Computer Networks 235 (2023) 109994

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Survey paper

A survey on blockchain envisioned attribute based access control for internet of things: Overview, comparative analysis, and open research challenges

Syed Sajid Ullah *, Vladimir Oleshchuk, Harsha S. Gardiyawasam Pussewalage

Department of Information and Communication Technology, University of Agder, Grimstad, N-4898, Norway

ARTICLE INFO

Keywords:
Blockchain
Internet of things (IoT)
Access control
Attribute based access control
Networking
Security

ABSTRACT

The Internet of Things (IoT) network is rapidly expanding due to sudden technological advancements, which enable objects to become intelligent and contribute to the network. Before permitting a newly added IoT device to communicate with the network, it is essential to provide access and authenticate the device's legitimacy by ensuring that it has not been tampered. Recently, blockchain technology has been integrated into Attribute Based Access Control (ABAC) protocols to supply a more robust security mechanism for access control in IoT. The IoT and blockchain-based ABAC serve as the foundation of this survey, offering a comprehensive introduction to both topics. Additionally, several security concerns and vulnerabilities associated with Blockchain Envisioned ABAC (BE-ABAC) are presented. A Comparison with related surveys has also been made. Besides, we also present a comparative analysis based on evaluation based on Distance from Average Solution (EDAS) to rank the best schemes among the suggested BE-ABAC schemes. In conclusion, we discuss some open research challenges in an IoT network that uses blockchain to manage access control.

1. Introduction

The Internet of Things (IoT) has been a topic of great interest to both academics and industry professionals in recent years [1]. It encompasses a network of physical devices, such as smart appliances, cars, and other gadgets, which can communicate and exchange data with each other via the Internet. The purpose of IoT is to establish an interconnected system where devices can function independently, resulting in smoother automation and the ability to gather and analyze data on a massive scale. The potential of IoT to transform our way of life and work has made it one of the most promising and extensively researched technologies of our time [2]. It is projected that by 2030, there will be approximately 500 billion of these devices in use [3]. The IoT is a rapidly developing technology currently being utilized extensively in various fields, including intelligent transportation, home automation, innovative healthcare, drones etc. Concerns regarding the informational safety of IoT devices are receiving much attention in both academic circles and the business world. Access Control (AC) is a crucial technology to secure the data stored on IoT devices. The main objective of access control is to regulate the extent to which subjects, such as users, processes, and devices, are allowed to access specific resources or objects. The objective is to achieve a state of equilibrium in which the required access is granted to subjects so that they may carry out their responsibilities efficiently while, at the same time, the parameters of legal authorization are adhered to, and the information's integrity and confidentiality are preserved. The data that is saved on Internet of Things devices can have their protection increased and be shielded from unauthorized access and manipulation if access control measures are put into place [3].

Traditional access control models, such as discretionary access control (DAC) [4], mandatory access control (MAC) [5], and role-based access control (RBAC) [6], have limitations when it comes to providing a secure and effective mechanism for information protection in the large-scale and complex environment of IoT. These models are designed for closed systems and are not equipped to handle the dynamic interactions of many devices in an IoT setup. The ABAC model proposed in [7] addresses these challenges. As ABAC enables fine-grained access control by utilizing attributes to define user permissions [8]. This procedure allows for the efficient differentiation of user permissions relying on attributes, leading to a more manageable, efficient, secure and scalable AC system for the resource-constrained environment of IoT.

AC techniques can ensure that only authorized participants can access the available resources [9]. The MAC model provides protection on multiple levels. Each resource requires a different degree of discretion on the user's part. Users can gain access to the resources if they have been granted the necessary permissions to maintain a particular level of confidentiality [10]. An individual who owns a resource in DAC is the one who is responsible for deciding who can access the resource and

* Corresponding author.
E-mail addresses: syed.s.ullah@uia.no (S. Sajid Ullah), vladimir.oleshchuk@uia.no (V. Oleshchuk), harsha.sandaruwan@uia.no (H.S.G. Pussewalage).

https://doi.org/10.1016/j.comnet.2023.109994
Received 16 May 2023; Received in revised form 19 July 2023; Accepted 21 August 2023
Available online 24 August 2023

under what conditions. For instance, in operating systems, the person who owns the file is the one who decides who can access the file and how they can do so. This includes both read and write permissions. This model offers a fundamental level of safety [10]. Users' permissions are delegated to them in accordance with their roles within a system using the (RBAC) model [11]. Access decisions are made based on the relationships between roles and permissions and between users and roles. However, despite its usefulness in specific settings, RBAC's static and user-centric nature may not meet the demands of IoT access control. Traditional access control mechanisms can reliably guarantee that authorized users have access to the resources [9]. The MAC model protects multiple levels. Each resource requires a different degree of discretion on the user's part. Users can gain access to the resources if they have been granted the necessary permissions to maintain a particular level of confidentiality [10]. An individual who owns a resource in DAC is the one who is responsible for deciding who can access the resource and under what conditions. For instance, in operating systems, the person who owns the file is the one who decides who can access the file and how they can do so. This includes both read and write permissions. This model offers a fundamental level of safety [10]. Users' permissions are delegated to them in accordance with their roles within a system using the (RBAC) model [11]. Access control models, including RBAC, tend to have lower management efficiency when it comes to the complex requirements of IoT systems. This highlights the need for alternative access control models better suited to IoT environments' dynamic and expansive nature. Implementing detailed access control scenarios in these models is challenging while simultaneously applying the principle of least privilege [11]. Nevertheless, the IoT requires an access control model that is dynamic, fine-grained and goes beyond user-centricity.

The ABAC model is distinct from more conventional approaches to access control in that it does not establish permission to access resources based on the relationship that exists between subjects and those resources. Instead of using permissions to define access, the model uses attributes, which results in the model being more flexible and dynamic. The system can easily be modified to accommodate the addition of new resources, contextual information, or actions by simply assigning new permissions to existing attributes. ABAC can convert policies and rules into permissions on the fly by taking into account the attributes of the request. These attributes can be broken down into three categories: subject attributes, resource attributes, and environmental attributes like time and location. These attributes provide a more comprehensive definition of the subject and resource, including fixed characteristics like roles and changing characteristics like age or weather conditions. As a result, ABAC enables the creation of access policies that can effectively respond to changing environmental conditions [12].

Compared to more traditional access control models, the number of possible access condition combinations that can be implemented using ABAC is significantly higher [10]. In contrast to traditional access control models, fine-grained access control rules and policies can be defined thanks to the diversity of the attributes [13]. This makes it possible to implement more granular levels of security. Policies and rules governing access are composed of various subjects, objects (in the form of resources), and environmental attributes. The ABAC model can support dynamic and context-sensitive access control rules by considering environmental factors like date, location, time, threat levels, and IP address. Interoperability is supported by ABAC, which is another reason that makes it more convenient for the IoT. Access to the relevant resource is granted to the user, provided that the characteristics of the unknown user satisfy the criteria of some of the policies and rules already in place [13]. Since the nature of IoT devices and systems is such that they are always evolving, it is necessary to implement an access control mechanism that is equally dynamic, context-aware, attribute-based, and flexible. This requirement is met by ABAC, which enables the formulation of dynamic and sensitive-to-context access control rules by making use of attribute data. The decision regarding access control is not made based on the user's identity; rather, it is based on the characteristics of both the user and the environment. ABAC can make access control decisions that are well-suited to the environment of the IoT because it takes into account contextual factors such as the current time, location, threat level, and IP address. ABAC is still unprotected in run-time access to add new users to complex IoT networks.

Blockchain with ABAC is an excellent architecture for IoT, thanks to its excellent characteristics that make it reliable. Due to the decentralized nature of blockchain technology, problems associated with centralized management, such as single points of failure, are no longer an issue. Because it removed all third parties' needs from the equation, there is no longer any need for us to be concerned about any privacy leakage emanating from the transaction. In addition to that, a history log that cannot be tampered with and is completely reliable. It is recommended that an ABAC using blockchain for IoT be pre-deployed to address the issues of centralized and complex IoT networks. The data on a network can be controlled by its access control mechanism if it is incorrect, invalid, illegal, or unauthorized. In addition to controlling who can access what, it also monitors the number of network resources being used and the proportion of those resources being distributed among the various users based on attributes. A side benefit of this solution is that it stops potentially harmful devices from being connected to the network. In addition, privacy and security can be preserved in an IoT environment with a BE-ABAC for IoT. This type of access control restricts the capabilities of unauthorized users while preventing legitimate users from abusing their privileges in any way. Participants who have been allowed using authentication are the only ones allowed access to protected content.

1.1. *Motivation and contributions*

The IoT has recently seen a rise in popularity and has become a significant center of interest for both academia and industry. Using the underlined networks, this cutting-edge architectural framework provides connectivity to the real world via the Internet. The IoT aims to connect the smart and intelligent devices, including automobiles, household appliances, and physical devices, allowing the devices to collect and share data via the use of the Internet independently. However, as the number of connected devices increases, the need for an efficient and secure AC for the data they produce becomes vital. The security of the IoT environment is a critical issue, as many connected devices and the sensitive nature of the data they produce make them prime targets for cyber attacks. Conventional AC techniques face challenges in adapting to the IoT ecosystem as it rapidly expands. IoT technology involves the connection of various devices for data exchange and thus requires secure and efficient AC to this data. Conventional techniques may not be adequate in providing the level of security and efficiency required in this context. Since they are not designed to handle the huge amount of scalability and complexity of IoT environment, and they often rely on centralized authorities to manage AC policies, making them vulnerable to attack.

The objective of this study is to investigate the possibility of integrating blockchain technology into the ABAC framework to improve the security and effectiveness of IoT applications. Blockchain works as a decentralized and distributed ledger, and has the potential to provide record-keeping that is both secure and transparent. It is possible to construct an ABAC system that is more secure and reliable than those constructed using traditional methods by capitalizing on blockchain's inherent security and immutability. In this paper, we aim to evaluate blockchain-envisioned ABAC schemes suggested for IoT. In addition, the suggested schemes will be evaluated for their performance. Besides, this research explores the potential of using blockchain technology to improve the security and efficiency of IoT AC by evaluating blockchain-envisioned ABAC schemes for IoT. Finally, this research offers a concise summary and a comparison of BE-ABAC [14–29]. We believe that it will be beneficial for fresh readers to have a comprehensive understanding of the BE-ABAC schemes and their potential utilization across the applications of the IoT. During this study, we have analyzed and compared all (to the best of our knowledge) ABAC schemes for the IoT that utilized blockchain technology.

In the discussion presented above, ten essential characteristics of BE-ABAC in the context of the Internet of Things were presented. These characteristics are as follows: (1) the employment of a cryptographic hardness algorithm; (2) the incorporation of formal proof; (3) extensive cost analysis; (4) the assurance of confidentiality; and (5) the facilitation of scalability. (6) The procedure of authenticating users or entities in order to confirm their identities before allowing them access to a system. (7) The administration of resources, with the goal of maximizing the productive distribution and exploitation of system resources. (8) The process of transferring access rights, which enables users with approved access to delegate some of their permissions to other entities. (9) The protection of data integrity, which involves ensuring that information does not become inaccurate and does not get changed. (10) The enforcement of permissions, controlling and regulating access to system resources based on predefined rules and policies. The ten aforementioned features play a crucial role in characterizing access control within the domain of blockchain-enabled IoT. These features encompass a wide range of aspects, including resource management, enforcement of access control policies with robust security measures, and the delegation of access rights between entities in expansive blockchain-enabled IoT systems. A comprehensive analysis of these categories is provided in the relevant literature. The existing access control methods have made attempts to address certain aspects, but they do not sufficiently cover all the necessary features to ensure efficient access control for IoT systems, specifically in preventing unauthorized users from gaining access. It is important to acknowledge that access control in the IoT necessitates careful consideration during the design phase, particularly with regard to critical IoT requirements. This ensures the access control system can deliver scalable, efficient, lightweight, trustworthy, and robust policy enforcement mechanisms. The following is a summary of the primary contributions:

- The survey aims to provide a comprehensive understanding of BE-ABAC in the IoT applications
- To begin, we provide a comprehensive introduction to the IoT and BE-ABAC. In addition, we outline security challenges, risks, and attacks that may be conceivable in BE-ABAC in the IoT paradigm.
- After that, we conduct an in-depth analysis of the various BE-ABAC schemes presented for securing IoT.
- In addition, we offer a comprehensive analysis that contrasts the proposed survey with other surveys previously conducted for access control in the blockchain.
- Besides, we also conduct a comparative analysis based on the Evaluation based on the Distance from Average Solution (EDAS) method to determine the most effective among the proposed Blockchain-Enhanced ABAC (BE-ABAC) schemes.
- In conclusion, the study suggests challenges that need to be solved and new lines of inquiry for the future.

1.2. Survey organization

The organization of the paper is shown in Fig. 1.

2. Background

This section presents the ABAC System, the Basics of ABAC, and ABAC for Blockchain.

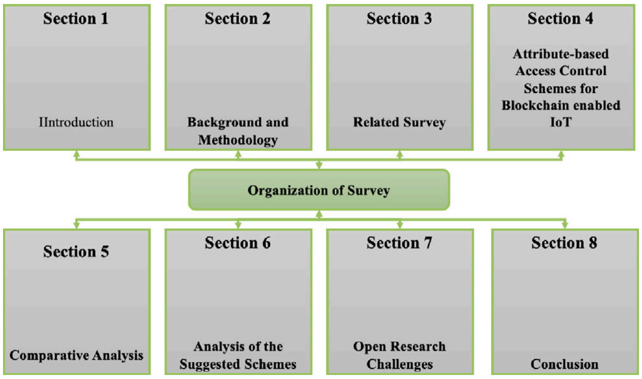

Fig. 1. Organization of paper.

2.1. Attribute-based access control system

The ABAC is a method of managing AC that is based on attributes rather than identities. ABAC takes into consideration a number of characteristics of the things that are being managed rather than basing choices regarding AC merely on the identity of the user. Generally speaking, these characteristics are classified as either subject, resource, or environmental traits. This approach to AC makes it possible to have a system that is more adaptable and dynamic, able to react to shifts in the surrounding environment and give finer-grained AC. Besides, the implementation of ABAC in a blockchain setting offers other advantages, such as decentralized and tamper-proof record-keeping [30]:

- User Attributes: In this context, user attributes are attributes or elements of information that describe the users who make use of the given system. These characteristics can also include professional information such as job title, role, and security clearance as well as personal information including age, name, and address. Another vital quality that may be taken into account is a user's trust level, which refers to the degree to which the computer system places its faith in the users. The level of access and permissions a user has within the given system can be partially determined by the qualities described here.
- Object Attributes (OA) are the attributes of the resources that are made available by the system. The given attributes can be associated with the object's metadata, such as the author's name, the creation date, the last change date, the size, the kind of file, and the level of security. Besides, object characteristics can also include information describing the contents of the object, such as the name of a patient (for example, in health records), the number of a student (for example, in student records), or the title of a particular chapter. The object attributes provide important information about the resource, which helps determine the access level that should be granted to a user.
- Environmental Attributes: The current state of an environment can also provide attributes used for AC decisions. These attributes can include the current time, day of the week, number of users logged in, CPU usage, available memory, etc.
- Connection Attributes: In ABAC, session attributes normally represent characteristics specific to the user's current session. It can include the IP address, physical location, start time and duration of the session, hostname, number of access requests, etc. These attributes are related only to the duration of the user's session.
- Characteristics of Administration: In ABAC, certain attributes are established by an administrator or an automated process and apply to the entire system. These attributes, known as configuration attributes, can impact AC decisions and include elements such as the threat level, minimum trust level required for access, maximum session length, and others. These attributes provide

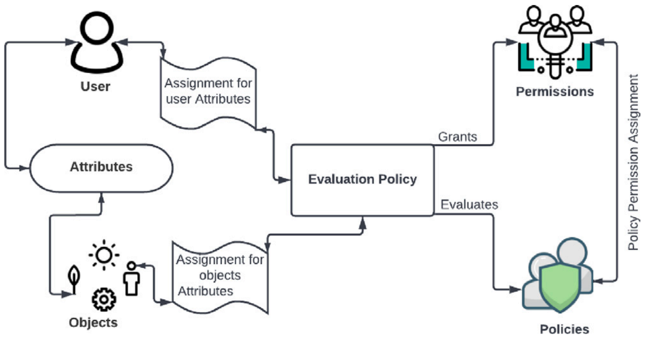
User
Assignment for user Attributes
Permissions
Policy Permission Assignment
Attributes
Evaluation Policy
Grants
Evaluates
Assignment for objects Attributes
Objects
Policies

Fig. 2. The core of ABAC model.

a framework for the system to operate within and shape AC policies.

In an optimal setup, the attributes are inherent characteristics of the components within the system and do not require manual input from administrators. For instance, most attributes related to an object stem from the metadata linked with the object. The outcome of a Boolean statement that compares characteristics can be used as the basis for creating access policies using policy languages. These policies can be used to restrict access to particular resources or objects. ABAC models allow for the creation of flexible regulations based on real-world properties of elements in a system rather than manually assigning roles or permissions to users based on their identities. With ABAC, regulations are enforced based on knowledge of a user's attributes, making the process more user-friendly. The key advantage of ABAC is its intuitive nature, where technical permission sets are hidden behind simple user profiles that can be updated by authorized personnel. This ensures that users always have the necessary access if their attributes are current. The other advantage of ABAC is the flexibility it provides; almost anything about the user and the business can be represented, which enables the business to think in terms of how it operates as a business rather than how it operates in terms of information technology. The applications that users can access, the types of data that can be accessed, the transactions they can submit, and the operations they can perform all change dynamically based on the context in which they work. The result is that administrations using ABAC can make decisions based on information about real-time operations that are clearer and more concise.

2.2. Core of attribute-based access control

This section outlines a brief overview of the ABAC model, considering its common components and typical variations [31]. Figs. 2 and 3 demonstrate the core and blockchain versions of the ABAC model, respectively. The majority of ABAC models generally consist of the following elements, which are frequently found in various ABAC systems:

- Users (U): The collection of individuals accessing the system is called "Users". Notably, the size of this group is not necessarily limited, as it is possible for new users to be granted access even after the set was initially established. This is commonly seen in service-oriented architectures and information-sharing systems spanning organizational boundaries.
- Objects (O): The collection of all items with integrity preserved by the system.
- Attributes (A): The collection of attributes with a distinct name used in the system forms the Attributes (A). In some models, each attribute is associated with a type or divided into groups based on the access control object they apply to organize the data efficiently.

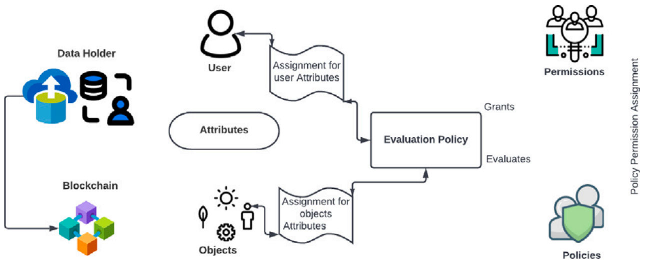

Fig. 3. The core of ABAC model for blockchain.

- Permissions (PMS): The whole catalogue of user permissions can be bestowed upon individual users. Permissions in some models are represented as object-operation pairs, which is analogous to how permissions are represented in RBAC; however, this is not always essential. Permissions in some ABAC models are defined as a combination of policy and operation. These permissions allow access to perform a specific operation on an object that meets the policy criteria. The object must satisfy the policy to be granted access.
- Policies (P): The complete collection of access policies used to regulate the use of the system. In most cases, these policies are expressed in a language specifically designed for policy writing and are connected, in some fashion, to the permissions they issue.
- Blockchain integration with ABAC: The integration of blockchain with Attribute-Based Access Control (ABAC) presents potential benefits and challenges. Blockchain, a decentralized and distributed digital ledger, can enhance the security, transparency, and auditability of access control mechanisms. By storing access control policies and permissions on the blockchain, the system ensures transparency and immutability of access decisions [32,33]. Although integrating blockchain with ABAC has many benefits, it also presents some challenges. The scalability of blockchain becomes a concern because its consensus and data storage mechanisms may face limitations when supporting many users and objects. Developing and implementing blockchain is complex, requiring specialized knowledge and expertise. Additionally, privacy concerns arise when storing sensitive attribute information on a public or private blockchain, requiring robust encryption and access control measures. When it comes to blockchain technology, organizations need to consider regulatory compliance. They must adhere to data protection, retention, and privacy regulations while navigating the legal landscape. To avoid delays and vulnerabilities, the governance and consensus mechanisms should be carefully designed to handle conflicts in access control policies and attribute values. A comprehensive assessment of the combination of blockchain and ABAC is absolutely crucial. While the potential benefits, such as improved security and transparency, are tempting, organizations must not overlook the serious challenges regarding scalability, complexity, privacy, regulations, and governance. To ensure that the benefits of integrating blockchain outweigh the drawbacks and align with the specific needs and limitations of the organization, proper planning and evaluation are imperative [32,33].

2.3. Access control in blockchain enabled IoT

Access control in the IoT necessitates meticulous deliberation during the design phase, wherein one must duly consider the pivotal IoT requirements. This is imperative to provide scalable, efficient, lightweight, reliable, and resilient policy enforcement mechanisms. Due to their extensive scale and heterogeneous composition, decentralized policy management is imperative in IoT networks. The convergence

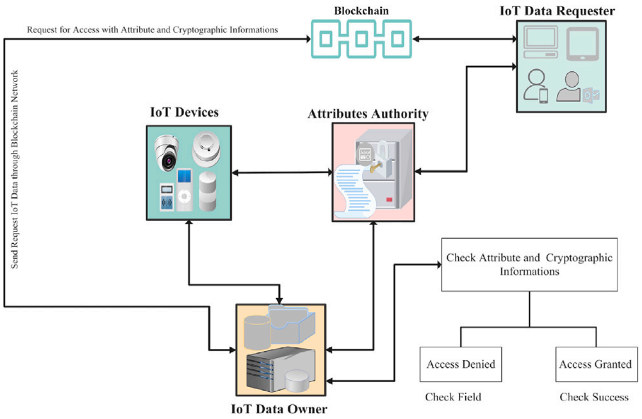
Blockchain
IoT Data Requester
Request for Access with Attribute and Cryptographic Informations
Send Request IoT Data through Blockchain Network
IoT Devices
Attributes Authority
Check Attribute and Cryptographic Informations
Access Denied
Access Granted
Check Field
Check Success
IoT Data Owner

Fig. 4. Access control in blockchain enabled IoT.

of ABAC and blockchain technology has become a notable solution in overcoming the constraints of traditional access control mechanisms like RBAC and DAC. This integration offers a more effective and precise access control method for extensive IoT systems operating across various jurisdictions. Fig. 4 showcases a conceptual representation of blockchain-powered ABAC for IoT access management. By harnessing the capabilities of the decentralized storage and computational infrastructure offered by blockchain technology, novel prospects emerge. The inherent characteristics of blockchain, including decentralization, consensus algorithms, immutability, irreversibility, tamper resistance, accessibility, and auditability, provide a robust and dependable method for storing transactions in a distributed manner across the network. These properties are not readily attainable solely through the aforementioned traditional access control mechanisms. By leveraging the integration of BAC with blockchain technology, the field of IoT access control stands to gain significant advantages from the decentralized and transparent nature of the blockchain. This integration enables enhanced policy enforcement, secure management of attributes, and the ability to make precise access control decisions. The integration of ABAC and blockchain technology exhibits the capability to tackle the scalability, trust, and efficiency obstacles linked with access control in extensive IoT implementations.

3. Related surveys

This study aims to survey and summarize the existing literature on access control in the context of IoT and Networks using blockchain technology. A comprehensive search was conducted using various online databases such as IEEE Explore, Springer, Science Direct, and Researchgate. A manual search was also performed in relevant areas to gather relevant information. The review aims to provide an overview of all the existing survey papers on blockchain-based access control for securing IoT and Networks. The study also reviews all the available security surveys on access control in the domain of IoT. Finally, Table 1 summarizes the related survey on access control schemes for blockchain.

In 2019, Rouhani and Deters [32] examine the challenges present in current access control systems and discuss how blockchain technology could help address these challenges. The authors give an overview of research and platforms related to access control that has been proposed for different domains. They also summarize the current state of blockchain-based access control systems and their problems.

In 2019, Riabi et al. [34] explored the difficulties of access control in the context of the IoT. The authors analyzed the limitations of conventional access control methods in satisfying the needs of the IoT and examined the potential for decentralized access control through the use of secure blockchain architecture. Based on a review of related literature, the authors identified two models for blockchain-based access control: the Transaction-BAC model and the Smart Contract-BAC model. They conducted a comprehensive evaluation and comparison of these models, concluding that the transaction model aims to secure access tokens and leverage the benefits of smart contracts, one of which is to address the issue of centralized access control having a single point of failure.

In 2020, Ghaffari et al. [35] explain the current suggested authentication and AC solutions using blockchain and smart contracts. The authors first gave a brief history of AC, authentication, and distributed ledger technology. The authors then propose a taxonomy to classify the existing methods based on their type, application environment, and use of blockchain. Finally, the authors evaluate the benefits and limitations of the propose approach in various aspects, including security, resource consumption, and privacy. Later, Abdi et al. [36] summarize the different AC strategies used in IoT. The authors compare each scheme's scalability, distribution, security, user-centricity, privacy, and enforcement policies. They also discuss the challenges of creating decentralized AC mechanisms for IoT and suggest areas for future research.

In 2021, Sookhak [37] add a comprehensive survey that aims to discuss blockchain-empowered AC solutions in the healthcare environment. The authors aim to understand the current advancements and categorize them into themes. The authors also aimed to discuss the security concerns associated with existing schemes and the necessary security requirements for creating a detail AC. Besides, the authors also compare traditional AC schemes to blockchain-empowered approaches, identifying unresolved issues and potential areas for future research. Later, Hussain et al. [38] discuss the challenges faced by IoT security, including AC for unauthorized participants and IoT security standards. The authors add the shortcomings of traditional AC techniques in meeting the security requirements of the IoT and evaluate the potential of employing blockchain technology to provide a secure framework for AC. The authors also examine the role of blockchain in addressing various IoT security standards and identify the gaps for future improvement, unresolved problems, and challenges. Later in the same year, Patil et al. [39] add a variety of blockchain-empowered new solutions to the literature for IoT AC as well as the improvement of security and privacy the Vehicular Ad-hoc Network (VANET), healthcare, and supply chain networks. Besides, the survey also investigates the solutions now accessible for various performance indicators, including scalability, privacy, extensibility, accuracy, storage overhead and computation overhead respectively. Later, Abdulrahman et al. [40] present a review and compares the most recent blockchain-enabled solutions AC in IoT. Moreover, the authors recommend a set of requirements that should be considered when employing blockchain technology to AC in an IoT environment.

4. Blockchain envisioned attribute-based access control schemes for IoT

IoT research has experienced a meteoric rise due to the explosion of new objects appearing in communications and networking technology. The ability to share data, simplify access, and perform remote monitoring are benefits that can be gained from connecting various smart devices over the internet [5]. One of the most significant challenges the IoT must overcome is its centralized structure, the client–server model. It is possible for a failure of the entire network to be caused by a lack of trust between the various participating devices; therefore, a solution that can be trusted is required to avoid this problem. Several approaches have been proposed in recent years, but blockchain is becoming increasingly popular due to its properties, such as its decentralized structure, security, and immutability. We divided these schemes into the following two main categories in Fig. 5.

Table 1
Summary of access control survey on blockchain.

S.no	Years	Survey	Summary
1	2019	Rouhani and Deters [32]	Provide an outline of the issues present in the existing access control (AC) schemes and then describe how blockchain technology can assist in finding solutions to these issues. The authors offer an overview of the current state of blockchain-based AC systems and the issues they face.
2	2019	Riabi et al. [34]	Shows AC's challenging nature within the IoT framework. Investigate the shortcomings of conventional AC in terms of meeting the demands of the IoT. Identify two distinct models based on their assessment of the relevant literature: The Transaction-BAC model and the Smart contract-BAC model.
3	2020	Ghaffari et al. [35]	Explain the present solutions in deploying of blockchain. The authors provide a concise overview of the history of AC and authentication technology in addition to distributed ledger technology.
4	2020	Abdi et al. [36]	Presents a summary of the various AC strategies seen in IoT. Include a table that compares the various AC strategies examined. Discuss the difficulties in developing decentralized AC mechanisms for IoT systems and potential future research directions.
5	2021	Sookhak [37]	Outlines an extensive overview on the blockchain-based AC methods in the healthcare domain. This survey categorizes existing and future AC area improvements. A thematic taxonomy of the blockchain-based AC methods is also presented.
6	2021	Hussain et al. [38]	Explore the fundamental challenges IoT security poses, including AC for unauthorized users and IoT security standards. Authors evaluate the possibilities to spread AC by implementing the safe design the blockchain accommodates. The survey also explores how to leverage the blockchain to fix some of the standards important to IoT security challenges.
7	2021	Patil et al. [39]	Present various blockchain-based solutions now available in the academic literature for IoT AC. Investigates the solutions now accessible for various performance indicators, including scalabilities, privacy, extensibilities, accuracy, storage overhead, and compute overhead.
8	2021	Abdulrahman et al. [40]	Review and compares the most recent state-of-the-art solutions in blockchain-based AC for IoT. Suggest some requirements that should be considered when applying blockchain technology to AC in an IoT environment.

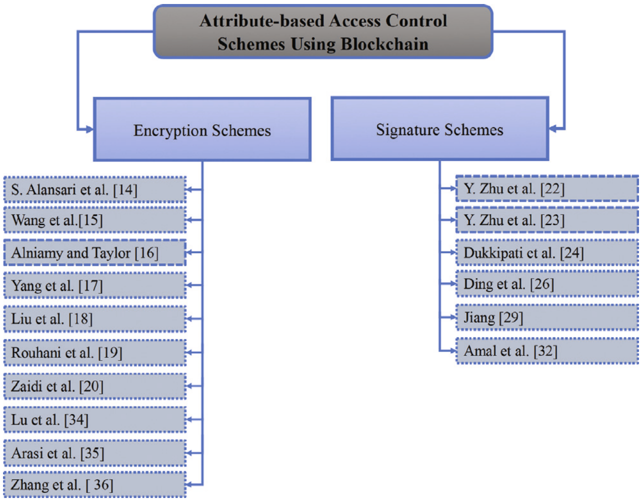

Fig. 5. Classification of BE-ABAC schemes.

4.1. Encryption-based ABAC schemes for blockchain-based IoT

In ABAC encryption-based schemes, the encryption primitive is utilized to secure the attributes and AC policies linked to participants and objects. This can be obtained by encrypting the attributes and AC policies with the help of complex cryptographic algorithms. The Access decisions are made by decrypting the attributes and comparing them to the AC policies. This ensures that only authorized participants with the correct decryption keys can access the encrypted attributes and make access decisions using the decrypted data. The encryption-empowered schemes emphasize the importance of achieving the confidentiality and integrity of attributes and AC policies.

In this section, we reviewed and compared the suggested ABAC schemes for blockchain-empowered IoT that use encryption for security purposes to provide secure access.

In 2017, Alansari et al. [14] propose an innovative identity and access management solution for cloud federations. Using the technology, federated organizations can implement ABAC policies on their data that do not compromise their users' privacy. Users' identities are checked against the policies, and if those identities match, the users are permitted access to the federated data. However, the users' identities are not revealed to the federated organization that owns the data. Utilizing blockchain technology with trusted hardware from Intel enables the system to provide further assurance that the policy review procedure is honest and transparent. It does this by utilizing blockchain technology to ensure that users' identifying attributes and access control policies cannot be updated by a malicious user, while Intel software guard extensions (SGX) safeguard the integrity and secrecy of the policy enforcement process. The authors explore potential future extensions and explain the access control mechanism. The authors utilize bilinear Pairing algorithm for encrypting data. However, this approach demands extensive computation and communication resources because of the complex nature of the algorithm. Furthermore, the authors did not provide any formal security proof.

In 2018, Wang et al. [15] conduct research on data storage and sharing in decentralized storage systems. The authors studied data storage and sharing issues in these systems and devised a framework to address them. This framework combines the Interplanetary File System, the Ethereum blockchain, and ABAC technology. In the proposed framework, the data owner has the ability to encrypt the data and assign access policies to data users through secret key distribution. This allows for fine-grained control over who has access to the data. The framework also implements a keyword search function on the encrypted data in the decentralized storage systems using smart contracts on the Ethereum blockchain. This helps to overcome the issues that arise when traditional cloud servers do not return accurate results or all of the results from a search. The authors tested the proposed framework on a Linux system and the Ethereum official test network Rinkeby. The results showed that the scheme was technically viable. The authors utilize bilinear Pairing algorithm for encrypting data. However, this approach demands extensive computation and communication resources because of the complex nature of the algorithm. Additionally, the authors did not provide any formal security proof. Moreover, revealing the private key invite series of attacks.

In 2020, Alniamy and Taylor [16] propose an architecture model that enhances fine-grained access control for data stored in the cloud. The model integrates the Hyperledger blockchain technology and the ABAC scheme to provide secure and controlled access to shared files in a decentralized environment. The system encrypts shared data with access policies linked to attributes, allowing data owners to manage their data and prevent unauthorized access. The Hyperledger blockchain ensures the privacy and integrity of stored files, managing the generation of keys, assignment of policies, and serving access requests. The propose system prototype was realized with chain codes, and its performance was evaluated on the Hyperledger Composer blockchain environment. Unfortunately, the author did not include any information about the encryption algorithm used. Additionally, the authors did not provide formal security proof to ensure security.

In 2021, Yang et al. [17] propose a non-interactive access control strategy for the IoT based on blockchain technology, Pastel Network (PSL)and ABAC. A data holder sends their information to be stored on a cloud server. For a user to have access to the data, the user must first add the attributes as a transaction to the blockchain. Following this, a smart contract will execute the PSI protocol to determine whether or not the characteristics set satisfies the threshold structure. If the need is satisfied, the data user will be granted access to the data holder's data. The data holder encrypts the data address using the public key of the user who was selected and then delivers the encrypted data address to the user. While still maintaining trusted access control, the propose approach can preserve both the privacy of access policies and the privacy of characteristics. However, this approach demands extensive computation and communication resources because of the complex nature of the algorithm. Additionally, the authors prove the security informally and fail to provide formal security proof. In 2021, Liu et al. [18] proposed a revocable ABAC system for blockchain-enabled IoT applications. The authors enhance Waters' ciphertext policy attribute-based encryption (CP-ABE) scheme into a revocable ciphertext policy attribute-based encryption (RCP-ABE) scheme by adopting a technique based on binary trees and allowing for the revocation of attributes. The authors create a revocable ABAC system by merging the RCP-ABE with blockchain technology. The propose system can enable expressive access control policies and grants the authority of an attribute the ability to revoke the attributes of users or a portion of their attributes. According to the findings of the security study, the developed system satisfies a number of desirable features. These include forward security, backward security, secrecy, and integrity. The authors fail to demonstrate the security features they assert to possess properly. The authors prove the security informally and fail to provide formal security proof. Furthermore, the propose approach utilizes a sophisticated algorithm bilinear pairing, which requires substantial computational and communication resources.

In 2021, Rouhani et al. [19] discussed how permissioned blockchains could be used as trustable backends in access control systems, providing a solid basis for audits. The authors suggest a distributed ABAC system based on Hyperledger Fabric, emphasizing audibility and scalability. Data encryption is used for secure ABAC. The authors validate the proposed method by means of a Use Case involving an application for decentralized access control management in digital libraries. First, the authors give an in-depth analysis and synthesis of previous research on blockchain-based access control studies. The next thing they do is describe the system architecture and the implementation details. During the experimental evaluation of our solution, various parameters derived from the Hyperledger Caliper framework were considered in terms of the system's performance. The authors claim that the proposed proof-of-concept system can properly handle a throughput of 270 transactions per second, with an average latency of 0.54 s per transaction, according to the data analysis. However, the authors did not provide security proof. In 2021, Zaidi et al. [20] proposed an ABAC mechanism for IoT. The propose mechanism provides local access, authorization of clients, privacy, and interoperability by utilizing smart contract data sharing and user-controlled encoded policies. Additionally, the authors claim that the proposed mechanism will provide local access. It is possible for the user to own their data and be authorized to share it with other people. The authors argue that there is currently no solution that can meet all of the requirements of the propose paradigm. The ABAC model is utilized due to its excellent compatibility and expressiveness. Using blockchain for authentication and smart contracts for the data access process in propose mechanism allows the authors to circumvent the problems of high computational time and overhead to some extent. This is accomplished by deploying a number of smart contracts for every additional user, which comes with the risk of a single point of failure and the de-authentication of previously authenticated users. To ensure data confidentiality, the authors also created a contract establishing ownership for each user in relation to their individual gadgets. Within the confines of propose blockchain design, it is not possible for any organization to divulge genuine user data under any circumstances. Off-chain data are always stored in an encrypted format, which eliminates the possibility of tampering with the data. After the invocation of smart contracts, the data will be accessible only to those customers who are in compliance with the set policies. The authors fail to demonstrate the security features they assert to possess properly. The authors prove the security informally and fail to provide formal security proof. Furthermore, the propose approach utilizes a sophisticated algorithm bilinear pairing, which requires substantial computational and communication resources. Furthermore, the algorithm fails to specify the utilization of pairing operations, which indicates that the mathematical construction is incomplete.

Lu et al. [21] propose secure IoT data sharing and fine-grained access control to accomplish a data access control strategy based on the ABAC algorithm and blockchain technology. The hash value of the data, the location information of the encrypted data, and the access control technique are all recorded on the blockchain in the proposed system. Achieving efficient and granular access to data is made possible by the blockchain's capacity to guarantee the data's integrity and incorruptibility. The proposed system not only assures that the data cannot be modified but also ensures that the access control method cannot be modified in any way. A further benefit of the proposed solution is that it reduces the strain on the blockchain's storage capacity and significantly enhances its ability to scale. The experiment was designed to demonstrate that the proposed scheme is superior to the cloud storage scheme. In addition, the proposed scheme was made for a fine-grained access control system that integrates symmetric encryption methods and ABAC in its workings. In the proposed method, the data are initially encrypted using the symmetric encryption algorithm, and then the symmetric encryption key is encrypted using the ABAC technique. This system protects the integrity of the data collected by IoT devices, enabling data owners to exercise fine-grained control over who can access their data, and assures that the data cannot be altered in any manner. However, the propose requires a secure channel to distribute keys among the participants.

In 2022, Arasi et al. [22] proposed an efficient data-sharing strategy for cloud storage utilizing attribute access control with fair mediation in cloud storage using blockchain networks and an auditable attribute-based encryption scheme (AABES). The AABES encrypts a file by linking it to an access policy; the resulting ciphertext is then saved in the cloud. Only users with the required attribute set who comply with the access policy specified in a monotonic tree structure can access the outsourced encrypted file. Collusion attempts are unsuccessful against the access structure. In the proposed system, the authors primarily concentrate on designing a reliable and effective access control mechanism utilizing blockchain, offering fair mediation to cloud users if their file integrity is compromised. The fraudulent cloud service provider is punished by paying the users whose data integrity was compromised, effectively managing permitted user access and secure data sharing. By taking advantage of the blockchain's capabilities, the access policy set up of ABAC in the smart contract identifies and bans the user from further access to the blockchain network when unlawful access is made to the stored data. By prohibiting potential threats from accessing the stored data, the proposed approach guarantees data privacy, integrity, availability, and data ownership of persons. The authors utilize bilinear Pairing algorithm for encrypting data. However, this approach demands extensive computation and communication resources because of the complex nature of the algorithm. Additionally, the authors provide informal analysis and fail to provide any formal security proof.

Zhang et al. [23] propose a blockchain-enabled ABAC strategy with hidden policies for smart healthcare systems. To prevent single-point failure, the propose system introduces several authorities. In particular, online–offline encryption reduces the load of users' online computing by moving computation chores to users' free time, and policy concealment safeguards users' sensitive data. To facilitate the outsourcing of decryption between users and mobile edge computing servers, fair payments are also accomplished based on blockchain and smart contracts. The experimental results demonstrate that the propose scheme is computationally efficient and secure in the random oracle model, making it applicable to the edge computing environment. The authors utilize bilinear Pairing algorithm for encrypting data. However, this approach demands extensive computation and communication resources because of the complex nature of the algorithm.

Lesson Learned: It is important to mention that while many researchers discuss pairing-based ABAC for IoT, which highlights the overall complexity of pairings and procedures to speed up pairing computation, these schemes suffer from heavy computational overhead due to the use of pairing. In Pairing-based ABAC, IoT users create bilinear pairing independently to generate single encryption and verify the encryption text, respectively, using hard problems like Computational Diffie–Hellman (CDH) assumption, which leads to high computational overhead in resource-constrained blockchain-based IoT devices, even though it provides a desired level of security. Moreover, the above review shows that apart from Zhang et al. [23], the rest of the schemes do not have any formal proof. As a result, it can be challenging to ensure that all of the desired security requirements are met not with the desired level of efficiency. Besides, In Tables 2, 3, we discuss the diverse array of access control solutions for the IoT that are constructed upon the principles of blockchain technology. Our focus is directed towards ten pivotal aspects of access control, namely: (1) the implementation of robust cryptographic hardness algorithms, (2) the utilization of formal proofs, (3) the meticulous analysis of costs, (4) the preservation of confidentiality, and (5) the attainment of scalability. The key aspects of (6) authentication, (7) resource management, (8) access right transfer, (9) integrity, and (10) permission enforcement. Below, we present a concise overview of the aforementioned features attain by each scheme in the Table. Effective resource management is of utmost importance in the context of IoT devices, considering the inherent constraints posed by limited battery life, memory capacity, and processing capabilities. The concept of access rights transfer refers to the act of transmitting access control permissions (along with any accompanying conditions) from one entity to another. Enforcing access control delegation to IoT devices is of utmost importance in ensuring secure and efficient system operations. The enforcement of permissions must be customized according to the specific requirements of an IoT system. Flexibility in policy management is a fundamental attribute of an access control system. In the current resource-constrained environment, the demand for lightweight algorithms with formal proof has become imperative in order to ensure confidentiality, integrity, and authentication. This uncertainty may arise as a result of IoT device failures, unreliable data sources, or even system failures. Moreover, the utilization of attributes can effectively handle the identification of entities (including uncertainties in observations derived from both physical and digital data) on a scalable level that is not reliant on a singular, specific identity for each entity. Finally, it is crucial to emphasize the significance of scalability in IoT access control, given the resilient and ever-changing nature of data and resources. In the subsequent Table 2, we present the classification each scheme.

Table 2
Access control features of encryption-based ABAC schemes for blockchain-based IoT.

Scheme	Management of resources	Transfer of access to rights	Enforcement permission	Attribute management
Alansari et al. [14]	N/A	N/A	YES	YES
Wang et al. [15]	N/A	YES	N/A	YES
Alniamy and Taylor [16]	N/A	YES	YES	YES
Yang et al. [17]	N/A	YES	N/A	YES
Liu et al. [18]	N/A	YES	YES	YES
Rouhani et al. [19]	YES	YES	N/A	YES
Zaidi et al [20]	N/A	YES	YES	YES
Lu et al. [21]	N/A	N/A	YES	YES
Arasi et al. [22]	N/A	N/A	N/A	YES
Y. Zhang et al. [23]	N/A	YES	YES	YES

4.2. *Signature-based ABAC schemes for blockchain-based IoT*

A Signature-based ABAC scheme uses digital signatures to ensure that attributes and access policies are intact and authentic. The given process utilize complex cryptographic algorithms to generate digital signatures for access policies and attributes. These digital signatures serve as proof of integrity and authenticity. The Access decisions are taken by verifying the digital signatures of the attributes and compare the digital signature with the AC policies. This assures that only attributes and AC policies with valid digital signatures are allowed for AC. The digital signature-based scheme normally underscores the importance of verifying the integrity and authenticity of attributes and AC management.

In this section, we reviewed and compared the suggested ABAC schemes for blockchain-empowered IoT that use digital signatures for security purposes to provide secure access.

In 2018, Zhu et al. [24] introduce the possibility of constructing a secure resource-sharing platform using a blockchain-based decentralized environment. The authors propose a novel AC platform called transaction-based access control (TBAC), combining blockchain technology and the ABAC model. The authors claim the propose TBAC mechanism with 4 different transactions for subject registration, object escrow and publication, access request and grant. To ensure security in attribute exchange and dynamic policy decision-making, the authors also developed a cryptosystem called CryptoTBAC. Unfortunately, no cryptographic technique was shown to support the authors' claims. The authors propose a theoretical modal with no security proofs. Also, the algorithm for this technique is unclear. In 2021, Zhu et al. [25] presented a new digital asset management platform named DAM-Chain, which utilizes TBAC. The platform merges the principles of ABAC and blockchain technology. The ABAC provides flexible authorization mechanisms for escrowing digital assets into the blockchain, while the blockchain transactions serve as a traceable and verifiable medium for access requests. The authorization mechanisms are decentralized, including subject registration, object escrowing and publication, access request, and grant. The DAM-Chain platform offers flexible permission management and a transparent, verifiable access authorization procedure in an open, decentralized environment by taking advantage of ABAC and blockchain technology. The authors utilize bilinear Pairing algorithm for encrypting data. However, this approach demands extensive computation and communication resources because of the complex nature of the algorithm. Besides, the authors did not offer formal proof.

In 2018, Dukkipati et al. [26] present an ABAC model that leverages blockchain technology to address security and privacy challenges. The framework is comprehensive and includes a discussion of each block in detail, followed by a thorough explanation of the implementation. The proposed model was tested when an access policy was evaluated for sharing or updating traffic signal data. The evaluation of the model considered various attributes, such as memory usage, the number of transactions needed to evaluate a user request, and the use of smart contract algorithms and tokens. Although the approach has potential, it was noted to have privacy concerns and a lack of explicit security evidence. The propose scheme did not offer formal security proof.

In 2019, Ding et al. [27] propose a new ABAC scheme that incorporates blockchain technology to enhance access management for resource-constrained IoT devices. The aim was to address the trust issue and improve the system's robustness with a decentralized and scalable access control mechanism. The authors introduced a new type of transaction for recording attribute permissions and designed the scheme so that IoT devices do not rely on the consensus process of the blockchain network. As a result, the overall processing and communication overhead is greatly reduced. In addition, some parts of the proposed scheme, such as the consensus algorithm and the authentication and key agreement (AKA) protocol, have a modular architecture, significantly improving the system's adaptability and making it easier to maintain and upgrade. The security analysis over ECC confirmed that the proposed technique is secure for use in actual applications, and the simulated experiments demonstrate that it is an effective and efficient method for enforcing stringent and fine-grained access control in the IoT. Using Elliptic Curve Cryptography (ECC) makes the propose scheme efficient. However, the scheme lack formal security proof.

In 2021, a blockchain-ABAC system was proposed by Jiang [28]. The proposed scheme uses the blockchain as the trusted center in the access control model, and it implements the ABAC policy by generating smart contracts. In the access procedure, the resource owner and the visitor communicate through the blockchain's nodes by invoking smart contracts. In addition, the proposed scheme has been tested on equipment that is typical of the whole, and the testing results indicate that the proposed system is both effective and feasible. Though, using Elliptic Curve Digital Signature Algorithm (ECDSA) makes the propose scheme efficient. However, the scheme lack formal security proof.

In 2021, Amal et al. [29] revealed blockchain-based ABAC and fine-grained access control, which maintains user privacy and accountability. The authors constructed a permission blockchain prototype and ran numerous tests to establish the solution's scalability, which they presented at the conference. This study examines the threat model. Despite this, the proposed approach consumes a lot of computation and communication resources due to the intensive Bilinear Pairing algorithm. There is also no formal security proof for the proposed system.

Lesson Learned: In the following discourse, we discuss the diverse array of access control solutions for the IoT that are constructed upon the principles of blockchain technology. Below, we present a concise overview of the aforementioned features attained by each scheme in Table 3. After conducting a comprehensive study, we found that the recommended methods have significant drawbacks for computational and communication resource utilization. It is important to mention that while many researchers discuss pairing-based ABAC for IoT, which highlights the overall complexity of pairings and procedures to speed up pairing computation, these schemes suffer from heavy computational overhead due to pairing. In Pairing-based ABAC, IoT users create bilinear pairing independently to generate a single signature and verify the signature text, respectively, using hard problems like CDH and ECDLP assumption, which leads to high computational overhead in resource-constrained blockchain-based IoT devices, even though it provides a desired level of security. Moreover, the above review shows that apart from a few schemes, the rest have no formal proof. As a result, it can be challenging to ensure that all of the desired security requirements are met, not with the desired efficiency level.

Table 3
Access control features of signature-based ABAC schemes for blockchain-based IoT.

Scheme	Management of resources	Transfer of access to rights	Enforcement permission	Attribute management
Zhu et al. [24]	YES	YES	N/A	YES
Zhu et al. [25]	N/A	YES	N/A	YES
Dukkipati et al. [26]	YES	YES	N/A	YES
Ding et al. [27]	YES	YES	N/A	YES
Jiang [28]	YES	N/A	YES	YES
Amal et al. [29]	N/A	YES	N/A	YES

5. Comparative analysis

This section will evaluate each blockchain-envisioned ABAC scheme presented to secure the IoT based on security hardness, security proof, cost, security validation tools, and security properties.

5.1. Performance evaluation matrices

IoT networks are differentiated from other networks by their severe hardware constraints. Therefore, to achieve the lowest possible overall energy consumption, every IoT process should use the absolute minimum amount of memory and processing power possible while also transferring the absolute minimum amount of data possible using the minimum number of messages. Because the requirements are so stringent, authors usually incorporate performance assessments in their articles to demonstrate their schemes' efficiency in resolving the problem.

The strategies outlined in the previous section have a potential risk of having a single point of failure. As IoT devices' computation and power requirements are minimal, it is simple for a hostile actor to take control of them. Because of this, putting your faith in access policies might not be the best choice. The use of blockchain technology to enable trustworthy distributed access control is one potential solution to the problem described above. In addition, we have compared all the blockchain-envisioned ABAC schemes with their findings and shortcomings, as shown in Table 4. A few ABAC methods envisioned for use with blockchains are presented below, along with some recent use cases.

5.2. Quantitative analysis

We use quantitative analysis, including security attributes, to evaluate the safety of the suggested ABAC mechanisms that have been given to safeguard the Internet of Things. Table 3 compares the levels of security offered by [14–29].

The analysis of the security properties of any access control system requires security proof, which is very significant and can also be used to verify that the scheme in question is valid. It is of the utmost importance to ensure that the prerequisites and requirements for security are met. ROM, or the Standard Model, is frequently utilized when evaluating the efficiency of various access control schemes. The $\surd$ represents this security strength is satisfied, as shown in Table 5. From Table 5, it is evident that Y. Zhu et al. [24], Y. Zhu et al. [25], Dukkipati et al. [26], Alniamy and Taylor [16], Jiang [28], Zaidi et al. [20] and Lu et al. [21], did not define the security hardness algorithm for their schemes. In comparison, the authors S. Alansari et al. [14], Wang et al. [15], Yang et al. [17], Liu et al. [18], Rouhani et al. [19], Amal et al. [29], Arasi et al. [22] and Y. Zhang et al. [23] utilized costly bilinear pairing for their schemes while the Ding et al. [27] utilized Elliptic Curve Cryptography. Similarly, the authors S. Alansari et al. [14], Y. Zhu et al. [24], Y. Zhu et al. [25], Dukkipati et al. [26], Wang et al. [15], Ding et al. [27], Alniamy and Taylor [16], Jiang [28], Liu et al. [18], Rouhani et al. [19], and Lu et al. [21] fails to provide any formal proof to support their claims. Besides, almost all the schemes suffer from cost-related issues. Finally, Ding et al. [27] provide proof using a security validation tool.

Table 4
Comparative analysis of ABAC schemes for blockchain.

S.no	Scheme	Finding	Limitations
1	S. Alansari et al. [14]	Proposed access management solution for cloud federated blockchains. This scheme builds ABAC policies on data while protecting users' privacy, the developers claim. The system also uses blockchain technology and Intel SGX trusted hardware to ensure the policy review process is fair.	The proposed approach consumes a lot of computation and communication resources due to the intensive Bilinear Pairing algorithm. There is also no formal security proof for the proposed system.
2	Y. Zhu et al. [24]	Proposed DAM-Chain, a revolutionary digital asset management platform The authors examine four types of ABAC access control transactions and their algorithms.	No cryptographic technique was shown to support the authors' claims. The authors propose a theoretical modal with no security proofs. Also, the algorithm for this technique is unclear.
3	Y. Zhu et al. [25]	Proposed DAM-Chain, a revolutionary digital asset management platform The authors examine four types of ABAC access control transactions and their algorithms.	No cryptographic technique was shown to support the authors' claims. The authors propose a theoretical modal with no security proofs. Also, the algorithm for this technique is unclear.
4	Dukkipati et al. [26]	Build an ABAC for IoT-based blockchain that allows users to access and control their data. The contribution describes the show, how a blockchain can be used to create access control measures.	The given approach has privacy issues and lacks explicit security evidence.
5	Wang et al. [15],	Propose an architecture that combines DSS-ILS, Ethereum, and ABE technology. Using this system, the data owner can distribute secret keys to users and encrypt shared data, allowing for fine-grained data access control.	Unfortunately, the proposed approach uses a heavy Bilinear Pairing algorithm that consumes a lot of computation and communication resources, and there is no formal security proof to ensure its security. Moreover, revealing the private key invites a barrage of attacks.
6	Ding et al. [27]	Proposed ABAC strategy for IoT. Employ blockchain technology to avoid single points of failure and data tampering. The proposed solution has proven to be resilient to threats and can be employed in IoT systems.	Using ECC consumes a lot of processing and communication resources. There is no formal security proof to guarantee the proposed scheme's security.
7	Alniamy and Taylor [16]	Developed a cloud computing architectural model that offers finer control over cloud-stored data. The ABE protects data from illegal access while letting data owners monitor and control their data. Encryption is used for data under the authority of an access control with attributes.	The authors did not provide formal security proof for this system.
8	Yang et al. [17]	Propose an IoT Blockchain-based non-interactive access management system based on PSI technology. The data owner transfers it to a cloud-based storage service provider. To access the data, the user must first create a blockchain transaction. The proposed solution protects access policy and attributes privacy while ensuring reliable access control and authentication.	The proposed approach uses a heavy Bilinear Pairing algorithm, which requires a lot of computation and communication resources.
9	Jiang [28]	Introduced smart contract-based access control, which eliminates the importance of a central trusted server and instead uses the blockchain to complete access authorization.	Though the given scheme contains a security issue and uses a lot of computation and communication resources.
10	Liu et al. [18]	Proposed a revocable ABAC system for blockchain applications. The design approach allows for ABAC and user revocation.	The proposed approach uses a heavy Bilinear Pairing algorithm, which requires a lot of computation and communication costs.
11	Rouhani et al. [19]	ABAC (ABAC) on blockchain will allow reliable auditing of access attempts. An example of the proposed technique's effectiveness is a self-contained digital library.	The proposed approach uses a heavy Bilinear Pairing algorithm, which requires a lot of computation and communication resources.
12	Amal et al. [29]	Revealed blockchain-based ABAC and fine-grained access control, which maintains user privacy and accountability. This study examines the threat model.	The proposed approach consumes a lot of computation and communication resources due to the intensive Bilinear Pairing algorithm. There is also no formal security proof for the proposed system.

(*continued on next page*)

5.3. Comparisons through security properties

This section compares the various blockchain-envisioned attribute-based access control schemes, as indicated in Table 4. In Table 6, we have outlined the security properties of various types of blockchain-envisioned attribute-based access control schemes. These security properties include confidentiality, integrity, authentication, and scalability.

5.4. Lesson learned

After conducting a comprehensive study, we came to the conclusion that the methods recommended in the study require a substantial amount of computational and communication resources because of the cost-intensive Bilinear Pairing algorithm. Unfortunately, the authors did not provide any formal security proof to guarantee the security of their scheme. Most of their security claims were based on informal assumptions rather than formal security evidence in the Random Oracle Model or Standard Model, raising concerns about the scheme's security. Furthermore, the authors failed to meet all of the security requirements listed in Table 6, leaving room for improvement in terms of security. These limitations highlight the need for further research to develop a more secure and efficient solution.

6. Analysis of the suggested schemes

The EDAS is a widely utilized method for evaluating various potential answers and deciding which one provides the best results.

Table 4 (*continued*).

S.no	Scheme	Finding	Limitations
13	Zaidi et al. [20]	Proposed a blockchain-based ABAC approach for the IoT. IoT devices can control the user's environment and collect personal data. Smart contracts are used to automate data access, while Proof of Authority improves system performance and reduces gas usage.	The proposed approach consumes a lot of computation and communication resources due to the intensive Bilinear Pairing algorithm. There is also no formal security proof for the proposed system.
14	Lu et al. [21]	Propose using ABE with blockchain technologies to regulate IoT data access. Data encryption and ABE algorithms are used to create fine-grained access control while ensuring Internet of Things security.	The proposed method uses a sophisticated Bilinear Pairing technique that consumes computation and communication resources. There is also no explicit security proof for the proposed approach.
15	Arasi et al. [22]	Introduce a data-sharing system incorporating blockchain technology and ABAC. The author creates a trustworthy blockchain-based scheme for safe data sharing with integrity audits that maintain data integrity.	The suggested scheme relied on bilinear pairing, which suffers from many simultaneous pairing operations. Moreover, the authors provided no formal proof to back up their claims about security features.
16	Y. Zhang et al. [23]	Proposed blockchain-enabled ABAC with Confidentiality for smart healthcare systems. The proposed scheme avoids single-point failure and reduces online operations costs due to online–offline encryption. The authors provided formal security proof under the random oracle model.	This scheme sufferers from heavy consumption and Communication costs due use of BP.

Table 5
Literature summary of the ABAC schemes for blockchain.

Scheme	Cryptographic algorithm (Security hardness)	Security proof	Cost	Security tools
S. Alansari et al. [14]	Bilinear Pairing	No	High	No
Y. Zhu et al. [24]	Not Defined	No	High	No
Y. Zhu et al. [25]	Not Defined	No	High	No
Dukkipati et al. [26]	Not Defined	No	High	No
Wang et al. [15]	Bilinear Pairing	No	High	No
Ding et al. [27]	Elliptic Curve Cryptography	No	Average	AVISPA
Alniamy and Taylor [16]	Not Defined	No	High	No
Yang et al. [17]	Bilinear Pairing	Yes	High	No
Jiang [28]	Not Defined	No	High	No
Liu et al. [18]	Bilinear Pairing	No	High	No
Rouhani et al. [19]	Bilinear Pairing	No	High	No
Amal et al. [29]	Bilinear Pairing	Yes	High	No
Zaidi et al [20]	Not Defined	Yes	High	AVISPA
Lu et al. [21]	Not Defined	No	High	No
Arasi et al. [22]	Bilinear Pairing	Yes	High	No
Y. Zhang et al. [23]	Bilinear Pairing	Yes	High	No

Table 6
Comparative analysis of ABAC schemes for blockchain.

Scheme	Confidentiality	Integrity	Authentication	Scalability
S. Alansari et al. [14]	Yes	No	No	Yes
Y. Zhu et al. [24]	No	Yes	Yes	No
Y. Zhu et al. [25]	No	Yes	Yes	No
Dukkipati et al. [26]	No	Yes	Yes	No
Wang et al. [15]	Yes	Yes	No	No
Ding et al. [27]	No	Yes	No	No
Alniamy and Taylor [16]	Yes	Yes	No	No
Yang et al. [17]	Yes	Yes	No	Yes
Jiang [28]	No	Yes	Yes	No
Liu et al. [18]	Yes	Yes	No	No
Rouhani et al. [19]	Yes	Yes	No	No
Amal et al. [29]	No	Yes	Yes	Yes
Zaidi et al [20]	Yes	Yes	No	No
Lu et al. [21]	Yes	Yes	No	Yes
Arasi et al. [22]	Yes	Yes	No	Yes
Y. Zhang et al. [23]	Yes	Yes	No	Yes

Table 7
Performance metrics of suggested schemes.

Scheme	Cost efficiency	Security proof	Confidentiality	Authentication
Alansari et al. [14]	0.5	1	0	1
Y. Zhu et al. [24]	0	1	1	0
Y. Zhu et al. [25]	0	1	1	0
Dukkipati et al. [26]	0	1	1	0
Wang et al. [15]	0.5	1	0	1
Ding et al. [27]	1	1	1	0
Alniamy and Taylor [16]	0	1	0	1
Yang et al. [17]	0.5	0	0	1
Jiang [28]	0	1	1	0
Liu et al. [18]	0.5	1	0	1
Rouhani et al. [19]	0.5	1	0	1
Amal et al. [29]	0.5	0	1	0
Zaidi et al [20]	0	0	0	1
Lu et al. [21]	0	1	0	1
Arasi et al. [22]	0.5	0	0	1
Y. Zhang et al. [23]	0.5	1	1	0

This technique, initially presented by Gorhabaee et al. [41], assesses two functions, namely Positive Distance from Average and Negative Distance from Average. EDAS is a method of Multiple-Criteria Decision-Making that determines the best alternative by calculating the distance between each solution and the average solution [42,43]. EDAS calculates the distance between each solution and the average solution. Comparative analysis is a common application of EDAS used to resolve conflicting criteria [43]. The Table 7 compares the various performance indicators that have been specified. In this scenario, the EDAS methodology is applied to determine which values for the four procedures will produce the best results in light of the parameters that have been chosen. In addition, a ranking of the existing schemes is determined by employing evaluation scores denoted by the symbol (μ) based on selected qualities. The performance matrices of the earlier systems are compared to one another in Table 7.

Note: we assumed the following values to be added to fuzzy-based EDAS for the chosen parameters i.e., Cost Efficiency, Security Proof, Confidentiality and Authentication,

Step One (Average Solution): In step one, the average of the selected matrices is calculated.

$$(\phi) = [\theta_b]_1 * \beta \tag{1}$$

Table 8
Average of the selected matrices.

Criterion	Non-beneficial	Beneficial	Beneficial	Beneficial
Scheme	Cost efficiency	Security proof	Confidentiality	Authentication
Alansari et al. [14]	0.5	1	0	1
Y. Zhu et al. [24]	0	1	1	0
Y. Zhu et al. [25]	0	1	1	0
Dukkipati et al. [26]	0	1	1	0
Wang et al. [15]	0.5	1	0	1
Ding et al. [27]	1	1	1	0
Alniamy and Taylor [16]	0	1	0	1
Yang et al. [17]	0.5	0	0	1
Jiang [28]	0	1	1	0
Liu et al. [18]	0.5	1	0	1
Rouhani et al. [19]	0.5	1	0	1
Amal et al. [29]	0.5	0	1	0
Zaidi et al [20]	0	0	0	1
Lu et al. [21]	0	1	0	1
Arasi et al. [22]	0.5	0	0	1
Y. Zhang et al. [23]	0.5	1	1	0
Average	0.3125	0.75	0.4375	0.5625

While

$$= \frac{\sum_{i=1}^{y} X_a b}{y}. \tag{2}$$

In the previous step, the performance of the selected metrics was assessed as the criteria for recommending solutions. The outcome of the calculations from Eqs. (1) and (2) can be combined to create a (π) value for each evaluation result on each chosen metric. The results are displayed in Table 8.

Step Two (Positive Distance from Average (PD_{avg})): The (PD_{avg}) is obtained by using the following mathematical formula.

$$PD_{avg} = [(PD_{avg})_{ab}]_{\beta*\beta} \tag{3}$$

If the state bth is favorable, then

$$(PD_{avg})_{ab} = \frac{MAX(0,(Ave_b - X_{ab}))}{Ave_b} \tag{4}$$

And for less favorable, it becomes;

$$(PD_{avg})_{ab} = \frac{MAX(0,(X_{ab} - Ave_b))}{Ave_b} \tag{5}$$

The final outcome of this calculation is presented in Table 9.

Step Three (Negative Distance from Average (ND_{avg})): In this step, the (ND_{avg}) is calculated using the following mathematical equations.

$$ND_{avg} = [(ND_{avg})_{ab}]_{\beta*\beta} \tag{6}$$

If the bth criterion is more favorable than

$$(ND_{avg})_{ab} = \frac{MAX(0,(Ave_b - X_{ab}))}{Ave_b} \tag{7}$$

And less desirable, then the given above equations become

$$(ND_{avg})_{ab} = \frac{MAX(0,(X_{ab} - Ave_b))}{Ave_b} \tag{8}$$

"The bth rated algorithm from the average value of the ath rating performance matrix is represented by $(ND_{avg})_{ab}$, as displayed in Table 10". Step Four (Weighted Sum of the Positive Distance $WSPD_{avg}$):

Table 9
Positive Distance from Average.

Scheme	Cost efficiency	Security proof	Confidentiality	Authentication
Alansari et al. [14]	0	0.333333333	0	0.777777778
Y. Zhu et al. [24]	1	0.333333333	1.285714286	0
Y. Zhu et al. [25]	1	0.333333333	1.285714286	0
Dukkipati et al. [26]	1	0.333333333	1.285714286	0
Wang et al. [15]	0	0.333333333	0	0.777777778
Ding et al. [27]	0	0.333333333	1.285714286	0
Alniamy and Taylor [16]	1	0.333333333	0	0.777777778
Yang et al.	0	0	0	0.777777778
Jiang [28]	0	0.333333333	1.285714286	0
Liu et al. [18]	0	0.333333333	0	0.777777778
Rouhani et al. [19]	0	0.333333333	0	0.777777778
Amal et al. [29]	0	0	1.285714286	0
Zaidi et al [20]	1	0	0	0.777777778
Lu et al. [21]	1	0.333333333	0	0.777777778
Arasi et al. [22]	0	0	0	0.777777778
Y. Zhang et al. [23]	0	0.333333333	1.285714286	0

Table 10
Negative Distance from Average.

Scheme	Cost efficiency	Security proof	Confidentiality	Authentication
Alansari et al. [14]	0.6	0	1	0
Y. Zhu et al. [24]	0	0	0	1
Y. Zhu et al. [25]	0	0	0	1
Dukkipati et al. [26]	0	0	0	1
Wang et al. [15]	0.6	1	1	0
Ding et al. [27]	2.2	0	0	1
Alniamy and Taylor [16]	0	0	1	0
Yang et al. [17]	0.6	1	1	0
Jiang [28]	0	0	0	1
Liu et al. [18]	0.6	0	1	0
Rouhani et al. [19]	0.6	0	1	0
Amal et al. [29]	0.6	1	0	1
Zaidi et al [20]	0	1	1	0
Lu et al. [21]	0	0	1	0
Arasi et al. [22]	0.6	1	1	0
Y. Zhang et al. [23]	0.6	0	0	1

In this stage, the $WSPD_{avg}$ for the designated schemes is considered, as demonstrated in Table 11.

$$WSPD_{avg} = \sum_{b=1}^{y} \gamma_b PD_{ab} \tag{9}$$

Step Five (Weighted Sum of the Negative Distance $WSND_{avg}$): The $WSND_{avg}$ for the chosen scheme is calculated in this stage using the formula provided. The results are presented in Table 12.

$$WSND_{avg} = \sum_{b=1}^{y} \gamma_b ND_{ab} \tag{10}$$

Step Six (Ranking): "The scores obtained are based on the $WSPD_{avg}$ & $WSND_{avg}$, which are calculated using the rated methods specified in Eqs. (11) and (12), respectively".

$$N(WSPD_{avg}) = \frac{WSPD_{avg}}{MAX_a(WSPD_{avg})} \tag{11}$$

$$N(WSND_{avg}) = 1 - \frac{WSND_{avg}}{MAX_a(WSND_{avg})} \tag{12}$$

Table 11
The weighted sum of the Positive Distance.

Weightage	0.4	0.15	0.15	0.15	
Scheme	Cost efficiency	Security proof	Confidentiality	Authentication	$WSPD_{avg}$
Alansari et al. [14]	0	0.05	0	0.1166667	0.166667
Y. Zhu et al. [24]	0.4	0.05	0.192857	0	0.711039
Y. Zhu et al. [25]	0.4	0.05	0.192857	0	0.711039
Dukkipati et al. [26]	0.4	0.05	0.192857	0	0.711039
Wang et al. [15]	0.6	0.05	1	0.1166667	0.711039
Ding et al. [27]	0	0.05	0.192857	0	0.311039
Alniamy and Taylor [16]	0.4	0.05	0	0.1166667	0.634848
Yang et al. [17]	0	0	0	0.1166667	0.116667
Jiang [28]	0.4	0.05	0.192857	0	0.711039
Liu et al. [18]	0.05	0	0	0.1166667	0.234848
Rouhani et al. [19]	0.05	0	0	0.1166667	0.234848
Amal et al. [29]	0	0	0.192857	0	0.192857
Zaidi et al [20]	0.4	0	0	0.1166667	0.584848
Lu et al. [21]	0.4	0.05	0	0.1166667	0.566667
Arasi et al. [22]	0	0	0	0.1166667	0.116667
Y. Zhang et al. [23]	0	0.05	0.192857	0	0.311039

Table 12
The weighted sum of the Negative Distance.

Weightage	0.4	0.15	0.15	0.15	
Scheme	Cost efficiency	Security proof	Confidentiality	Authentication	$WSND_{avg}$
Alansari et al. [14]	0.24	0	0.15	0	0.54
Y. Zhu et al. [24]	0	0	0	0.15	0.15
Y. Zhu et al. [25]	0	0	0	0.15	0.15
Dukkipati et al. [26]	0	0	0	0.15	0.15
Wang et al. [15]	0.24	0	0.15	0	0.39
Ding et al. [27]	0.88	0	0	0.15	1.03
Alniamy and Taylor [16]	0	0	0.15	0	0.15
Yang et al. [17]	0.88	0.15	0.15	0	0.69
Jiang [28]	0	0	0	0.15	0.15
Liu et al. [18]	0.24	0	0.15	0	0.39
Rouhani et al. [19]	0.24	0	0.15	0	0.39
Amal et al. [29]	0.24	0.15	0	0.15	0.39
Zaidi et al [20]	0	0.15	0.15	0	0.30
Lu et al. [21]	0	0	0.15	0	0.30
Arasi et al. [22]	0.24	0.15	0.15	0	0.69
Y. Zhang et al. [23]	0.24	0	0	0.15	0.39

"The score values are derived from the normal distribution of $N(WSPD_{avg})$ & $N(WSND_{avg})$, which are calculated based on the evaluation scores (μ) of the rated schemes as specified in Eq. (13)".

$$\mu = \frac{1}{2}(NWSPD_{avg} - NWSND_{avg}) \tag{13}$$

where $0 \leq \mu \geq 1$

"The ultimate result of μ is calculated based on the combined values of both $WSPD_{avg}$ & $WSND_{avg}$ as shown in Table 13".

The aforementioned methodology is utilized in this section to address a case study on diverse, efficient scheme selections, including the works of Yang and Wang [17], R. Nidhya et al. [21], Ullah et al. [39], and Tao Wan et al. [12]. Eqs. (1) and (2) were subsequently employed to derive the objective weights for all decision matrices acquired from the chosen parameters. Ultimately, the collective weights were computed by taking the average of the objective weights assigned to each criterion. Table 7 presents the weights assigned to individual objectives and the combined weights for all objectives. Subsequently, the mean decision matrix was formulated, and the outcomes are presented in Table 8. The mean solution was subsequently computed using Eqs. (3)–(6), as illustrated in Table 5, which also includes the precise value. The PDA and NDA values were computed utilizing Eqs. (7) and (8), respectively, and are presented in Tables 9 and 10. In Eqs. (9) and (10) are utilized to compute the weighted sum of PDA and Weighted NDA for multiple alternatives. In Eqs. (11) and (12) are utilized to compute the $WSND_{avg}$ and $N(WSND_{avg})$. After performing defuzzification on the evaluation score, the alternatives were ranked using Eq. (13). The process described earlier calculates the value and determines the final ranking based on the selected parameters for various approaches. The results show that the solution with the highest assessment scores is the best one.

According to the findings of the EDAS technique shown in Table 13 (Ranking), the schemes [17,22–26], and [28] have higher assessment scores among the blockchain-envisioned attribute-based access control schemes. Through a comparative study using fuzzy logic-based EDAS, schemes [21,27] were found to be average regarding the selected matrices, while the rest were ranked lower, as shown in Table 11.

7. Open research challenges

This section outlines several potential research challenges that blockchain-envisioned ABAC schemes may face.

7.1. Cost-effective approach

Designing a lightweight ABAC scheme that uses blockchain technology in IoT is a key challenge that must be met. The authors used

Table 13
Ranking based on the selected parameters.

Scheme	$WSPD_{avg}$	$WSND_{avg}$	$N(WSPD_{avg})$	$N(WSND_{avg})$	(μ)	Rank
Alansari et al. [14]	0.166666667	0.54	0.234398782	0.475728155	0.854368932	6
Y. Zhu et al. [24]	0.711038961	0.15	1	0.854368932	0.927184466	1
Y. Zhu et al. [25]	0.711038961	0.15	1	0.854368932	0.927184466	1
Dukkipati et al. [26]	0.711038961	0.15	1	0.854368932	0.927184466	1
Wang et al. [15]	0.234848485	0.39	0.330289193	0.621359223	0.475824208	5
Ding et al. [27]	0.311038961	0.15	0.437442922	0	0.218721461	9
Alniamy and Taylor [16]	0.634848485	0.15	0.892846271	0.854368932	0.873607602	2
Yang et al. [17]	0.711038961	0.15	1	0.854368932	0.927184466	1
Jiang [28]	0.711038961	0.15	1	0.854368932	0.927184466	1
Liu et al. [18]	0.234848485	0.39	0.330289193	0.621359223	0.475824208	5
Rouhani et al. [19]	0.234848485	0.39	0.330289193	0.621359223	0.475824208	7
Amal et al. [29]	0.192857143	0.69	0.271232877	0.330097087	0.300664982	8
Zaidi et al [20]	0.584848485	0.3	0.822526636	0.708737864	0.66563225	4
Lu et al. [21]	0.584848485	0.3	0.79695586	0.708737864	0.76563225	3
Arasi et al. [22]	0.711038961	0.15	1	0.854368932	0.927184466	1
Y. Zhang et al. [23]	0.711038961	0.15	1	0.854368932	0.927184466	1

bilinear pairing and Elliptic Curve Cryptosystems (ECC) to solve this problem. Bilinear pairing, on the one hand, is hampered by the fact that it requires a lot of computation. To make computation easier, the ECC employs a 160-bit key. A 160-bit key, on the other hand, is still out of reach for machines with limited resources that create enormous amounts of random data. For this purpose, a new scheme must be constructed while keeping the shortcomings of the bilinear pairings and ECC.

7.2. Provable security

When examining the security of a technique, the overwhelming majority of authors prefer to use informal and very descriptive forms. This means that no standard procedures (i.e., standard model or ROM) are employed to evaluate or demonstrate the security of the proposed schemes. The authors develop scenarios to demonstrate the schemes' security or describe their individual elements and how they work together to provide the schemes' security and resilience to various attacks. There is no formal evidence to back any of the authors' assertions regarding the security properties of the existing access control schemes for blockchain; hence they made a fraudulent claim about the security proof of the existing systems. Designing lightweight provable secure access control schemes for Blockchain-enabled IoT applications under ROM or standard model is still an open challenge.

7.3. Efficient resource management

Efficient Resource Allocation and Utilization in IoT Devices: Resource management poses a significant challenge in IoT devices with limited resources. The optimal performance of an Attribute-Based Access Control (ABAC) scheme relies heavily on the efficient allocation and utilization of computational power, memory, and energy resources. It is imperative to thoroughly evaluate and implement dynamic resource allocation, power optimization, and workload distribution strategies.

7.4. Cost consumptions

Computation and communication costs are key performance indicators. As a result of the restricted processing capacity available on IoT nodes, the design strategies must be as computationally efficient. The most common computation cost calculation method is to time the required operations. The ABAC access control schemes for blockchain proposed in the literature consumed high Computation and communication costs due to the use of large numbers and heavy operations of bilinear pairing and ECC such as hashing, encryption, signing, point multiplication, etc. Designing robust security and lightweight technique more appropriate for Blockchain-enabled IoT applications is still challenging for the research community.

7.5. Transfer and verification of access right

The transfer and verification of secure access rights pose significant challenges in facilitating the seamless exchange of access privileges between entities. To maintain the integrity of access control, it is imperative to implement robust mechanisms that strictly transfer access rights solely to authorized entities, thereby effectively preventing any unauthorized access or tampering. Developing robust and reliable protocols and cryptographic methodologies to ensure secure access rights transfer and verification is paramount.

7.6. Complexity assumptions

In most cases, the security of an ABAC scheme can be boiled down to the complex assumptions used. It is preferable to demonstrate the security following the recognized assumptions, the form of which should be short and the complexity of which should be demonstrated. Technically, the security proofs required under the complexity assumptions of brief forms are difficult to accomplish. This is because the assumption instance provides fewer parameters, which the challengers then employ.

7.7. Security and privacy

The IoT is a network that is susceptible to numerous kinds of cyberattacks. Any security strategy designed for an Internet of Things application must address important security challenges such as integration, availability, and access control. Due to the inherent properties of blockchain technology, including digital signatures and public blockchains, integrating blockchain technology and IoT provides us with integration and availability; however, privacy and access control remain major concerns. First, the data's privacy may be compromised because the data, in the form of transactions, are added to the public ledger once verified. Despite using private keys, a great deal of public information still poses a risk to information based on a user's identification. Second, each transaction must be checked to control both authorized and unauthorized access, which causes a problem with the system's scalability. As a result, we must design an access control solution capable of maintaining real-time data transmission, minimizing the latency it experiences, and eliminating unnecessary overheads.

8. Conclusion

Blockchain technology has recently been integrated into access control protocols for a more robust security mechanism. The Internet of Things and blockchain-based access control serve as the foundation of this survey, offering a comprehensive introduction to both topics.

Additionally, several security concerns and vulnerabilities associated with access control based on blockchain technology are presented. A Comparison with related surveys has also been made. Besides, we also present a comparative analysis based on evaluation based on Distance from Average Solution (EDAS) to rank the best schemes among the suggested Blockchain Envisioned Attributes Based Access Control schemes. In conclusion, we discuss some open research challenges in an Internet of Things network that uses blockchain to manage access control.

Declaration of competing interest

I, Syed Sajid Ullah with my co-authors, hereby declare that I have no conflicts of interest to disclose

I confirm that no relationships or affiliations may have influenced or could be perceived as potentially influencing the research conducted or the content presented. Moreover, there is no ethical issue in our survey paper.

I assure you that all information provided in this declaration is true and accurate to the best of my knowledge. I understand that should any conflicts of interest arise or become apparent after the submission of this statement, it is my responsibility to promptly inform the editors of Computer Networks.

Data availability

Data will be made available on request.

References

[1] M. Majid, S. Habib, A.R. Javed, M. Rizwan, G. Srivastava, T.R. Gadekallu, J.C. Lin, Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review, Sensors 22 (6) (2022) 2087.

[2] S. Kumar, P. Tiwari, M. Zymbler, Internet of things is a revolutionary approach for future technology enhancement: a review, J. Big Data 6 (1) (2019) 1–21.

[3] S. Hussain, S.S. Ullah, I. Ali, J. Xie, V.N. Inukollu, Certificateless signature schemes in industrial internet of things: A comparative survey, Comput. Commun. 181 (2022) 116–131.

[4] N. Kashmar, M. Adda, M. Atieh, From access control models to access control metamodels: A survey, in: InFuture of Information and Communication Conference, Springer, Cham, pp. 892–911.

[5] S. Osborn, Mandatory access control and role-based access control revisited, in: Proceedings of the Second ACM Workshop on Role-Based Access Control, pp. 31–40.

[6] R. Ghazal, A.K. Malik, N. Qadeer, B. Raza, A.R. Shahid, H. Alquhayz, Intelligent role-based access control model and framework using semantic business roles in multi-domain environments, IEEE Access 8 (2020) 12253–12267.

[7] V.C. Hu, D.F. Ferraiolo, R. Chandramouli, D.R. Kuhn, Attribute-Based Access Control, Artech House, 2017.

[8] S. Kaiwen, Y. Lihua, Attribute-role-based hybrid access control in the internet of things, in: InAsia-Pacific Web Conference, Springer, Cham, 2014, pp. 333–343.

[9] N. Ye, Y. Zhu, R.C. Wang, R. Malekian, Q.M. Lin, An efficient authentication and access control scheme for perception layer of internet of things.

[10] E. Yalcinkaya, A. Maffei, M. Onori, Application of attribute based access control model for industrial control systems, Int. J. Comput. Netw. Inf. Secur. 9 (2) (2017) 12–21.

[11] Y. Borse, A. Chawathe, A survey on access control in cloud computing, Int. J. Comput. Trends Technol. 59 (2) (2018) 81–84.

[12] V.C. Hu, D. Ferraiolo, R. Kuhn, A.R. Friedman, A.J. Lang, M.M. Cogdell, A. Schnitzer, K. Sandlin, R. Miller, K. Scarfone, Guide To Attribute Based Access Control (Abac) Definition and Considerations (Draft), Vol. 800, NIST Special Publ., 2013, pp. 1–54, (162).

[13] A. Ouaddah, H. Mousannif, A.Abou. Elkalam, A.A. Ouahman, Access control in the internet of things: Big challenges and new opportunities, Comput. Netw. 112 (2017) 237–262.

[14] S. Alansari, F. Paci, V. Sassone, A distributed access control system for cloud federations, in: 2017 IEEE 37th International Conference on Distributed Computing Systems, ICDCS, 2017, pp. 2131–2136.

[15] S. Wang, Y. Zhang, Y. Zhang, A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems, IEEE Access 6 (2018) 38437–38450.

[16] A. Alniamy, B.D. Taylor, Attribute-based access control of data sharing based on hyperledger blockchain, in: Proceedings of the 2020 the 2nd International Conference on Blockchain Technology (ICBCT'20), Association for Computing Machinery, New York, NY, USA, 2020, pp. 135–139.

[17] Q. Yang, M. Zhang, Y. Zhou, T. Wang, Z. Xia, B. Yang, A non-interactive attribute-based access control scheme by blockchain for IoT, Electronics 15 (2021) 1–11.

[18] X. Liu, Y.G. Zheng, X.Z. Li, A revocable attribute-based access control system using blockchain, J. Phys. Conf. Ser. 1971 (1) (2021) 012058.

[19] S. Rouhani, R. Belchior, R.S. Cruz, et al., Distributed attribute-based access control system using permissioned blockchain, World Wide Web 24 (2021) 1617–1644.

[20] S.Y.A. Zaidi, M.A. Shah, H.A. Khattak, C. Maple, H.T. Rauf, A.M. El-Sherbeeny, M.A. El-Meligy, An attribute-based access control for IoT using blockchain and smart contracts, Sustainability 13 (19) (2021) 10556.

[21] X. Lu, S. Fu, C. Jiang, P. Lio, A fine-grained IoT data access control scheme combining attribute-based encryption and blockchain, Secur. Commun. Netw. 2021 (2021) 1–13.

[22] Ad V.E. Arasi, K. Indra Gandhi, K. Kulothungan, Auditable attribute-based data access control using blockchain in cloud storage, J. Supercomput. (2022) 1–27, http://dx.doi.org/10.1007/s11227-021-04293-3.

[23] Y. Zhang, X. Wei, J. Cao, J. Ning, Z. Ying, D. Zheng, Blockchain-enabled decentralized attribute-based access control with policy hiding for smart healthcare, J. King Saud Univ. - Comput. Inf. Sci. (2022).

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

[25] Y. Zhu, Y. Qin, G. Gan, Y. Shuai, W.C.-C. Chu, TBAC: Transaction-based access control on blockchain for resource sharing with cryptographically decentralized authorization, in: 2018 IEEE 42nd Annual Computer Software and Applications Conference, COMPSAC, 2018, pp. 535–544.

[26] C. Dukkipati, Y. Zhang, L. Chieh Cheng, Decentralized, BlockChain based access control framework for the heterogeneous internet of things, in: Proceedings of the Third ACM Workshop on Attribute-Based Access Control (ABAC'18), Association for Computing Machinery, New York, NY, USA, 2018, pp. 61–69.

[27] S. Ding, J. Cao, C. Li, K. Fan, H. Li, A novel attribute-based access control scheme using blockchain for IoT, IEEE Access 7 (2019) 38431–38441.

[28] X. Jiang, A blockchain-based access control scheme, in: J. Phys.: Conf. Ser. 1955, 4th International Symposium on Big Data and Applied Statistics (ISBDAS 2021), Dali, China, 2021, pp. 21–23.

[29] A. Ghorbel, M. Ghorbel, M. Jmaiel, Accountable privacy preserving attribute-based access control for cloud services enforced using blockchain, Int. J. Inf. Secur. 2021 (2021) 1–22.

[30] Hamed Arshad, Christian Johansen, Olaf Owe, Semantic attribute-based access control: A review on current status and future perspectives, J. Syst. Archit. 129 (2022) 102625.

[31] Aghili, Seyed Farhad, Mahdi Sedaghat, Dave Singelée, Maanak Gupta, MLS-ABAC: Efficient multi-level security attribute-based access control scheme, Future Gener. Comput. Syst. 131 (2022) 75–90.

[32] S. Rouhani, R. Deters, Blockchain based access control systems: State of the art and challenges, in: IEEE/WIC/ACM International Conference on Web Intelligence, 2019, pp. 423–428.

[33] S. Nakamoto, Blockchain: a peer-to-peer electronic cash system, 2008.

[34] I. Riabi, H.K. Ayed, L.A. Saidane, A survey on blockchain based access control for internet of things, in: 2019 15th International Wireless Communications & Mobile Computing Conference, IWCMC, IEEE, 2019, pp. 502–507.

[35] F. Ghaffari, E. Bertin, J. Hatin, N. Crespi, Authentication and access control based on distributed ledger technology: A survey, in: 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services, BRAINS, IEEE, 2020, pp. 79–86.

[36] A.I. Abdi, F.E. Eassa, K. Jambi, K. Almarhabi, A.S. AL-Ghamdi, Blockchain platforms and access control classification for IoT systems, Symmetry 12 (10) (2020) 1663.

[37] M. Sookhak, M.R. Jabbarpour, N.S. Safa, F.R. Yu, Blockchain and smart contract for access control in healthcare: a survey, issues and challenges, and open issues, J. Netw. Comput. Appl. 178 (2021) 102950.

[38] H.A. Hussain, Z. Mansor, Z. Shukur, Comprehensive survey and research directions on blockchain iot access control, Int. J. Adv. Comput. Sci. Appl. 12 (5) (2021).

[39] P. Patil, M. Sangeetha, V. Bhaskar, Blockchain for IoT access control, security and privacy: a review, Wirel. Pers. Commun. 117 (3) (2021) 1815–1834.

[40] E. Abdulrahman, S. Alshehri, A. Cherif, Blockchain-based access control for the internet of things: A survey, in: 2021 IEEE Asia-Pacific Conference on Computer Science and Data Engineering, CSDE, IEEE, 2021, pp. 1–6.

[41] M.Keshavarz. Ghorabaee, E.K. Zavadskas, L. Olfat, Z. Turskis, Multi-criteria inventory classification using a new method of evaluation based on distance from average solution (EDAS), Informatica 26 (2015) 435–451.

[42] Lotfi A. Zadeh, Fuzzy Logic. Comput. 21 (1988) 83–93.

[43] G. Mehmood, M.Z. Khan, A. Waheed, M. Zareei, E.M. Mohamed, A trust-based energy-efficient and reliable communication scheme (trust-based ERCS) for remote patient monitoring in wireless body area networks, IEEE Access 8 (2020) 131397–131413.

Syed Sajid Ullah, received his master's in computer science degree (MS) from Hazara University Mansehra, Pakistan in 2020. Working as a Research Fellow in the Department of Information and Communication Technology, University of Agder, Norway. He has many publications in the fields of ICT and computer science. He is working as a reviewer in more than 20 journals. His research interests are cryptography, access control, blockchain, IoT, and Quantum Cryptography.

Vladimir Oleshchuk (Senior Member, IEEE) received the Ph.D. degree in computer science from the Taras Shevchenko Kyiv National University, Kyiv, Ukraine, in 1988, where he worked as an Associate Professor before joining the University of Agder (UiA), Norway, 1992. He is currently a professor with the Department of Information and Communication Technology, UiA. He is a senior member of the ACM. His current research interests include access control models, blockchain systems, privacy, and trust-aware applications.

Harsha S. Gardiyawasam Pussewalage (Member, IEEE) received the B.Sc. (Hons.) in engineering degree from the University of Ruhuna, Sri Lanka, in 2010, and the M.Sc. and Ph.D. degrees in information and communication technology (ICT) from the University of Agder (UiA), Norway, in 2013 and 2019, respectively. He is currently employed as an Associate Professor with the Department of ICT, UiA. His current research interests include access control models, security protocols, privacy-preserving protocols, and blockchain systems.