Management.
112. Y. Huang, Y. B. R. L. J. L. Z. a. P. S., 2019. Smart Contract Security: A Software Lifecycle Perspective. IEEE Access, Volume 7, pp. 150184-150202, 2019.
113. Yan Zhu, Y. Q. G. G. a. S. Y., 2018. TBAC: Transaction-Based Access Control on Blockchain for Resource Sharing with Cryptographically Decentralized Authorization. Beijing, IEEE.
114. Yang Lu, Y. L. Y. L., 2019. The blockchain: State-of-the-art and research challenges. Journal of Industrial Information Integration , Volume 15, pp. 80-90.
115. Yanru Chen, L. T. B. L. Y. L. B. X. & Chen, L. y., 2023. Capability and Blockchain-Based Fine-Grained and Flexible Access Control Model. 37(6), pp. 197-205.
116. Yining Hu, M. L. A. M. K. T. G. J. A. S., 2019. arxiv.org. [Online] Available at: Hu, Y., Liyanage, M., Mansoor, A., Thilakarathna, K., Jourjon, G. and Seneviratne, A. (2019) Blockchain-based Smart Conhttps://arxiv.org/abs/1810.04699 [Accessed 24 April 2024].
117. Yuanyu Zhang, S. K. Y. S., 2018. Smart Contract-Based Access Control for the Internet of things. IEEE Internet of things journal.
118. Yuta Nakamura, Y. Z. M. S. a. S. K., 2018. Capability-Based Access Control for the Internet of things. Ikoma, Nara Japan., IEEE, p. 12.
119. Zhang, D. X. a. Y., 2014. Specification and Analysis of Attribute-Based Access Control Policies. IEEE Eighth International Conference on Software Security and Reliability-Companion, San Francisco, pp. pp. 41-49.