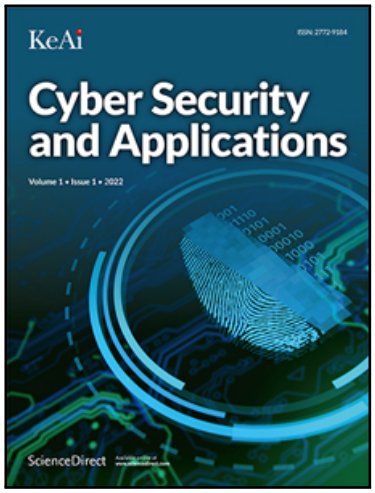
Journal Pre-proof



Securing Distributed Systems: A Survey on Access Control Techniques for Cloud, Blockchain, IoT and SDN

Lewis Golightly, Paolo Modesti, Rémi Garcia, Victor Chang

PII: S2772-9184(23)00003-6
DOI: https://doi.org/10.1016/j.csa.2023.100015
Reference: CSA 100015

To appear in: *Cyber Security and Applications*

Received date: 8 October 2022
Revised date: 25 February 2023
Accepted date: 3 March 2023

Please cite this article as: Lewis Golightly, Paolo Modesti, Rémi Garcia, Victor Chang, Securing Distributed Systems: A Survey on Access Control Techniques for Cloud, Blockchain, IoT and SDN, *Cyber Security and Applications* (2023), doi: https://doi.org/10.1016/j.csa.2023.100015

- Reviews the current state-of-the-art Access Control deployed in businesses.
- Reviews emerging and innovating Access Control in recent literature.
- Applies Access Control to four domains: Cloud, IoT, Blockchain and SDN.
- Addresses Organizational adoption strategies for Access Control.

Securing Distributed Systems: A Survey on Access Control Techniques for Cloud, Blockchain, IoT and SDN

Lewis Golightly[a], Paolo Modesti[a], Rémi Garcia[a], Victor Chang[b]

[a] *Teesside University, Middlesbrough, United Kingdom*
[b] *Aston University, Birmingham, United Kingdom*

Abstract

Access Control is a crucial defense mechanism organizations can deploy to meet modern cybersecurity needs and legal compliance with data privacy. The aim is to prevent unauthorized users and systems from accessing protected resources in a way that exceeds their permissions. The present survey aims to summarize state-of-the-art Access Control techniques, presenting recent research trends in this area. Moreover, as the cyber-attack landscape and zero-trust networking challenges require organizations to consider their Information Security management strategies carefully, in this study, we present a review of contemporary Access Control techniques and technologies being discussed in the literature and the various innovations and evolution of the technology. We also discuss adopting and applying different Access Control techniques and technologies in four upcoming and crucial domains: Cloud Computing, Blockchain, the Internet of Things, and Software-Defined Networking. Finally, we discuss the business adoption strategies for Access Control and how the technology can be integrated into a cybersecurity and network architecture strategy.

Keywords: Access Control, Distributed Systems, Security, Cloud, Blockchain, IoT, SDN

1. Introduction

In modern society, many digital innovations have transformed how organizations operate and function, creating a reliance on interconnected systems. The evolution of networking has provided businesses with efficient and cost-effective data storage, and communication solutions that have required advanced Authentication and Authorization solutions [1]. Access Control (AC) is an authorization solution to avoid data security issues by fulfilling specific security

Email addresses: l.golightly@tees.ac.uk (Lewis Golightly), p.modesti@tees.ac.uk (Paolo Modesti), r.garcia@tees.ac.uk (Rémi Garcia), victorchang.research@gmail.com/v.chang1@aston.ac.uk (Victor Chang)

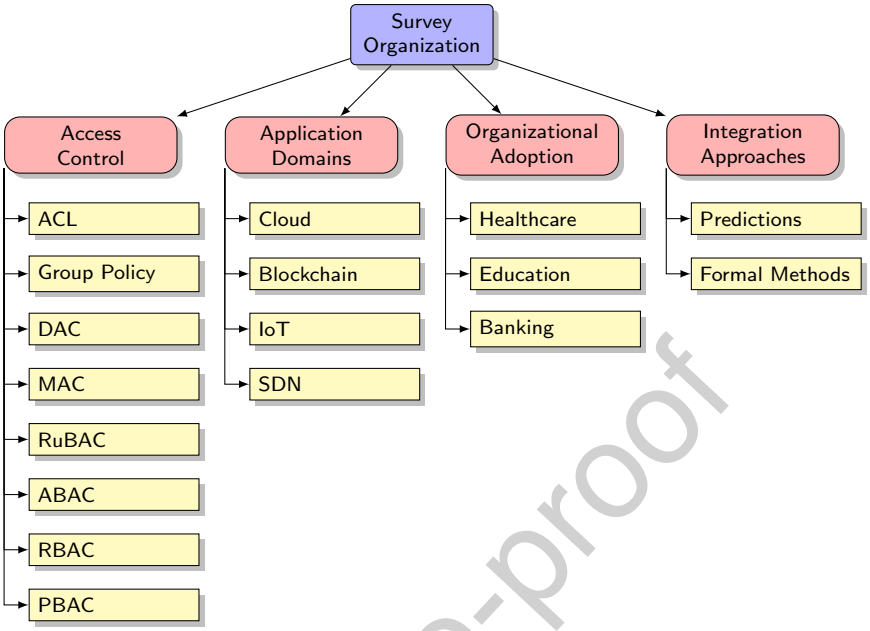


Figure 1: Survey Structure

requirements to prevent unauthorized access to different resources. As AC is a very active research area, the present survey aims to investigate existing technical solutions and application domains, considering issues around reliable digital transformation strategies for organizations and businesses.

1.1. Research Contributions

The main contributions of this paper are:

1. A review and evaluation of traditional and novel approaches on AC in light of solutions in the academic literature.
2. An analysis of innovative solutions for different application domains: Cloud Computing, Blockchain, IoT, and Software-defined Networking.
3. A discussion on organizational adoption case studies for AC in business environments.

Outline of the Paper. The structure of the paper can be observed in Figure 1 where we highlight the main topics in order. Throughout Section 2, we introduce background information on the main approaches in AC. In Section 3, this study highlights features of mainstream AC solutions, and evaluates them in Section 4. In the following sections, we review literature that illustrates novel AC solutions, respectively for Cloud computing (Section 5), Blockchain (Section 6), IoT-based

environments (Section 7) and Software Defined Networks (Section 8). In Section 9, we review case studies in key industry sectors such as Healthcare, Banking, and Education and present experiences of enterprise deployment, and in Section 10 we discuss integration of AC with other techniques. Open problems and future opportunities are discussed in Section 11.

2. Background

Access Control is a valuable technique for maintaining information security by defining who or what can see or use resources. According to the NIST [2], *Access Control* is defined as:

> *'An array of procedures or processes, usually automatic, which grants access to a specific location or information being controlled, in combination with pre-established policies and rules'.*

AC is considered by Qiu et al. [3] as the backbone of information security, even in fields including Cloud Computing and the Internet of Things. They highlight AC's ability to monitor access to resources and effectively prevent unauthorized information flow.

2.1. Fundamentals

Access Control is implemented through an authorization process built into an operating system or an application, which enforces a policy granting or denying the user access to specific data. The policy definition allows not only to specify who gets access but also what type of access should be granted.

According to Stallings and Brown [4], Access Control solutions can be developed considering three main principles:

Authentication The process of verifying that particular credentials of a user (*subject*) and different system entities are correct.

Authorization The process of granting or denying access permissions for a system resource (*object*), deciding for what purpose a subject is trusted.

Audit Independent review examining the system records or activities to enable us to understand the state of system controls. In addition, performing an audit can help to ensure compliance with the already established policies and operational procedures, detect security breaches, and provide recommendations to improve Information Security Management Systems (ISMS).

Subjects are considered accountable for the actions they have performed. There are different defined classes of users (subjects) that hold different access rights. For example, we could have:

Owner Creator of a resource (file).

Group A group of users with specific access rights in addition to the owner.

World Users who cannot access the system and are excluded from the categories *owner* or *group* for resources.

Access rights determine methods for how subjects can access objects. For example:

Read A subject can see the data in the object. The ability to copy and print is included in the Read access.

Write A subject can modify or delete data in an object.

Execute A subject can execute specific programs.

Delete A subject can delete specific objects such as files or records.

Create A subject can create new files, records, or fields.

Search A subject can list the files in the directory and search the full directory.

AC systems can be centralized or decentralized [5]:

Centralized Access Control gives subjects access to every application, website, and ad-hoc computing resource from a particular profile, using exact credentials from all locations. In addition, all data assets in control of the user are under unified identity management.

Decentralized Access Control removes the need for a determined administrator to manage or grant access to specific users in particular software or online platforms. Besides, the users do not necessarily control their credentials. For example, in Bitcoin, encryption keys are automatically generated and associated with an account.

Hu et al. [6] identify challenges in deploying AC in distributed architectures where some systems have not been created to accommodate AC. In particular, they investigate tensions caused by overly stringent rules and the risk of severe data loss with too permissive sharing. Authentication management can also be challenging due to poor coordination among independent systems.

According to Bertino et al. [7], good policies need to be consistent, relevant, minimal, and complete with respect to the activity performed by the subjects. In particular:

- *Consistency*: it is important that AC solutions also provide denials (negative policies) as well as permissions (positive policies).
- *Relevance*: there cannot be active policies that include rules that are not applicable to any activity the subjects perform; useless policies will erode cybersecurity. For example, an attacker could exploit useless rules.
- *Minimality*: it is necessary to make sure the policy does not use redundant or reducible rules. To illustrate, if a policy allows subjects to read every file in a directory, then explicitly granting read permissions to every subject on every individual file would lead to a uselessly inflated rule space.
- *Completeness*: for all actions executed from subjects in the system, there must be a corresponding policy handling those execution requests.

- *Correctness*: assures that policies comply with the development goals. Policy correctness is verified through semantic properties that depend on the application.

2.2. Related Work

Different approaches are designed to address different technical, organizational, and business needs. The main approaches, reviewed in Section 3, belong to the following families: *Discretionary Access Control* (DAC), *Mandatory Access Control* (MAC), *Attribute-Based Access Control* (ABAC), *Role-Based Access Control* (RBAC), and *Policy-Based Access Control* (PBAC).

Several surveys have been conducted to investigate state-of-the-art on AC research. Servos and Osborn [8] present a taxonomy of current AC approaches and open problems focusing on ABAC and PBAC research. Kashmar et al. [9, 10] review AC models explaining and analyzing the research challenges, considering objectives and limitations, and emphasizing current technological evolution and trends. They also review AC meta-models and compare centralized and decentralized environments.

Zhang et al. [11] consider the essential requirements for AC, presenting the current state of AC in Fog Computing focusing on DAC, MAC, RBAC, ABAC, UCON (*Usage Control-based Access Control*) and RMAC (*Reference Monitoring Access Control*). Paci et al. [12] evaluate Access Control for Community-Centered Collaborative Systems, looking at usability and performance in a controlled experiment. Parkinson et al. [13] present a security analysis of AC focusing on RBAC, DAC, MAC, and ABAC. They consider the security in real-world applications using empirical analysis.

Langaliya et al. [14] classify AC approaches into two main categories:

1. Traditional AC models (DAC, MAC, RBAC, ABAC) are compared by user convenience, performance, re-usability, role assignment, single point of failure, node overhead, and authentication methods.
2. ABE-based AC models (ABE – Attribute Based Encryption, Key Policy Atribute Based Encryption (KP-ABE), Ciphertext Policy Attribute Based Encryption (CP-ABE), Hierarchical Attribute Based Encryption (HABE), and Hierarchical Attribute - Set Based Encryption (HASBE), compared by fine-grained Access Control, efficiency, computational overhead, and collision resilience.

Various papers have reviewed Software Access Control linked to our application domains of Cloud, SDN, IoT, and Blockchain.

Ometov et al. [15] provide insights on distributed computing and compare threats and security measures for data privacy in the Cloud, Edge, and Fog layers. The cloud layer security features work with the server and users, focusing on data privacy, such as Access Control mechanisms, data encryption, and authentication features. The edge layer uses sharing information responsibility, outsourcing, and using non-fixed storage to mitigate data breaches whilst the

fog layer uses strict rules and regulations to prevent denial of service (DoS) from being performed. They define the fog layer as more robust than other layers for handling security challenges.

Ravidas et al. [16] provide an analysis of state-of-the-art authorization technologies and review opportunities for implementing Access Control into IoT. The paper suggests applying PBAC as the software mechanism, which consists of six steps for access and authorization and a four-part mechanism that uses a PAP, PDP, PIP, and PEP before granting access to the requester. The paper addresses open challenges with security adoption in this domain, as a one size fits all approach does not work due to the variations and complexity of IoT architectures. A more methodical approach is required on a case-by-case basis.

Sookhak et al. [17] convey a detailed review of granular Access Control development in Blockchain technology for the Healthcare industry by utilizing smart contracts for authorization, identification, and authentication security. They define various challenges and limitations of using Access Control with Blockchain technology, such as user and attribute revocation, the privacy of outsourced data in the cloud, scalability, and latency.

Chica et al. [18] convey a comprehensive review of SDN and security measures for their implementations. They highlight the significant quantity and variety of vulnerabilities in SDNs and how cyber-attacks that target the environment are becoming increasingly sophisticated. They also look at the opportunities for improving security in this area by using fortification through authentication and trust mechanisms in the architectural control plane by the controller understanding and authenticating trusted devices.

Our review covers traditional and novel methods for Access Control. We consider how innovations are deployed in businesses and organizations, along with a review of recent work. Moreover, we explore the application of AC to new areas such as IoT, Cloud Computing, Blockchain, and SDN. Table 1 gives an overview of the surveyed solutions for different application domains.

3. Access Control Solutions

In this section, we highlight different AC approaches (Discretionary, Mandatory, Attribute-Based, Role-Based, and Policy-Based) along with standard implementation mechanisms (Access Control Lists and Matrices, Capability Lists) and applications (Group Policies).

3.1. Access Control Lists (ACLs)

An *Access Control List* is composed of rules to grant or deny access to particular resources. An ACL is managed by one or more *Access Control Entities* (ACEs) defining the rules for a particular user or security identifier. New entries are usually appended at the end of the ACL. ACLs can be enforced in various domains, e.g. Filesystem and Networking through software or hardware solutions like Ternary Content Addressable Memory (TCAM) [50, 51] to speed

Table 1: Access Control Solutions for different application domains

Domain	RBAC	ABAC	PBAC
Cloud	Alshammari, 2021 [19] Anilkumar and Subramanian, 2021 [20] Li et al, 2012 [21]	Choi et al., 2014 [22] Fugkeaw and Sato, 2015 [23] Xue et al., 2016 [24] Gupta et al., 2020 [25] Saravanan and Umamakeswari, 2021 [24]	Ennahbaoui and Idrissi, 2021 [26]
Blockchain		Zhu et al., 2018 [27] Lin et al., 2018 [28] Lyu et al., 2020 [29] Li et al., 2020 [30] Xu, 2020 [31] Shi et al., 2021 [32] Song et al., 2021 [33] Pussewalage et al., 2018 [34]	
IoT	Mahalle et al., 2013 [35] Hussein et al., 2017 [36] Alramadhan and Sha, 2017 [37]	Saha et al., 2021 [38] Gupta et al., 2020 [39] Xiong et al., 2020 [40] Pinno et al., 2020 [41] Sun et al., 2020 [42]	
SDN	Yakasai and Guy, 2015 [43] Do Hoang et al., 2021 [44] Mattos and Duarte, 2016 [45] Al-Alaj et al., 2019 [46]	Duy et al., 2021 [44] Paladi and Gehrmann, 2019 [47] Matias et al., 2014 [48] Tseng et al., 2017 [49]	

up request processing. ACLs can be deployed in various operating systems, including the popular Linux and Windows, demonstrating flexibility as a security measure for systems and infrastructures.

User	**File A**	**File B**	**File C**	**Printer**
Alice	RW	R	R	OK
Bob	RW	RW	R	OK
Lewis	RW			OK
Paolo	R		R	
Victor			R	OK

Figure 2: Access Control Lists

3.1.1. Filesystem ACL

A Filesystem ACL restricts access to files and directories by telling operating systems what users have the authority to access particular resources and what privileges the users are granted (Figures 2 and 3). The diagram, represents the administrator being able to set specific access permissions.

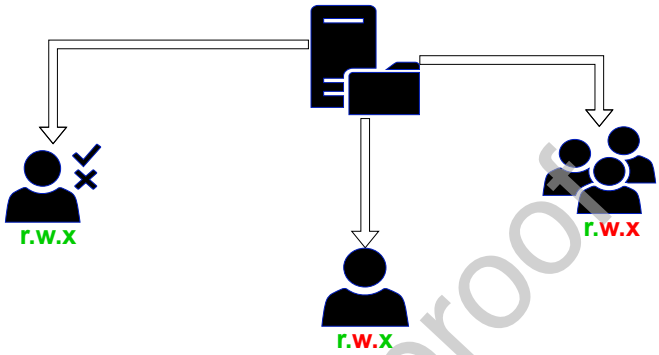


Figure 3: Filesystem ACL application example

According to Mahoney et al. [52], File-systems ACLs are an efficient and secure protection mechanism. When ACLs for File-systems are configured and deployed correctly, they are oriented around data and maintained by the data owners. In addition, the algorithm used for checking permissions appears to be particularly simple to implement and verify. However, the system scans the ACL for each initial access of an object, which is more time-consuming than accessing a table entry in an Access Control Matrix. Furthermore, understanding what files are accessible to a subject can be computationally expensive due to how the data is maintained. Hence, if a subject leaves or is reassigned, it can be necessary to search for all files associated with that user.

3.1.2. Networking ACL

Networking ACLs operate by filtering access to the network, telling network devices (e.g., routers and switches) what types of traffic and what activities are allowed (Figure 4). For example, an ACL can specify the source and destination addresses, the communication protocol (UDP or TCP), the port numbers, etc.

Pattan et al. [53] recently studied the integration of Software-Defined Networking with Active Directory, analyzing how ACLs can be used to provide a security solution in combination with a software-defined segmentation policy, grouping static and dynamic ACLs linked to the traffic. Dynamic ACLs are defined at access policy execution and are enforced in particular access sessions.

There are various known issues. ACLs are usually stored in device configurations, which can lead to complications due to the integrity or functionalities of the device. Moreover, ACLs can be altered if the device is compromised.

In general, challenges with using this technique come from network administrators' difficulties in managing ACLs in complex environments. For example,

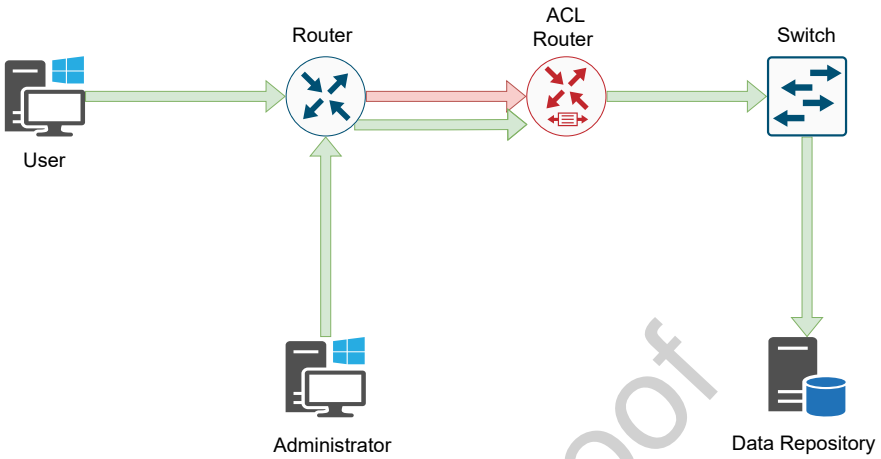


Figure 4: Example of Networking ACL application

Wakabayashim et al. [54] noticed two particular issues: 1) ACL scanning is sometimes done ineffectively in linear time for every incoming piece of data. 2) Inefficient or redundant rules can also appear. Rules are defined as unnecessary when they target packets that are not appearing throughout real traffic. A rule is unnecessary when other preceding rules already handle its packet targets.

3.2. Capability List (CL)

A *Capability List* can be a token or ticket granting access for the subject to objects in the computer system. The subject is evaluated against the capability list before being granted access to the specific object (Figure 5).

User	File A	File B	File C	Printer
Alice	RW	R	R	OK
Bob	RW	RW	R	OK
Lewis	RW			OK
Paolo	R		R	
Victor			R	OK

Figure 5: Capability List

3.3. Access Control Matrix

An (A)CL can be generalized to an *Access Control Matrix*. According to Huang et al. [55], the mechanism is implemented as an array of cells with a column for each object and a row for each subject. An entry in a particular cell is the subject access mode on corresponding objects. A column represents an object access list; a row is equivalent to a subject access profile (Figure 6).

User	File A	File B	File C	Printer
Alice	RW	R	R	OK
Bob	RW	RW	R	OK
Lewis	RW			OK
Paolo	R		R	
Victor			R	OK

Figure 6: Access Control Matrix

3.4. Group Policy

Group Policies are a feature of UNIX-like and Microsoft Windows operating systems, including distributed environments such as Microsoft Active Directory, that have authority over subject accounts' working environment. Group Policies provide centralized management and configuration for operating systems, user settings, and applications to allow efficient ACL management. As discussed in [56], group policies can be used when various users interact with the AC system. Inside the group, users share common permissions. Figure 7 describes the capability of the Administrator to add a new policy to the Group Policy, which is then performed through Active Directory to multiple users, Desktop PCs and servers.

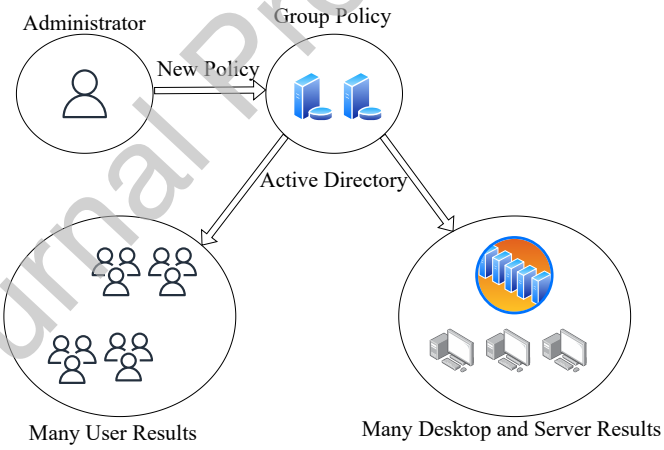


Figure 7: Group Policy application example

Stöckle et al. [57] investigated the use of automation to implement Windows security in large-scale and complex modern systems. Such complexity creates opportunities for attackers to exploit the system when a misconfiguration or vulnerability is present. Many organizations cannot efficiently control all the aspects of a process that relies on the manual configuration of ACLs and group policies, with rules added and removed at different moments by different system administrators. The authors present a proof-of-concept implementation and

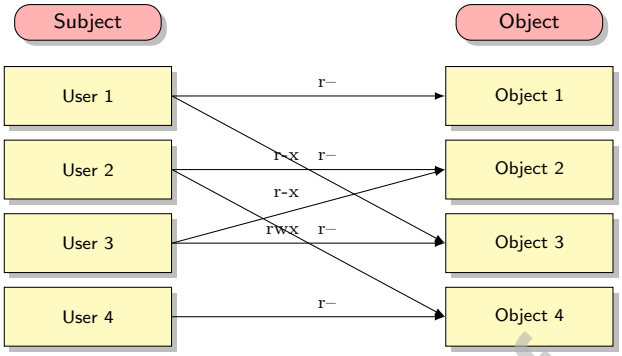


Figure 8: DAC Model

documentation to automate the process and run consistency checks to minimize the risk of misconfiguration that administrators can inadvertently introduce.

3.5. Discretionary Access Control (DAC)

Discretionary Access Control is an authorization technique processing the requester identity or rules of access (authorizations) by utilizing evaluation criteria provided by trusted computer systems to limit object access (Figure 8).

DAC is implemented using ACLs, considered a viable AC solution when the number of users and resources is small. DAC is the most common AC solution for Windows and UNIX-like operating systems. However, it presents several drawbacks in Cloud-based environments, as discussed by Gagandeep and Arvinder [58]. Firstly, the inability to facilitate the management of processes at the admin level. Secondly, an object owner granting access to the object to other users could create a security issue. Thirdly, complex auditing plays a role. Under a DAC system, keeping track of the data is challenging since it is not a centralized system, only allowing administrators to monitor each ACL's local flow.

DAC relies on the system's maintenance of the ACL. There is a need for constant granting and revoking of AC permissions. Moreover, DAC has minimal negative authorization power. El Sibai et al. [59] discuss a significant drawback in the lack of control over the flow of information. Indeed, data can be duplicated between objects, which allows unauthorized subjects to access data copies even when the owner has not allowed a subject to access the original data.

3.6. Mandatory Access Control (MAC)

Mandatory Access Control is often used in businesses with strict security requirements, such as governments and public services. MAC controls access by comparing security labels, which carry the status of sensitivity or criticality of system resources. This requires creating different security clearance levels and associating objects in the system with one of these security levels. In practice,

every object may be assigned a label such as: *Unclassified*, *Confidential*, *Secret*, or *Top Secret*. Access above a subject's own clearance is denied (Figure 9).

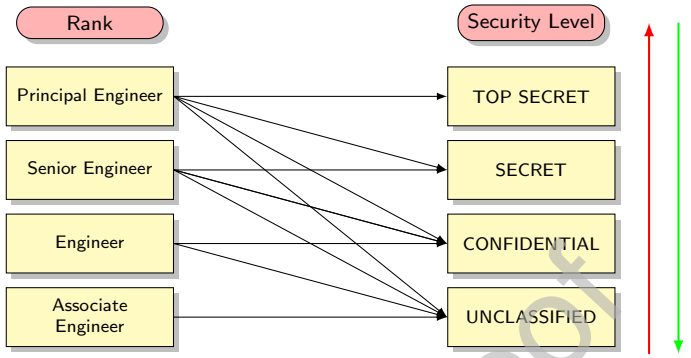


Figure 9: MAC Model

MAC uses subject clearance, and object labels for system-enforced Access Control [60]. Labeling objects consists of pre-defining their security level. This means subjects cannot modify the permissions as only the administrator can. For example, they cannot grant access to other users to the objects they have access to. MAC is known to have open problems. Firstly, MAC creates a significant demand for maintenance to update the list with user base expansion and turnover during business development. The solution also scales poorly, as new users and information require constant updates for objects and account configurations. The main limitations of MAC technology have been discussed by El Sibai et al. [59]. In particular, MAC cannot have fine-grained Access Control or duty separation. In addition, deploying a MAC solution is costly and complex due to the high reliance on trusted components and applications for MAC labels and properties.

3.6.1. Rule-based Access Control

Rule-based Access Control (RuBAC) evolves from a traditional MAC approach. This overcomes limitations in managing complex permissions that the original solution cannot handle. A semantic rule-based extension model to handle access policies is presented in [61]. Another example of a rule-based approach is the *Lattice-based Access Control* (LBAC), where lattices are used to define a multi-layer security policy. A specific application to healthcare systems is presented in [62]. The combination of sensitivity levels and other categories for objects equates to security levels. These are demonstrated as lattices that detail the hierarchical relationships of the security levels. When a security level is affected by subjects and objects:

- The security level associated with objects reflects the security classification.

- The security level associated with objects provides classification using the stored information.
- The security level associated with the subject is determined by information sensitivity.
- Subjects in the same category have the same security clearance level.

3.7. Attribute-Based Access Control (ABAC)

In *Attribute-based Access Control* (Figure 10), access and authorization are determined by attributes related to a subject and accessed object. All objects and subjects have a set of related attributes like *Location*, *Creation*, and *Access Rights*. Access to objects is granted or denied depending on if there is a matching between object and subject attributes.

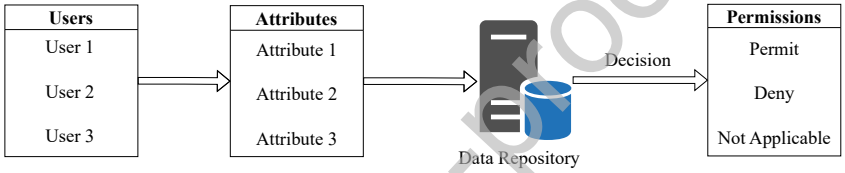


Figure 10: ABAC Model

Vijayalakshmi and Jayalakshmi [63] consider ABAC a flexible and efficient solution to establish security rules or policies based on attributes or environmental conditions.

An ABAC limitation is the challenging auditing. For security and regulatory compliance, it is imperative to see precisely what resources a user has access to. Compared to other approaches, such as RBAC, where the administrator can look at assigned user privileges, ABAC does not allow looking up users' access permissions. Thus, it requires checking every object against the access policy. Finally, technology can be very complex. It takes administrators a significant amount of time to specify many policies to determine what attributes users must have to access the resources. Servos and Osborn [8] highlight multiple problems primarily due to the technique's relative infancy, as the complex systems struggle to provide flexible and granular AC policies.

To mitigate the challenges and constraints of ABAC, hybrid ABAC models, and frameworks have been considered. Ding et al. [64] presented a novel ABAC solution utilizing Blockchain for the Internet of Things (IoT). The research addresses the increasing need for security in IoT systems, as prior solutions cannot cope with IoT's highly demanding and complex architecture. The proposed model includes attribute authorities, Blockchain managers, and distributors of attributes. The system works by applying a transaction related to an attribute, reaching a consensus, and then writing a new block into the Blockchain. The model provides a decentralized and scalable AC system that requires less trust, making the existing system more robust.

3.8. Role-based Access Control (RBAC)

Role-based Access Control gives access and authorization utilizing user roles. This gives subjects implicit and explicit permissions for a particular role. Role permissions are inherited using role hierarchy and determine the permissions required to execute explicit operations, as shown in Figure 11. Specific roles can be given to one or multiple users. Unlike other AC solutions, it can be used to establish a company-wide security policy that goes beyond the capabilities of ACLs, defining how users can modify a file.

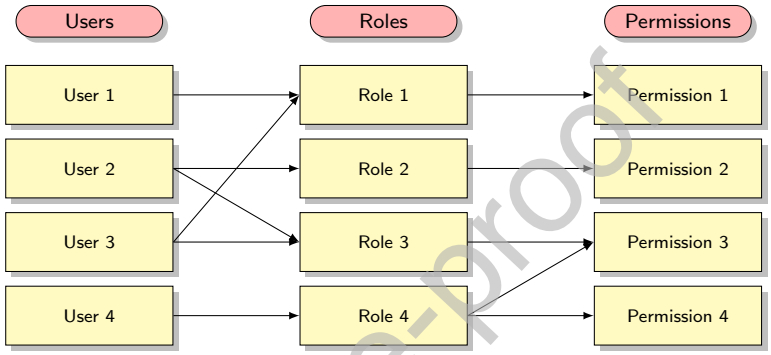


Figure 11: RBAC Model

Different RBAC approaches have been proposed:

- **Flat** This model uses the three primary rules of RBAC. The system should support many-to-many and many-to-many permission role assignments. Users should be allowed to use the permissions of multiple roles at the same time [65].
- **Hierarchical** This model utilizes all the rules and capabilities of Flat RBAC and defines seniority between relationships. Senior roles are composed of all roles that are below them [66].
- **Constrained** This model utilizes all of the features of Hierarchical RBAC and adds support for the separation of duties (SoD). It applies when there is a requirement for more than one person to complete a task [67].
- **Symmetric** This is the highest level of RBAC deployment and has all the requirements of Constrained RBAC along with a feature of support for permission-role review [68].
- **Temporal** This extends the RBAC model and supports the enabling and disabling of roles [69].

RBAC issues and limitations include *role explosion*, as the model has difficulties scaling to meet the complex AC requirements associated with evolving businesses and strict cybersecurity regulations. RBAC also lacks Security Risk

Tolerance, which indicates the level to which the information needs to be defended against confidentiality or integrity attacks. Furthermore, the solution lacks scalability and dynamism due to focusing only on employee roles and using these as the means of authorization. Finally, implementing this technique into businesses can be expensive and complicated, depending on the scale of the organization.

Laverdière et al. [70] present the architecture of RBAC as decoupling policy enforcement and decisions with:

- a *Policy Decision Point* (PDP), which will grant or deny the requests by interpreting the policy.
- a *Policy Enforcement Point* (PEP) to communicate with the PDP and enforce policy decisions focusing on privileged actions. PEPs can be deployed across the code base, with their reach depending on specific AC policies.

The state of the art for RBAC has been evaluated by Xu et al. [71] considering its general limitations and constraints, which include having a static design and inefficiencies in updating AC policies or handling repeated encryption when securely sharing files. Using an identity-based cryptosystem, the authors propose an expressive RBAC model for the Cloud environment, particularly Cloud storage. The solution aims to enhance RBAC, improving efficiency and flexibility by adding a mechanism of role inheritance that makes the permission assignment more efficient and precise. They performed functional testing and performance analysis, demonstrating how the system can complete an array of functions, understand the dynamic AC of ciphertext data, and keep the operations completion time at an acceptable level.

3.9. Policy-based Access Control (PBAC)

Policy-based Access Control (Figure 12) provides a strategic solution for the management of subject access to multiple systems. It combines roles for subjects with policies that determine a particular role's access privileges. According to Pal et al. [72], PBAC architecture provides fine-grained AC for authorized subjects to services whilst defending resources from unauthorized access. PBAC has particular disadvantages regarding its implementation complexity and the time and resources needed to deploy many policies and attributes whilst establishing the rules.

Zong et al. [73] use PBAC for robotic applications to improve the security aspects of Robot Operating Systems, allowing the Administrator to revoke permissions dynamically. The model is designed to include Permission Categories, Policy-based AC, Identity Tokens, and Access Tokens. The Policy Engine is designed to include Policy Representation, User Identity, and Permission Revoking. The experiments demonstrate use cases such as an unauthorized operator trying to perform a task, an authorized user performing the same task, and permission revocation from the authorized group of all users except the Administrator. Majahan et al. [74] explore a hybrid PBAC, ABAC, and RBAC solution

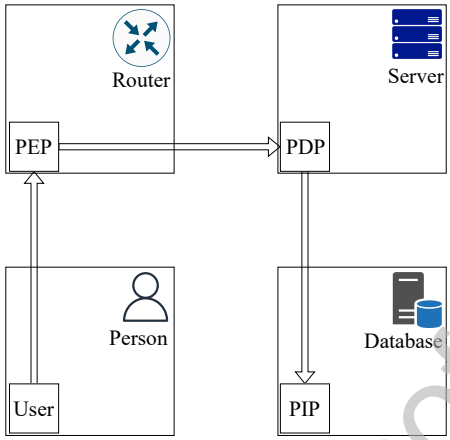


Figure 12: PBAC Model

(PAR-AC), to perform efficient management and utilization of resources. It consists of three steps: (1) New subject registration, (2) For current users, login (policy-based authentication), and (3) After authentication, an AC mechanism grants specific privileges to users, depending on their clearance level.

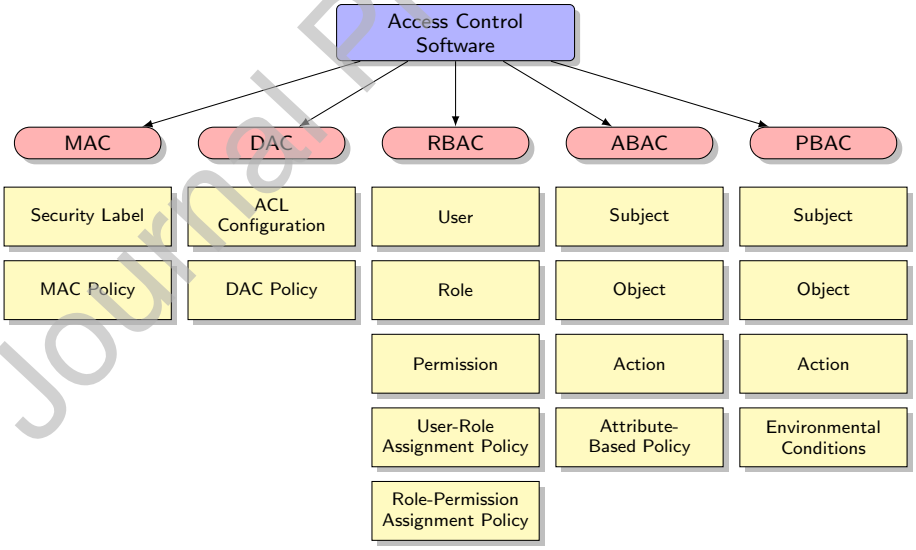


Figure 13: Access Control Taxonomy

4. Access Control Solutions Evaluation

In this section, we evaluate different Access Controls methods (Figure 13) considering the following aspects: functionalities, algorithms and data structures, advantages, disadvantages, deployment opportunities, and open problems. In Table 2, we summarize the main aspects regarding algorithms, data structures and their functionalities.

4.1. ACL

Functionalities. ACLs provide fine-grained control over network traffic by limiting access to sensitive resources to only authorized users. This helps to enhance network performance by preventing unauthorized users from consuming resources [97].

Algorithms and Data Structures. ACLs use capability lists to specify the set of permissions that a given subject has for each object. ACLs can be managed using Active Directory or network hardware, or by using modern implementations based on relational databases [75, 4]. Various optimization techniques can be applied to ACLs to reduce packet latency without compromising security requirements [76].

Advantages and Disadvantages. ACLs offer a simple and transparent model for system administrators to control access to specific objects, and it is easy to modify the ACLs to update access policies. ACLs can be efficient when dealing with long lists of subjects as logarithmic search is possible in most cases. However, managing ACLs can be complex, especially in large networks with many resources and users [98].

Open Problems. ACLs can grant write access to a specific file, but do not provide fine-grained control over how the user can modify the file, which can lead to data loss or corruption [99].

Deployment Opportunities. ACLs have lower computational overhead compared to stateful firewalls, and can be implemented on various platforms such as Windows, Linux, and routing hardware. To provide comprehensive security, ACLs should be deployed on all network interfaces [100].

4.2. DAC

Functionalities. DAC allows subjects to manage their own data and efficiently access data belonging to other subjects. It enables subjects to autonomously develop parameters for access, and its maintenance is relatively simple. Every piece of data can have individual access restrictions, and access to objects is restricted based on the identity of the subjects. DAC is typically implemented using Access Control Lists (ACLs) and is centrally controlled (Atlam et al. [101]).

Table 2: Access Control Algorithms and Data Structures

AC Model	Data Structure	Algorithms	Functionalities
ACL	Capability Lists, Access Lists [75], Relational Database [4]	Rule Boundary, Removing Shadow Rules, Removing Covered Rules, Combining Rules [76]	The algorithms find rules that can be removed safely, including shadow and covered rules. They also reorder the rules in the ACL based on the actual hit counts, hit count prediction, and rule latency [75, 76]
DAC	Tree Structure [77], Access Matrix [78, 79, 80, 81, 82], Capability List [83], Authorization Table [4]	Critical Set Detection (CSD) [84]	Authorizations contain temporal intervals of validity automatically revoking authorization at expiration time [84]
DAC (Bell-Lapadula)	Tree Structure [77], Access Matrix, Capability List [83], Authorization Table [4]	Discretionary Security Property [85]	This implements discretionary policies to execute particular actions on resources using capability tickets [86]
MAC	Lattice [87]	Digital Signature [88]	The Kernel checks the digital signature associated with each readable and executable file [88]
MAC (Bell-LaPadula, Biba Integrity)	Lattice [87]	*(STAR) Security Property, Simple Integrity Axiom (SI Axiom) [89, 90]	The models enforce reversed policies: Biba prohibits writing from the lower levels as well as reading from higher levels to lower levels whereas Bell-LaPadula forbids writing from the higher levels and reading from the lower levels [91]
ABAC	Policy Matrices, Logs [4, 92]	Attribute Extraction, Relation Extraction, Rule Pruning, Policy Refinement [93]	This provides extraction of algorithms, relations, and rules from the data store as well as refining policies for enhanced maintenance and policy quality [93]
RBAC	Permission Lists [94], Access Matrix, Hierarchical tree [4]	URA97, PRA97, RRA97 [95]	URA97 focuses on the user role assignment, PRA97 focuses on the permission role assignment and RRA97 focuses on the role-role assignment [95]
PBAC	Policy Matrices [4]	Retrieving Data Resource Catalog [96]	Provides privileges differentiation services for a significant quantity of users, and resource content [96]

Algorithms and Data Structures. In file systems, permissions can be applied in a folder tree structure [102]. Each subject has an Access Matrix, where each column links to an object, and each cell contains a set of access rights. The storage for the rows in the matrix is known as the Capability List [83]. The algorithm used in DAC allows temporal authorization, which uses a beginning and end time for authorization [84].

Advantages and Disadvantages. DAC offers several advantages, such as allowing users to transfer ownership of an object to other subjects and enabling them to define access rights for other subjects. It also restricts subject access after repetitive authentication failures, and unauthorized subjects do not have access to object properties such as file name, size, and directory path. However, DAC has inherent vulnerabilities, such as software misconfiguration and Trojan Horse attacks. Its negative authorization power is limited, meaning it cannot restrict access to specific subjects.

Open Problems. DAC cannot ensure comprehensive security because users can share their data as they deem appropriate.

Deployment Opportunities. DAC can be used to improve compliance and allow organizations to monitor network activities.

4.3. MAC

Functionalities. The administrator can granularly define access rights to an object, and users cannot edit them. It protects against Trojan Horse attacks due to its inability to declassify data or share access to classified data. An operating system or database constrains access privileges: each subject and device on the system is assigned a classification and clearance level. This is implemented by ACLs and controlled centrally [103].

Algorithms and Data Structures. The lattice divides access into various compartments to define the levels of security for users and data [87]. The algorithm restricts modification or changes by enforcing rules. A file or executable can only be replaced with another file or executable that has the same digital signature, which can be verified using any public key in the binary with the same file name [88].

Advantages and Disadvantages. MAC provides a robust security solution as only the System Administrator can access or modify controls, resulting in fewer potential security errors. The centralized control under one authority creates a fully centralized system. However, manual configuration of security levels and clearances requires continual scrutiny by administrators, leading to poor maintainability. Additionally, this AC method cannot scale automatically, as subjects must ask for access to all new information and cannot configure access parameters for their information.

Open Problems. Complicated setup process and inflexible.

Deployment Opportunities. High-level data protection and centralized information.

4.4. ABAC

Functionalities. Dynamic Data Access is possible for flexibility and scalability with low maintenance. The attributes of specific subjects granularly restrict network access to ensure security compliance [104].

Algorithms and Data Structures. The Policy Matrices use the column headers as the user attributes to grant or deny access privileges [105]. ABAC logs can be observed to understand patterns around the subjects, resources, and environmental conditions [92]. The algorithms present matrices arrangement in the model and automate the process of generating policies through policy mining [93].

Advantages and Disadvantages. Automatically update permissions with low administration overhead and fine-grained security. Complex implementation compared to other AC models.

Open Problems. Difficult to implement, requiring hundreds of thousands of attributes to establish rules and policies.

Deployment Opportunities. Achieves higher access security beyond the limitations of access based on roles.

4.5. RBAC

Functionalities. RBAC supports simple and complex rules and restricts access according to the roles of specific subjects. There are three main steps in RBAC implementation: Role Assignment, Role Authorization, and Permission Authorization [106].

Algorithms and Data Structures. RBAC uses an Access Matrix as a table with roles in the rows and different objects and actions in the columns [107]. A Permission List stores each data object with details of who can perform specific operations on that object [108]. The Tree structure defines the role hierarchy in the system [109]. The algorithms grant and revoke a user's access, permission, and modifications between the relationships of the same types of roles [95].

Advantages and Disadvantages. RBAC improves overall security compliance, confidentiality, and privacy of resources, including personal data or systems. It also gives differentiated access to users depending on their roles, with particular permissions for each role. Security is embedded in the organizational structure and strategy. RBAC supports the separation of duties (SoD) and is flexible. However, role explosion can happen when permissions are too fine-grained, which can be costly and difficult to manage, making RBAC complex and confusing. An RBAC solution requires the administrator to have an in-depth understanding of the security map of the organization and how permissions were previously allowed before deployment. After the solution is distributed, responding to developing security threats and risks is challenging. Defining roles can be straightforward when RBAC is first implemented into the business, but adding more roles and staff can be challenging as time passes. An expanding RBAC solution can be costly, resulting in the need to scale up the infrastructure at the same rate as the personnel grows.

Open Problems. Users are only assigned permissions with roles, not objects or operations.

Deployment Opportunities. RBAC improves compliance, confidentiality, and access management standards for businesses.

4.6. PBAC

Functionalities. User roles are used in combination with attributes to determine granular individual access privileges. Rules are visible with PIPs, and decision and enforcement processes are clearly separated [110].

Algorithms and Data Structures. The Policy Matrices will use the column headers as the user attributes to grant or deny access privileges [105]. The algorithm retrieves stored access control variables, such as the user, resource, and permissions used alongside the policy points [96].

Advantages and Disadvantages. Flexible development and integration with other techniques. It is supportive of organizational scalability and compliance. Deployment can be difficult, as well as managing a high volume of requests, and with the complexity of the technology, administration management, and troubleshooting can be complex.

Open Problems. Meeting the five key criteria of Consistency, Relevance, Minimality, Completeness, and Correctness is complicated in distributed policies.

Deployment Opportunities. Appropriate for distributed workforce and collaboration.

5. Access Control for Cloud-Based Environments

Cloud computing is adopted to make computer resources available on demand, particularly data storage or computing power which works without direct user management (Figure 14). This can be demonstrated in large-scale Cloud environments containing multiple functionalities distributed over various locations.

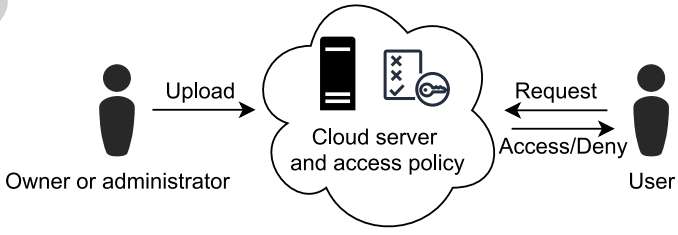


Figure 14: Cloud Access Control diagram

In Table 3, we can see some research on AC studies for Cloud environments. The research innovates on existing solutions and presents novel approaches.

Fugkeaw and Sato [23] present a solution for big data in Cloud environments. The technique is a *Collaborative - Ciphertext Policy - Attribute Role-Based Encryption* (C-CP-ARBE), which incorporates a cryptographic layer providing efficient confidentiality with big data. The evaluation assesses the technique's performance, which provides a practical AC deployment for big data hosted in a Cloud-based architecture. Future work focuses on a giant experiment to evaluate the performance of concurrent accesses on large data sets.

Xue et al. [24] introduce a *Location-aware Attribute-based Access Control* (L-ABAC) scheme for Cloud environments. The model comprises a data owner, an attribute authority, location servers, sensors, data consumers (users), and the Cloud server. They analyze the effectiveness of L-ABAC and demonstrate its small overhead for data consumers, attribute authorities, and the Cloud. There is a cybersecurity advantage of using an L-ABAC system since compromising a single server only impacts information associated with a specific location whilst other information remains confidential. Further research addresses restoration mechanisms if the specific location server is affected, including re-allocating updated location servers and secure re-encryption methods for specific data.

Gupta et al. [25] explore ABAC for Cloud-enabled industrial smart vehicles to allow location-specific and real-time notifications in smart transportation. The smart security solution integrates with a fine-grained ABAC model introducing groups as a dynamically assigned element based on the properties of the moving vehicles. Moreover, this system considers extensive policies concerning personalized privacy preferences to permit or refuse multiple activities. They use multiple real-world use cases and a prototype implementation in Amazon Web Services (AWS), which reflects the solution's usability and overall practicality. Further work aims to tackle in-vehicle AC security systems to develop trust-based risk-aware dynamic solutions.

Saravanan and Umamakeswari [111] investigate lattice-based Access Control in a Cloud environment to protect user information. They propose a novel solution using a hybrid algorithm, where the lattice is formed by using different security levels or values. They perform experiments and analyses by implementing the solution on a Cloud-based simulator (CloudSim). They used a double encryption approach using Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA). They found that the solution effectively gave users in Cloud-based environments enhanced data security.

Alshammari et al. [19] design an evaluation model based on trust that demonstrates high-reliability by implementing *Task Role-based Access Control* (T-RBAC) into a Cloud environment. It is tailored to decrease risk and create a Cloud storage system by providing enhanced security for specific attacks, including Sybil, collusion, and on/off attacks. It also enhances the system's flexibility. They utilize a range of criteria for this, including trust decline, task trust, interaction importance, conditional transfer, and subjectivity. This works by stopping a task or role in case of a data leak. Their study incorporates an effective trust model that utilizes inheritance and hierarchy in the trust evaluation of tasks and roles. The solution provides a countermeasure against specific cyber-attacks, including collusion and Sybil attacks [112], where few

entities forge other identities to compromise a significant portion of a system.

Anilkumar and Subramanian [20] propose the novel *Predicate-Based Access Control* solution using Open Stack Swift storage for Cloud-based environments. Their solution uses RBAC and provides an innovation using a fine-grained implementation of a Predicate-based Access Control solution, which automatically applies a security predicate to all queries on a table.

Ennahbaoui and Idrissi [26] present an agent-based framework that combines a robust authentication solution, a model for fine-grained AC, and a subject behavior analysis. Their framework aims to establish a dependable security policy that supports Cloud-assisted healthcare applications. Furthermore, this agent-based framework protects the provider platforms from external threats. The experiments assess the execution times of tasks, user behavior performance, and system penetration testing. They simulate the execution of common cyber threats, including the Reuse of IP addresses, Denial of Service, DNS attacks, NMAP TCP Scans, and Persistent Meterpreter Back-doors.

Choi et al. [22] criticize RBAC and *Context-aware Role-based Access Control* (C-RBAC) for being unable to ensure privacy and integrity. They propose an AC solution using context reasoning, which includes environmental context, purpose, permission level, and their conditions, purpose, and policies for administrators and users. Inside the Cloud, the subject receives authorization using inferences linked to context ontology. The model provides advantages such as more effective policy management.

Li et al. [21] introduce a refined RBAC model which can be utilized for Cloud Computing. The model revolves around three core cybersecurity principles: least privilege, separation of duties, and data abstraction. They tested multiple delivery models such as SaaS, PaaS, and IaaS. It is highlighted that Software-as-a-Service (SaaS) is the most mature service model that best complements the proposed RBAC system. RBAC can be deployed in Cloud environments and has been praised as a simple process when migrating traditional solutions to the Cloud. It has been highlighted that RBAC might not be fit for every security aspect of Cloud computing.

6. Access Control for Blockchain-Based Environments

A *Blockchain* is a distributed and decentralized data structure organized as a digital ledger that stores transactions in blocks across different systems (Figure 15). It can enhance cybersecurity, making tampering with any block extremely hard after it has been added to the Blockchain. A consensus mechanism provides integrity guarantees. Past transactions are stored, distributed, and duplicated across the network of computer systems in a way that allows the participants to monitor and verify them in a computationally inexpensive way individually. Current operations verification can involve heavy computation, especially for Proof of Work systems.

In Table 4, we can observe a variety of studies on AC for Blockchain environments. The research innovates on existing solutions and original approaches.

Table 3: Surveyed Access Control Solutions for the Cloud

Surveyed AC	AC Type	Technical Characteristics	Research Innovations
C-CP-ARBE Choi, et al., 2014 [22]	ABAC	Restricts Network Access based on the Attributes of individual users	Provides a high level of convenience and efficient policy management
L-ABAC Fugkeaw and Sato, 2015 [23]	ABAC	Roles of Users are combined with Attributes to determine individual Access privileges	With this technique, an attack on a location server only influences information linked to the location keeping other area information confidential
Cloud ABAC Gupta et al., 2020 [25]	ABAC	Developing a fine-grained ABAC system that introduces a concept of groups being dynamically associated with moving vehicles based on their specific attributes	Enabling location-specific and in-time alerts and notifications depending on the effect of execution of the Access Control policies in the system for smart transportation ITS environments
L-BAC Saravanan and Uma-makeswari, 2021 [24]	ABAC	Provides two-layer protection implementing two algorithms in a single application, mitigating vulnerabilities and protecting unauthorized access to data in the Cloud	This Access Control model has proved to be a strong cybersecurity technique making access to personal information very hard for attackers
T-RBAC Alshammari, 2021 [19]	RBAC	A User Access feature embedded into Microsoft Windows Operating Systems	Decreases risk by providing high security and improving the quality of decisions made by Cloud operators or data owners
P-BAC Anilkumar and Subramanian, 2021 [20]	RBAC	Restricts access to objects based on a subject's identity	The technology uses Swift, a storage service for objects in the cloud known as OpenStack restricting object access using ACLs
Agent-based Framework Ennahbaoui and Idrissi, 2021 [26]	PBAC	An operating system or database constraints the security clearance level of a subject	The solution provides the capacity for gathering the notions of role, task, attribute, constraint, and session, combining the authorization solution, Access Control model, and user behavior analysis
Product-lifestyle management Li et al, 2012 [21]	RBAC	Refined RBAC developed for the Cloud environment using security patterns	Extending RBAC from traditional application domains to the Cloud

Zhu et al. [27] implement ABAC into Blockchain to address digital asset management using distributed permissions. They present a novel Digital Access Management Platform (DAM-Chain) using *Transactional-Based Access Control* (TBAC). This provides an integration between the ABAC distribution model and a Blockchain, offering a method for the organization to easily find and ac-

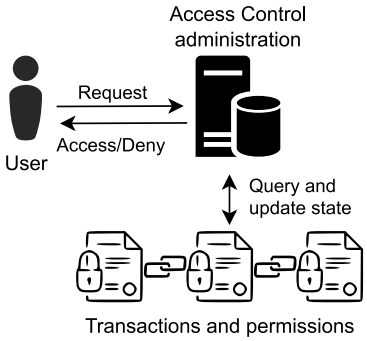


Figure 15: Blockchain-based Access Control diagram

cess digital assets consisting of three components: Asset Security, Secure Asset Issuance, and Distributed Permissions.

Lin et al. [28] present a novel framework using Blockchain for AC known as Blockchain-based Secure mutual authentication with fine-grained access control system for Industry (BSeIn), developed using cryptographic techniques such as Attribute-Based Signatures (ABS) and Multi-receiver encryption (MRE). They aim to provide cyber-resilience against the following attacks: User Impersonation attacks, Man-In-The-Middle (MITM) attacks, Data Modification attacks, Replay attacks, Denial of Service (DoS) attacks, and Distributed DoS (DDoS) attacks. They evaluate the running time of different cryptographic algorithms on several server configurations. Future research aims to explore possible optimizations using hardware or hybrid implementations.

Lyu et al. [29] propose a system called Secure Blockchain-based Access Control (SBAC). They use a mechanism with Blockchain-based access tokens which implements content AC on distribution, audition, and revocation, using access tokens transfer and access transactions. The system provides capabilities for auditing access to shared content and access decisions. They perform anti-counterfeiting and tamper-proof tests whilst also testing the system against the following cyber-attacks: Cache poisoning attacks, Cache data extraction attacks, DoS/DDoS attacks, and MITM attacks.

Song et al. [33] present *Smart-Contract based Access Control* (SCBAC). This uses ABAC to simplify and improve access management and provides a dynamic fine-grained AC method. Implementing AC systems using Blockchain through Smart Contracts highlights that the solution effectively deals with issues linked to single points of failure by achieving distributed AC and storing important data in multiple places.

Li et al. [30] developed a solution called Fine-grained Access control scheme for VANET Data based on Blockchain (FADB), a scheme for Vehicle Ad Hoc Network (VANET) data integrating Blockchain, IPFS distributed storage, and Ciphertext-based Attribute Encryption (CP-ABE). The solution is demonstrated as a platform for data-sharing that ensures data security, privacy protection,

and access restriction. FADB incorporates a new efficient encryption scheme (HECP-ABE). Combining the traditional CP-ABE encryption scheme with the Blockchain, they demonstrate the technique to enable distributed, fine-grained data-sharing services. It comprises multiple stages: user registration, data upload, and authorization access. They aim to explore future data security protection features, such as anonymity levels and stateless access.

Xu et al. [31] propose a *Blockchain-Based Secure Data-sharing platform with Fine-grained Access Control* (BDSS-FA). They propose a novel hierarchical attribute-based encryption (HABE) algorithm allowing various hierarchical authorization centers. The system model consists of a Key Generation Center, a Data Owner, a P2P-Based Data Distribution Platform, an IPFS Cluster, Hyperledger Fabric Blockchain, and a Data Consumer. The system performs System Initialization, User Registration, Data Upload, and Data Download. The Smart Contract permits the subjects to issue trusted, traceable, irreversible transactions and does not require supervision from third-party management. A Validation Contract is used to understand subject permissions, which means that subject attributes must meet the AC criteria to have access rights to distributed information. Additionally, a Decryption Contract allows partial decryption for the data being requested.

Shi et al. [32] establish a solution described as Blockchain-based access control Scheme (BacS), designed for two crucial attacks: (1) stealing and modifying data and (2) modifying elements in the authorization database. This solution eliminates a central authorization database but includes computational overhead, showing that some computational expense is necessary for the higher throughput.

Pussewalage et al. [34] present an AC scheme that supports controlled access delegation, ensuring flexible and secure sharing using ABAC. Their focus is on health information sharing to grant flexible access to registered and unregistered users. Blockchains manage attribute assignments, delegations, and revocations, making user authentication a simple and lightweight process. Future work opportunities intend to extend the work with a suitable trust model.

7. Access Control for IoT-Based Environments

The *Internet of Things* (IoT) leverages physical devices with embedded sensors, processing ability, software, and other technologies that provide connection and exchange information with multiple ad-hoc devices and systems through the internet and various communication media, as shown in Figure 16. A summary of surveyed works is included in Table 5.

Alramadhan et al. [37] survey AC applied to IoT environments. The main approaches considered are ACLs, Capability-based Access Control (CapBAC), RBAC, ABAC, and Relationship-based Access Control (ReBAC). These technologies are compared considering their characteristics applied to IoT, where three particular challenges linked to the technology are explained: Constrained Resources, Heterogeneity, and Ubiquitousness. The complexity of IoT induces

Table 4: Surveyed Access Control Solutions for Blockchain

Surveyed AC	AC Type	Technical Characteristics	Research Innovations
TBAC Zhu et al., 2018 [27]	ABAC	With this technique, transactions are used as a bridge integrating ABAC and Blockchain into a novel platform	Supports flexible permission management as well as a verifiable and transparent access authorization process
BSeIn Lin et al., 2018 [28]	ABAC	A technique that works by using Cryptographic materials, including Attribute-based Signatures (ABS) and Multi-receiver Encryption (MRE)	Offers cyber-resilience against the following attacks: User Impersonation attacks, DoS/DDoS attacks, Modification of broadcast transactions or response messages attacks, and MITM attacks
SBAC Lyu et al., 2020 [29]	ABAC	A secure Access Control framework that is Blockchain-based provides the content provider with the ability to share, audit, and revocate privileges	Gives the Content Provider (CP) complete control over their own content - ensuring strong efficiency and security characteristics
FADB Li et al., 2020 [30]	ABAC	This technique combines Blockchain, IPFS distributed storage, and CP-ABE encryption	A novel encryption scheme known as HECP-ABE combines the traditional CP-ABE encryption with Blockchain
BDSS-FA Xu, 2020 [31]	ABAC	A Blockchain-based secure data-sharing platform with fine-grained Access Control (BDSS-FA). Introduces a novel hierarchical attribute-based encryption (HABE) algorithm	Uses a Validation Contract to review the user permissions to ensure only the users whose attributes meet the Access Control criteria have the right to access the shared data
BacS Shi et al., 2021 [32]	ABAC	Using an account address of the node in the Blockchain (the user's wallet) as the identity to access the domain management server, it can redefine the Access Control permission of data and devices, and write to the Blockchain	enable encryption of all Access Control transactions that are issued by the domain management server. Access Control is feasible and secured to implementation in distributed IoT environments
SCBAC Song et al., 2021 [33]	ABAC	IoT Access Control solution based on Blockchain that uses attributes like traditional ABAC approaches	By utilizing public attributes, policies, and permissions on the Blockchain, it creates an open, transparent, secure, and trusted data privacy environment
Blockchain-Based Delegatable AC Scheme Pussewalage et al., 2018 [34]	ABAC	The solution proposes an attribute-based scheme that integrates with the capabilities of controlled access delegation. Blockchains manage attributes, delegations, and revocations	This data privacy solution provides security against attribute forgery, collusion, and pseudo-anonymity

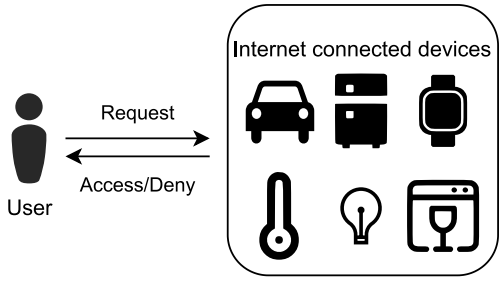


Figure 16: IoT Access Control diagram

specific requirements for AC implementation, including being lightweight and scalable.

Saha et al. [38] developed *Cipher-Policy Attribute-based Encryption* (CP-ABE) for user AC in IoT environments. Their solution supports a fine-grained, user-based AC mechanism with multiple Attribute Authorities (AA), constant key and ciphertext sizes. Secure data is acquired by the gateway nodes from the IoT smart devices, which are stored in partial blocks and converted into complete blocks by the Cloud servers in a P2P network. Their analysis also considers the communication and computational costs, showing the solution's effectiveness.

Gupta et al. [39] propose an AC model known as Google Cloud Platform IoT Access Control (GCP-IoTAC). The experiments focus on the users and resource authorizations, considering real-world scenarios in the healthcare and smart home use cases with RBAC authorizations. For future work, the authors propose using ABAC-based extensions with a role-centric method to improve interoperability and obtain a finer-grained AC.

Mahalle et al. [35] explore an *Identity Authentication and Capability-based Access Control* (IACAC) approach for IoT environments building a distributed, lightweight, and cyber-resilient solution. The researchers performed experiments and performance analysis using the RC5 stream cipher for encryption, considering DoS/DDoS attacks, MITM attacks, and Replay attacks.

Xiong et al. [40] propose a novel AC method known as *Secure and Efficient Multi-authority Access Control for IoT Cloud Storage* (SEM-ACSIT). The system allows for significantly reduced storage overhead in the system. Furthermore, the solution guarantees forward and backward security when taking away a user attribute. The experiments and analysis show that the technique benefits storage effectiveness and efficiency with low computational overhead whilst providing cybersecurity measures for robust data distribution for the Cloud storage environment in IoT applications.

Xu et al. [113] propose a *Blockchain-enabled decentralized Capability-based Access Control* (BlendCAC) procedure to be utilized in IoT environments. The architecture is a partially decentralized and federated framework that can leverage Smart Contracts and Blockchain environments. The experiments involved

the construction of a proof-of-concept prototype deployed in a physical IoT network environment. When evaluating the scheme, they consider two other AC techniques, RBAC and ABAC, that have been transcoded for independent Smart Contracts. It has been found that RBAC and ABAC require a localized datastore to sustain user-role permissions and handle attribute-permission policies for the authorization and validation process to be completed.

Hussein et al. [36] developed an approach called *Secure and Efficient Multi-Authority Access Control* (SEMAAC) for a healthcare use case scenario. They focused on a 'community' AC approach due to the structure of IoT environments rarely being completely isolated. The framework consists of the following elements: Authorization Server, Policy Decision Point (PDP), Certificate Authority (CA), Community Gatekeeper, Policy Enforcement Point (PEP), Community (a group of services that share common goals), and Capability (a data structure containing a set of access rights). Overall, the research presents positive steps for an AC system in which environments showcase an adaptable framework that other researchers can use to improve cybersecurity measures.

Sun et al. [42] designed a technique called *Lightweight Privacy-aware Access Control* (LPAC) for a smart health use case scenario. LPAC provides strong attribute privacy protection, fine-grained and lightweight access policies, offline and online encryption procedures, and efficient decryption methods. They present storage and computational comparison and a security analysis focusing on attack-resistance capability.

8. Access Control for SDN-Based Environments

Software-Defined Networking (SDN) is a network management platform solution that offers a dynamic, programmable, and efficient network configuration. Using an SDN approach can improve network performance and monitoring. Unlike traditional physical infrastructures, it enables a network infrastructure to leverage emulation, virtualization, and programmability rather than fixed physical devices, as shown in Figure 17.

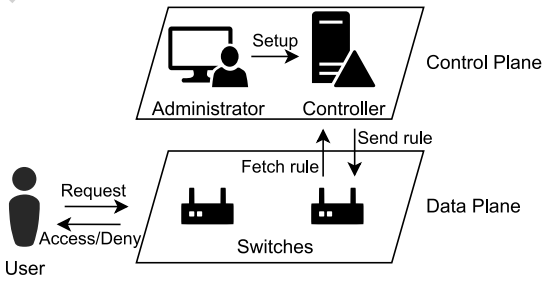


Figure 17: SDN-based Access Control diagram

In Table 6, we detail AC techniques applied to SDN technology with highlighted original approaches. Yakasai and Guy. [43] demonstrate AC being utilized in an SDN environment. RBAC is applied by defining central roles for

Table 5: Surveyed Access Control Solutions for IoT

Surveyed AC	AC Type	Technical Characteristics	Research Innovations
CapBAC Alramadhan and Sha, 2017 [37]	RBAC	It uses a row-oriented list style which associates every subject with one or more pairs of objects or their set permissions	The capabilities list is held by the accessor rather than the resources being accessed (unlike other AC solutions such as ACLs)
CP-ABE Saha et al., 2021 [38]	ABAC	Provides a finer-grained AC solution for IoT environments by supporting multiple Attribute Authorities (AA), constant key and ciphertext sizes simultaneously	Communication and computation are cost-effective. It is a robust AC solution
GCP-IoTAC Gupta et al., 2020 [39]	ABAC	Explores an AC solution for the Google Cloud IoT Platform	Allows secure communication for IoT devices, users, and applications
IACAC Mahalle et al., 2013 [35]	RBAC	A lightweight, distributed, and resilient security solution	Provides defense against common cyber-attacks for example, DoS/DDoS attacks, MITM attacks, and Replay attacks
SEM-ACSIT Xiong et al., 2020 [40]	ABAC	Guarantees forward and backward security when the subject attributes are revoked. Allows users to be supported in the authorization process providing access to the shared data with high flexibility	Significant storage overhead reduction
BlendCAC Xu et al., 2018 [113]	ABAC	A partially decentralized and federated framework	Ability to leverage Smart Contracts and a Blockchain-based IoT environment
SEMAAC Hussein et al., 2017 [36]	RBAC	Building on the concept of community to define the notion of rights	A novel community-driven framework for AC in distributed IoT contexts addressing complex requirements
LPAC Sun et al., 2020 [42]	ABAC	Robust attribute privacy protection, fine-grained and lightweight AC policies, online and offline encryption, and efficient decryption	Efficiently transforms the user attributes and access policy into a more succinct attribute vector and access vector

devices, a Policy Decision Point (PDP) for the central location policy definition, a Policy Enforcement Point (PEP), and a Policy Information Point (PIP) - which operates by combining PEP and PIP into a switch storing the identities of users, such as an LDAP data store. It also uses a novel policy enforcement method using a stateful role-based firewall with a component known as FlowIdentity, which is responsible for the functionality of the firewall.

Paladi and Gehrmann. [47] investigate scalable AC that can be used for the SDN resources by introducing a model restricting resource access using partial system views depending on the topology of resources and visibility of the underlying execution platform. This scheme combines previous AC approaches,

including *Capability Based Access* (CBA), ABAC, and PBAC. They claim that despite having some success, much more research and development must be undertaken to produce a more usable and scalable deployment and configuration mechanism for SDN.

Duy et al. [44] evaluated an AC technique in an SDN environment in conjunction with Blockchain. The model, known as Blockchain-based framework for Decentralized authentication and fine-grained Access Control (B-DAC), implements controller-dependent, application-transparent, strict, and decentralized AC. This ensures that all communications from all applications to the controller are verified before they transit to the network.

Matias et al. [48] illustrate a *Flow-based Network Access Control* (FlowNAC) solution in comparison to the IEEE 802.1X standard Port-based Access Control (PNAC). This study highlights improvements such as controlling individual access to many services simultaneously (instead of being limited to one, as seen in PNAC). The design and development of FlowNAC use SDN principles to allow segregation of the PEP at the data plane from the Attribute Authority process state on a different entity. This separation enables modular and independent scaling of each component as needed.

Mattos and Duarte. [45] propose a novel technique known as AuthFlow to provide AC in SDN environments. It uses OpenFlow as a mechanism to perform authentication and AC for SDN. It authenticates hosts above the MAC Layer using the IEEE 802.1X standard and a Remote Authentication Dial-In User Service (RADIUS) authentication server. The AuthFlow mechanism is implemented as a RADIUS authentication against an LDAP database. They developed and evaluated a prototype showing that the approach can prevent unauthorized hosts from being able to access network resources, notably when hosts are already authenticated. After a pre-defined period, they can lose their privileges, which means that the solution can be time-sensitive. AuthFlow provides enhanced management compared to other AC solutions, introducing more control over information and permitting the definitions of policies for flow AC associated with the host credentials.

Tseng et al. [49] propose controller-independent security that enhances the system's controller DAC capabilities, protecting the SDN controller against API attacks using an efficient and flexible method with dynamic AC. They developed a prototype that complements OpenDaylight and has a low deployment complexity. However, despite significant work in this research area (using permission sets to secure SDN controllers), detecting an API attack with static permission control has not been achieved.

Al-Alaj et al. [46] developed SDN-RBAC as an AC system to secure SDN controller applications. They have identified various approaches where the system can handle app sessions. This helps to apply the principle of least privilege at the application level and to their sessions.

The number of entries in ACLs can continually increase to ensure up-to-date security in an environment with massively diversified attack sources. The TCAM memory used to store them in network switches is particularly expensive, so minimizing the memory footprint with rule compression techniques is one

possible solution [114, 50, 51]. Distributing the access-control policy in smaller rule tables has also been discussed in many previous works [115, 116, 117]. To address some of their drawbacks like rule replication or packet structure modification, Abboud et al. [118, 119] propose an approach to distribute and update those rules with a focus on the Longest Prefix Match (LPM) priority policy. Their strategy applies to series-parallel network graphs, with a reduction process from any two-terminal directed acyclic graph to the series-parallel case.

9. Organizational Adoption

Access Control has a highly successful adoption history in many different businesses as part of their cybersecurity strategies. This section considers industry applications in Healthcare, Education, and Banking.

9.1. Healthcare

Tang et al. [120] demonstrate the Bell-LaPadula model [103] being integrated with Blockchain to provide a viable solution for Identity Management, Supply-chain Management, Insurance Claiming, and other applications where government agencies must ensure scalability and cybersecurity for their systems. Furthermore, this model is completely decentralized, unlike older centralized systems presently in use, and does not require any third parties to have the ability to provide a fair service to their involved peers.

Xu et al. [121] enable Access Control in Cloud provisioned healthcare systems. They define organizational rules as standard practices for subjects, which can adapt depending on the current needs. For example, Least Privilege, Least Separation of duties, Delegation of Tasks, Spatial and Temporal constraints, and Classification of Tasks can be desired. The solution extends *Task-Role Based Access Control* (T-RBAC) [122], including tasks and subject challenges supporting multi-tenant Cloud applications. This supports flexible access rights that can be adapted actively using fine-grained task and subject constraints and a scope level for all subjects.

Tanwar et al. [123] propose a Blockchain-based electronic healthcare record system for the 4.0 industry with increasing connectivity and smart automation. It mainly proposes (1) a Distributed Ledger, (2) a Consensus Mechanism, (3) Provenance, (4) Immutability, (5) Finality, and (6) Smart Contracts. Utilizing the technique for AC demonstrates benefits in information acquisition automation, validation processes, and aggregation of the correct information from multiple sources. It also shows tamper resistance and supports redundancy and fault tolerance in the system.

Chinnasamy and Deepalakshmi [124] deployed a cryptographic AC solution to secure Electronic Health Record (EHR) retrieval for healthcare in the Cloud. It uses hybrid cryptography to protect storage by combining the Key Generation Scheme of RSA (IKGSR) and Blowfish algorithms. Also, steganography is used to deal with issues of distributing keys and healthcare information. The security analysis shows resilience to multiple threats, including ciphertext attacks, plaintext attacks, and keyword guessing attacks.

Table 6: Surveyed Access Control Solutions for SDN

Surveyed AC	AC Type	Technical Characteristics	Research Innovations
Flow Identity Yakasai and Guy, 2015 [43]	RBAC	Works by using high-level rules based on role information (obtained from the authentication server) and SDN principles being pushed dynamically and instantaneously enforced at network endpoints. solving some traditional challenges of port-based AC	By using a novel Policy Enforcement Point (PEP), a stateful role-based firewall provides the network operators with a practical and improved enterprise security solution. It addresses the challenges that network vendors face with 802.1X
Paladi and Gehrmann, 2019 [47]	ABAC	Introduces a Taxonomy of resource access models for SDN infrastructure with a Network Access Control API	Allows the Network Access Control API to commit at deployment to the many resource access requirements enforced by secret components on the Network Controller platform
B-DAC Duy et al., 2021 [44]	RBAC	Decentralized Access Control Framework with prototype implementation using the Hyper-ledger Fabric Blockchain approach to secure the SDN controller. The aim is to provide security for the interactions between SDN controllers and network applications	The solution makes it futile for hackers to create a false entity for launching attacks on the SDN floodlight controller application channel
FlowNAC Matias et al., 2014 [48]	ABAC	Grants access rights to users to the network depending on the target service requested	The capability to individually control the access to several services at the same time (instead of just one) and provide the separation of the PEP at the data plane from the Attribute Authority process state on a separate entity
AuthFlow: Mattos and Duarte, 2016 [45]	RBAC	Used as a mechanism for authentication	Used in combination with OpenFlow Software-Defined Networking to provide Access Control to the infrastructure
Controller DAC Tseng et al., 2017 [49]	ABAC	A Proposed System that utilizes Controller-Independent Security	System Controller Dynamic Access Control (DAC) proposes to defend the SDN Controller against API attacks and cyber-attacks using a flexible method working with OpenDayLight with minimal deployment complexity
SDN-RBAC Al-Alaj et al., 2019 [46]	RBAC	Deploying Role-Based Access Control into an SDN environment	Demonstrating RBAC usability through an SDN Controller

Figueroa et al. [125] explore using and combining an ABAC system with an RFID system to produce a robust AC solution for healthcare. The system prevents unwanted assets from entering a location due to human error or out-

side attacks. Unlike traditional AC systems that rely on centralized techniques such as RBAC models, the proposed system relies on a decentralized model using policies from a decentralized application centered on a Blockchain system. The AC mechanisms for the system are derived from multiple elements: (1) Check the attributes of subjects, (2) Check the AC policies, (3) Evaluate object attributes, (4) Check the conditions of the environment.

Egala et al. [126] propose an AC framework using Blockchain to enhance cybersecurity in the Internet of Medical Things (IoMT). They propose an approach that addresses the challenges of data security, privacy, anonymity, latency, and traceability using decentralized IoMT-based healthcare systems. The techniques include *Selective Ring-based Access Control* (SRAC) algorithm and cryptography to assure medical data privacy. This works by using ring rules to control data access rights for real-world scenarios. Threat modeling and Logical analysis for a fortified chain ensure security, privacy, immutability, availability, trace anonymity, user control, and scalability.

9.2. Education

Alshahrani [127] discusses AC in education, particularly focusing on using trust-based algorithms for student assessment with E-learning platforms. A trust-based Blockchain system utilizes Smart Contracts to perform evaluations and courses whilst also collecting feedback on the advantages of the presented algorithm in comparison to the previous methodologies, namely enhanced cybersecurity in this area achieved by a highly secured data transmission with lower execution time and energy consumption than traditional methods, demonstrating the viability of Blockchain in this use case.

Li et al. [128] propose a platform for Access Control in mobile distance learning. There are five layers in the system architecture: (1) Client-side, (2) Presentation layer, (3) Business logic layer, (4) Persistence layer, and (5) Data layer. They utilize resource distribution in three stages - Resource Production, Resource Registration, and Resource Audit. The system uses a six-step methodology approach for Resource Management, which leverages traditional storage methods.

9.3. Banking

Joseph et al. [129] propose a Blockchain-based Decentralized Transaction Settlement System for AC to be deployed in the Banking industry. They identify traditional centralized architectures in the Banking sector as a factor limiting digital innovations. The proposed solution uses a decentralized banking solution by using Blockchain on the current banking infrastructure, mainly by changing how loans are given and issuing credit and debit transactions. Using Blockchain can achieve low cost and high security in the way payment transactions are made whilst making the verification of third parties redundant, thus reducing the processing times for traditional bank transfers. In addition, the proposed system can reduce the risk of data loss or modification when information is stored on a central server.

Zaidi et al. [130] use ABAC for IoT with Blockchain and Smart Contracts. This authentication solution enables local access, authorization of consumers, privacy, and interoperability, utilizing Blockchain for authentication, smart contracts for data access processing, and user-controlled encoded policies. This AC solution can be used in banking due to its fine-grained AC level. The researchers suggest that using ABAC for their use case achieves high compatibility and policy expressiveness.

Auxilia and Raja [131] present an AC solution for banking using Cloud environments using a Knowledge Based Security Model (KBSM). This solution captures the relationship between all AC elements (subject, object, and action). The system model consists of an ontology base, a policy base, an interface engine, and a policy engine. The initial element holds the subject's details (e.g., user credentials), object details (e.g., account and letter of credit), and action details (actions being performed on a bank resource). They aim to address the main cybersecurity challenges related to the transition of banking services to the Cloud environment: security breaches, governance, and Service Level Agreements (SLA).

Guo et al. [132] present a case study of a Multi-Authority ABAC model applied to the banking industry. The system uses an attribute-based access policy and Smart Contracts to provide a multi-authority AC solution. The system handles interactions between data users, data owners, and multiple authorities encoded into Ethereum Smart Contracts. They demonstrate a proof of concept for their solution implemented in Solidity and tested with the Rinkeby Ethereum testnet. The security analysis performed on the system used the Ethereum Blockchain to implement communications between participants, showing how to save data records and transaction information, thus giving users the ability to trace back specific information with the help of Blockchain technology.

Yu et al. [133] explore a *Blockchain-based Bell-LaPadula Model* (BC-BLPM) applied to the Banking industry. The solution includes three main layers: a Resource Layer, an AC Layer, and a Transaction-Forwarding layer. The Resource Layer consists of an array of computing resources (files, databases, etc.) stored in a computer or mobile device and is accessed through encrypted data transmission channels. In the AC Layer, nodes that perform data processing hold responsibility for developing Blockchain-based access domains. Such domains could maintain diverse data resources, abstracting from various company departments.

To maintain a thorough level of AC, the model implements attributes including audibility and scalability, using a multi-Blockchain architecture that can divide the network into multiple domains making the resource objects of different departments logically isolated, which improves resource maintenance efficiency and contributes to zero-trust networking practices.

9.4. Experiences of Organizational Deployment

Mohammed [134] considers the adoption of AC solutions in Cloud environments, identifying advantages such as better cost management and delivery

times as well as data sharing. In addition, adopting AC with Cloud infrastructure has been shown to help develop cybersecurity strategies contributing to data availability, accountability, and scalability, offering optimization, and more efficient processing. Moreover, AC can help businesses with digital transformations and overcome various challenges, including handling the inclusion of new workers, managing distinct identities' life cycles, and supervising a time-consuming off-boarding process without exposing the organization to significant cybersecurity threats.

Kawada et al. [135] highlight the three critical requirements needed for AC:

- *Expressiveness* - Data Access Control requires enough expressiveness to enable Access Control needed from potential applications.
- *Management simplicity* - Access authorization data management and maintenance must be simple.
- *Performance* - Data Access Control cannot force considerable performance degradation for processing data.

The access authorization data is highlighted using tabular formats, easing access policies' management. It also demonstrates that SQL queries allow for modeling access authorization data and access policies for potential applications, allowing administrators to utilize a typical Relational Database Management System (RDBMS) to retrieve information through access policies.

Fabian et al. [136] consider AC for semantic data federations for industrial product-lifestyle management. They showed that enforcing RBAC policies is extremely useful in systems where cooperating business partners need to share controlled semantic data. They introduced a novel security service, SemForce, as an AC infrastructure for semantic repositories, including XACML-compliant semantic PDPs and PEPs. The results show acceptable overhead when querying semantic data with SemForce and fast response times when there are multiple look-ups for matching roles to resources in industrial product-lifestyle management.

Chen et al. [137] developed an AC model and system architecture for resource sharing in organizations. They successfully proposed two AC models: RBAC and Project-Based Access Control. Furthermore, they provide user authority, certificate authentication, and AC which identifies subjects' identities online, updates and searches user authority lists, and accesses public and private resources. However, the research observed some issues, notably omitting access policies' integration in the non-RBAC system.

Daoudagh et al. [138] present an enterprise authorization policy life cycle based on ABAC. The life cycle has eight main objectives:

1. GDPR-based use case definition, a common base that can be discussed with stakeholders to determine a strategy for compliance.
2. Gather Authorization Requirements, defined as terms of statements and natural language authorization policies, including business requirements and cybersecurity best practices.

3. Identify Required Attributes in selection requirements as well as their origin, which can help with requirement reviews.
4. Author Authorization Policies, transforming natural language statements into machine-interpretable statements.
5. Validate the AC Policies and Mechanisms through testing, ensuring that the XACML policies meet the GDPR requirements.
6. Deploy the Architecture and define the contact point within the existing systems where different applications interact with the authorization system.
7. Deploy the XACML Policies according to the selected environment, which is usually specific to the nature of the business.
8. Run Access Reviews - test the policies linked to attributes for determining which attributes will be granted. To provide GDPR compliance, this should involve the simulation of realistic scenarios.

Silva et al. [139] discuss a framework known as ACROSS for AC for organizational adoption using ABAC. The framework is designed as an AC solution focusing on authentication and authorization for organizations, supporting identity and resource management concepts. There are many characteristics of ACROSS, including:

- Supporting multiple authentication techniques.
- Independence from the resource federation technique.
- Support for various attribute providers for an array of situations providing respect for user privacy using a unique opaque identity attribute.
- Advanced user-level classification with gender attributes and ABAC elements.
- Support for linking the user's electronic identities with attributes stored on various identity management systems.

Based on users' attributes (ABAC), ACROSS provides access levels adopting a user classification algorithm that can adapt to all organizations, providing a robust AC solution.

Duy et al. [140] explore a framework that can be used for organizational adoption known as B-DAC, which focuses on decentralized AC for the Northbound interface that secures SDN with Blockchain technology. The proposed framework secures interactions between SDN controllers and network applications, leveraging fundamental features in Blockchain. The technology achieves controller independence, application transparency, and strict decentralized AC, ensuring all communications from all applications to the controller are examined before transiting on the network, contributing to an overall zero-trust architecture.

Deepa et al. [141] provide a review of the future opportunities, approaches, and directions on Blockchain for big data and AC. For example, AC is achieving

data privacy and security in smart cities through Blockchain. Another opportunity is privacy preservation in Intelligent Transport Systems (ITS) for in-car navigation systems in smart cities. In addition, the paper discusses the significance of data mining by larger companies to help them provide meaningful customer service, optimize decision processes, and aid in forecasting future developments, making the data a precious asset.

Chen and Tsung [142] formulate a *Knowledge Based Access Control* (KBAC) model for sharing knowledge in virtual enterprises. The proposed model uses knowledge from workers in multiple organizations in an ontological knowledge description layer, solving-knowledge heterogeneity problems. It works by following three knowledge-sharing modes: role-based, task-based, and concept-based knowledge-sharing. In addition, the KBAC model uses functions that provide (1) Flexibility, (2) Secure inter-organizational services, (3) Centralized authorization management, and (4) Incorporation of knowledge dynamics.

10. Integration Approaches

This section discusses the opportunities of integrating Access Control with various other techniques that extend its reach and capabilities.

10.1. Assisted Predictions for Access Control

Researchers have proposed various assisted prediction models for AC that incorporate machine learning and data analytics techniques. These models aim to improve the efficiency and effectiveness of AC systems by predicting users' access requests, trust levels, and behavioral patterns, thereby reducing the workload of AC administrators. In this context, several recent studies have proposed innovative AC models that employ algorithms such as fuzzy logic, regression analysis, peer-to-peer federated learning, and Blockchain technology.

Jiang et al. [143] propose a greedy Access Control (AC) model for the healthcare domain that utilizes fuzzy trust prediction and regression analysis through two algorithms. They employ a trust model known as Fuzzy Trust-based Proactive Access Control Model (FTPACM), which comprises three AC modules: Identity Authentication (IA), which verifies user identity and handles user requests and new user registrations; Behavior Warning (BW), which analyzes user behavior and provides feedback on behavior characteristics to classify the user's trust level; and Access Policy Database (AP-DB), which utilizes user identification and trust level to determine the access view based on the access policy.

Lian et al. [144] propose a peer-to-peer federated learning model called P2PK-SMOTE that employs two algorithms and Blockchain technology to improve data privacy through decentralized data in the healthcare domain. The first algorithm focuses on the overall workflow and a data-sharing scheme, while the second algorithm focuses on client selection. When applied to three datasets, the authors observed successful results with minimal data sharing.

You et al. [145] propose a knowledge graph model for decision-making in AC. The construction algorithm builds an AC graph based on user and resource

attributes. The model was shown to be effective in improving AC in all scenarios by enhancing topological features. However, due to limitations in the dataset for company data security, one of the study's challenges was demonstrating high predictive performance without a richer dataset.

10.2. Integrating Formal Methods with Access Control

To reliably ensure that a given Access Control policy reflects its intended specification, automated verification through formal methods provides strong correctness guarantees. A core component of this effort is the formalization itself. User or data attributes must be clearly modeled to enforce a policy, usually encoded within an XML-based Access Control language, compliant with the XACML standard [146]. This enables different systems to apply a given policy using the same Access Control language. Combining different sub-policies requires a suitable merging process. As such, Lobo et al. [147] introduced the **PCL** language specifically tailored for specifying policy combining algorithms in an XACML framework.

Bertino et al. [148] presented a first step in the formalization of Access Control policies with a logical framework general enough to capture DAC, MAC, and RBAC models. It can represent objects, subjects, and privileges, possibly organized into hierarchies, sessions, and positive and negative authorizations. Those authorizations do not have to be always explicitly stated, as it supports the specification of inferred authorizations. When some rules contradict each other, it supports arbitrary conflict resolution mechanisms.

One essential property to verify about a policy is the absence of conflicts and gaps within its rules. Expressing conflicts as propositional constraints is demonstrated in [149], where SAT solvers are used to check if one such proposition is satisfiable. Further analysis to detect undefined behaviors is carried out in [150], where the composition of various sub-policies is considered. Using *unspecified* values for patterns not covered by a given sub-policy, they can detect if there are still undefined entries in the union of all sub-policies.

Other works target specific domains of Access Control. For example, Jha et al. [151] developed tools for the security analysis of RBAC policies using model-checking tools and logic programming, experimentally evaluating the two approaches. They also proved that this problem in the general case is **PSPACE**-complete. Access Control determines who can execute a given action in the smart contract space, and an application to the *Azure Blockchain Workbench* is demonstrated in [152]. On the SDN side, misconfigurations of firewalls can arise when maintaining the policy. Saâdaoui et al. [153] implemented a set of inference rules to automatically and optimally detect such anomalies with Flow-tables in OpenFlow-based networks.

11. Future Directions for Access Control Research

Throughout this section, we explore some potential research directions in the fields of Access Control, Data Privacy, and Information Security.

Colombo and Ferrari [154] suggest that AC in the context of Big Data and NoSQL databases is an area with much potential for exploration, particularly in terms of fine-grained AC within NoSQL management systems. They also note the need for unifying AC models and techniques to be used for enforcement purposes, as well as the development of Policy Analysis tools within federated environments.

Sarker et al. [155] investigate the use of Artificial Intelligence (AI) as a driver for cybersecurity innovation and suggest that AI could enhance cybersecurity defense mechanisms, including Access Control. They suggest that AI can perform intelligent decision-making, which could improve security measures such as Firewall, Anti-Malware, Sandbox, and Security Information and Event Management (SIEM).

Daoudagh and Marchetti [156] propose multiple research questions focused on Access Control, particularly in the context of the Attribute-Based Access Control (ABAC) model and its compatibility with the General Data Protection Regulation (GDPR). They ask whether systems can comply with the GDPR act fully, and to what extent GDPR's obligations can be represented and enforced using AC techniques. These questions open up the possibility for further research to be conducted, exploring the capabilities of different mainstream AC models in meeting GDPR requirements and ensuring the appropriate level of data privacy within an organization.

12. Conclusion

Throughout this survey, we reviewed the current state-of-the-art Access Control solutions used by organizations as a cybersecurity strategy for user and data authorization. As a specific contribution, we reviewed new solutions, exploring various modern application domains such as cloud computing, the Internet of Things (IoT), Blockchain, and Software-Defined Networking (SDN), evaluating their strengths and limitations. Moreover, we considered their organizational adoption through case studies in different sectors where these access control techniques have been deployed. Finally, we discussed future research directions to understand present challenges and address existing limitations.

13. Acknowledgement

This paper contributes to part of Lewis Golightly's PhD thesis.

References

[1] S. Dramé-Maigné, M. Laurent, L. Castillo, H. Ganem, Centralized, distributed, and everything in between: Reviewing access control solutions for the iot, ACM Comput. Surv. 54 (7). doi:10.1145/3465170.

[2] National Institute of Standards and Technology, Access control glossary. URL https://csrc.nist.gov/glossary/term/access_control

[3] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, B. Fang, A survey on access control in the age of internet of things, IEEE Internet of Things Journal 7 (6) (2020) 4682–4696.

[4] W. Stallings, L. Brown, Computer security: principles and practice, Forth Edition, Pearson Education Limited, 2018.

[5] T. Cerny, A. Walker, J. Svacina, V. Bushong, D. Das, K. Frajtak, M. Bures, P. Tisnovsky, Mapping study on constraint consistency checking in distributed enterprise systems, in: Proceedings of the International Conference on Research in Adaptive and Convergent Systems, 2020, pp. 167–174.

[6] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, Access control for emerging distributed systems, Computer 51 (10) (2018) 100–103.

[7] E. Bertino, A. A. Jabal, S. Calo, D. Verma, C. Williams, The challenge of access control policies quality, Journal of Data and Information Quality (JDIQ) 10 (2) (2018) 1–6.

[8] D. Servos, S. L. Osborn, Current research and open problems in attribute-based access control, ACM Computing Surveys (CSUR) 49 (4) (2017) 1–45.

[9] N. Kashmar, M. Adda, H. Ibrahim, Access control metamodels: Review, critical analysis, and research issues, J. Ubiquitous Syst. Pervasive Netw 3.

[10] N. Kashmar, M. Adda, M. Atieh, H. Ibrahim, A review of access control metamodels, Procedia Computer Science 184 (2021) 445–452.

[11] P. Zhang, J. K. Liu, F. R. Yu, M. Sookhak, M. H. Au, X. Luo, A survey on access control in fog computing, IEEE Communications Magazine 56 (2) (2018) 144–149.

[12] F. Paci, A. Squicciarini, N. Zannone, Survey on access control for community-centered collaborative systems, ACM Computing Surveys (CSUR) 51 (1) (2018) 1–38.

[13] S. Parkinson, S. Khan, A survey on empirical security analysis of access control systems: A real-world perspective, ACM Computing Surveys (CSUR).

[14] C. Langaliya, R. Aluvalu, Enhancing cloud security through access control models: A survey, International Journal of Computer Applications 112 (7).

[15] A. Ometov, O. L. Molua, M. Komarov, J. Nurmi, A survey of security in cloud, edge, and fog computing, Sensors 22 (3) (2022) 927.

[16] S. Ravidas, A. Lekidis, F. Paci, N. Zannone, Access control in internet-of-things: A survey, Journal of Network and Computer Applications 144 (2019) 79–101.

[17] 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, Journal of Network and Computer Applications 178 (2021) 102950.

[18] J. C. C. Chica, J. C. Imbachi, J. F. B. Vega, Security in sdn: A comprehensive survey, Journal of Network and Computer Applications 159 (2020) 102595.

[19] S. T. Alshammari, A. Albeshri, K. Alsubhi, Integrating a high-reliability multicriteria trust evaluation model with task role-based access control for cloud services, Symmetry 13 (3) (2021) 492.

[20] C. Anilkumar, S. Subramanian, A novel predicate based access control scheme for cloud environment using open stack swift storage, Peer-to-Peer Networking and Applications 14 (4) (2021) 2372–2384.

[21] W. Li, H. Wan, X. Ren, S. Li, A refined rbac model for cloud computing, in: 2012 IEEE/ACIS 11th International Conference on Computer and Information Science, IEEE, 2012, pp. 43–48.

[22] C. Choi, J. Choi, P. Kim, Ontology-based access control model for security policy reasoning in cloud computing, The Journal of Supercomputing 67 (3) (2014) 711–722.

[23] S. Fugkeaw, H. Sato, Privacy-preserving access control model for big data cloud, in: 2015 International Computer Science and Engineering Conference (ICSEC), 2015, pp. 1–6. doi:10.1109/ICSEC.2015.7401416.

[24] Y. Xue, J. Hong, W. Li, K. Xue, P. Hong, Labac: A location-aware attribute-based access control scheme for cloud storage, in: 2016 IEEE Global Communications Conference (GLOBECOM), 2016, pp. 1–6. doi:10.1109/GLOCOM.2016.7841945.

[25] M. Gupta, F. M. Awaysheh, J. Benson, M. Alazab, F. Patwa, R. Sandhu, An attribute-based access control for cloud enabled industrial smart vehicles, IEEE Transactions on Industrial Informatics 17 (6) (2020) 4288–4297.

[26] M. Ennahbaoui, H. Idrissi, A new agent-based framework combining authentication, access control and user behavior analysis for secure and flexible cloud-based healthcare environment, Concurrency and Computation: Practice and Experience (2021) e6712.

[27] 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), IEEE, 2018, pp. 193–200.

[28] C. Lin, D. He, X. Huang, K.-K. R. Choo, A. V. Vasilakos, Bsein: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0, Journal of Network and Computer Applications 116 (2018) 42–52.

[29] Q. Lyu, Y. Qi, X. Zhang, H. Liu, Q. Wang, N. Zheng, Sbac: A secure blockchain-based access control framework for information-centric networking, Journal of Network and Computer Applications 149 (2020) 102444.

[30] H. Li, L. Pei, D. Liao, S. Chen, M. Zhang, D. Xu, Fadb: A fine-grained access control scheme for vanet data based on blockchain, IEEE Access 8 (2020) 85190–85203. doi:10.1109/ACCESS.2020.2992203.

[31] H. Xu, Q. He, X. Li, B. Jiang, K. Qin, Bdss-fa: A blockchain-based data security sharing platform with fine-grained access control, IEEE Access 8 (2020) 87552–87561. doi:10.1109/ACCESS.2020.2992649.

[32] N. Shi, L. Tan, C. Yang, C. He, J. Xu, Y. Lu, H. Xu, Bacs: A blockchain-based access control scheme in distributed internet of things, Peer-to-peer networking and applications 14 (5) (2021) 2585–2599.

[33] L. Song, Z. Zhu, M. Li, L. Ma, X. Ju, A novel access control for internet of things based on blockchain smart contract, in: 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Vol. 5, 2021, pp. 111–117. doi:10.1109/IAEAC50856.2021.9390662.

[34] H. S. Gardiyawasam Pussewalage, V. A. Oleshchuk, Blockchain based delegatable access control scheme for a collaborative e-health environment, in: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1204–1211. doi:10.1109/Cybermatics_2018.2018.00214.

[35] P. N. Mahalle, B. Anggorojati, N. R. Prasad, R. Prasad, Identity authentication and capability based access control (iacac) for the internet of things, Journal of Cyber Security and Mobility 1 (4) (2013) 309–348.

[36] D. Hussein, E. Bertin, V. Frey, A community-driven access control approach in distributed iot environments, IEEE Communications Magazine 55 (3) (2017) 146–153.

[37] M. Alramadhan, K. Sha, An overview of access control mechanisms for internet of things, in: 2017 26th International Conference on Computer Communication and Networks (ICCCN), 2017, pp. 1–6. doi:10.1109/ICCCN.2017.8038503.

[38] S. Saha, D. Chattaraj, B. Bera, A. Kumar Das, Consortium blockchain-enabled access control mechanism in edge computing based generic internet of things environment, Transactions on Emerging Telecommunications Technologies 32 (6) (2021) e3995.

[39] D. Gupta, S. Bhatt, M. Gupta, O. Kayode, A. S. Tosun, Access control model for google cloud iot, in: 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), 2020, pp. 198–208. doi:10.1109/BigDataSecurity-HPSC-IDS49724.2020.00044.

[40] S. Xiong, Q. Ni, L. Wang, Q. Wang, Sem-acsit: Secure and efficient multiauthority access control for iot cloud storage, IEEE Internet of Things Journal 7 (4) (2020) 2914–2927. doi:10.1109/JIOT.2020.2963899.

[41] O. J. A. Pinno, A. R. A. Grégio, L. C. De Bona, Controlchain: A new stage on the iot access control authorization, Concurrency and Computation: Practice and Experience 32 (12) (2020) e5238.

[42] J. Sun, H. Xiong, X. Liu, Y. Zhang, X. Nie, R. H. Deng, Lightweight and privacy-aware fine-grained access control for iot-oriented smart health, IEEE Internet of Things Journal 7 (7) (2020) 6566–6575. doi:10.1109/JIOT.2020.2974257.

[43] S. T. Yakasai, C. G. Guy, Flowidentity: Software-defined network access control, in: 2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN), 2015, pp. 115–120. doi:10.1109/NFV-SDN.2015.7387415.

[44] P. T. Duy, H. D. Hoang, D. T. T. Hien, A. G.-T. Nguyen, V.-H. Pham, B-dac: A decentralized access control framework on northbound interface for securing sdn using blockchain, arXiv preprint arXiv:2111.00707.

[45] D. M. F. Mattos, O. C. M. B. Duarte, Authflow: authentication and access control mechanism for software defined networking, annals of telecommunications 71 (11) (2016) 607–615.

[46] A. Al-Alaj, R. Krishnan, R. Sandhu, Sdn-rbac: An access control model for sdn controller applications, in: 2019 4th International Conference on Computing, Communications and Security (ICCCS), 2019, pp. 1–8. doi:10.1109/CCCS.2019.8888031.

[47] N. Paladi, C. Gehrmann, Sdn access control for the masses, Computers & Security 80 (2019) 155–172. doi:https://doi.org/10.1016/j.cose.2018.10.003.

[48] J. Matias, J. Garay, A. Mendiola, N. Toledo, E. Jacob, Flownac: Flow-based network access control, in: 2014 Third European Workshop on Software Defined Networks, 2014, pp. 79–84. doi:10.1109/EWSDN.2014.39.

[49] Y. Tseng, M. Pattaranantakul, R. He, Z. Zhang, F. Nat-Abdesselam, Controller dac: Securing sdn controller with dynamic access control, in: 2017 IEEE International Conference on Communications (ICC), 2017, pp. 1–6. doi:10.1109/ICC.2017.7997249.

[50] Y. Sun, M. S. Kim, Tree-based minimization of TCAM entries for packet classification, in: 7th IEEE Consumer Communications and Networking Conference, CCNC 2010, Las Vegas, NV, USA, January 9-12, 2010, IEEE, 2010, pp. 1–5. doi:10.1109/CCNC.2010.5421589.

[51] A. Bremler-Barr, D. Hendler, Space-efficient tcam-based classification using gray coding, IEEE Trans. Computers 61 (1) (2012) 18–30. doi:10.1109/TC.2010.267.

[52] W. Mahoney, J. Harr, A linux implementation of windows acls, IJCSNS 10 (7) (2010) 1.

[53] M. Pattan, A. Arora, M. Jain, Generating a software defined segmentation policy from static/dynamic access control lists and active directory integration.

[54] K. Wakabayashi, D. Kotani, Y. Okabe, Traffic-aware access control list reconstruction, in: 2020 International Conference on Information Networking (ICOIN), 2020, pp. 616–621. doi:10.1109/ICOIN48656.2020.9016512.

[55] Y.-T. Huang, D.-L. Chiang, T.-S. Chen, S.-D. Wang, F.-P. Lai, Y.-D. Lin, Lagrange interpolation-driven access control mechanism: Towards secure and privacy-preserving fusion of personal health records, Knowledge-Based Systems 236 (2022) 107679.

[56] G. Sampemane, P. Naldurg, R. H. Campbell, Access control for active spaces, in: 18th Annual Computer Security Applications Conference, 2002. Proceedings., IEEE, 2002, pp. 343–352.

[57] P. Stckle, B. Grobauer, A. Pretschner, Automated implementation of windows-related security-configuration guides, in: 2020 35th IEEE/ACM International Conference on Automated Software Engineering (ASE), 2020, pp. 598–610.

[58] G. Kaur, A. Kaur, Review on the models of access control for cloud computing, FP-International Journal of Computer Science Research (IJCSR) 2 (1) (2015) 32–36.

[59] R. El Sibai, N. Gemayel, J. Bou Abdo, J. Demerjian, A survey on access control mechanisms for cloud computing, Transactions on Emerging Telecommunications Technologies 31 (2) (2020) e3720.

[60] M. U. Aftab, Z. Qin, K. Hussain, Z. Jamali, N. T. Son, N. Van Nam, T. Van Dinh, Negative authorization by implementing negative attributes in attribute-based access control model for internet of medical things, in: 2019 15th International Conference on Semantics, Knowledge and Grids (SKG), IEEE, 2019, pp. 167–174.

[61] Y. Zou, J. Deng, C. Xu, X. Liang, X. Chen, Semantic rule based rbac extension model for flexible resource allocation, in: 2019 12th International Symposium on Computational Intelligence and Design (ISCID), Vol. 2, 2019, pp. 221–224. doi:10.1109/ISCID.2019.10134.

[62] R. Kumar, R. Tripathi, Scalable and secure access control policy for healthcare system using blockchain and enhanced bell–lapadula model, Journal of Ambient Intelligence and Humanized Computing 12 (2) (2021) 2321–2338.

[63] K. Vijayalakshmi, V. Jayalakshmi, A similarity value measure of abac security rules, in: 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI), IEEE, 2021, pp. 565–571.

[64] 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.

[65] C. Blundo, S. Cimato, L. Siniscalchi, Managing constraints in role based access control, IEEE Access 8 (2020) 140497–140511.

[66] Y. Lee, K. M. Lee, Blockchain-based rbac for user authentication with anonymity, in: Proceedings of the Conference on Research in Adaptive and Convergent Systems, 2019, pp. 289–294.

[67] W. Sun, X. Yuan, H. Su, Role-engineering optimization with user-oriented cardinality constraints in role-based access control, International Journal of Network Security 23 (5) (2021) 845–855.

[68] J. T. Johnson, Recommendations for distributed energy resource access control., Tech. rep., Sandia National Lab.(SNL-NM), Albuquerque, NM (United States) (2021).

[69] E. Bertino, P. A. Bonatti, E. Ferrari, Trbac: A temporal role-based access control model, in: Proceedings of the fifth ACM workshop on Role-based access control, 2000, pp. 21–30.

[70] M.-A. Laverdière, K. Julien, E. Merlo, Rbac protection-impacting changes identification: A case study of the security evolution of two php applications, Information and Software Technology 139 (2021) 106630.

[71] J. Xu, Y. Yu, Q. Meng, Q. Wu, F. Zhou, Role-based access control model for cloud storage using identity-based cryptosystem, Mobile Networks and Applications 26 (4) (2021) 1475–1492.

[72] S. Pal, M. Hitchens, V. Varadharajan, T. Rabehaja, Policy-based access control for constrained healthcare resources, in: 2018 IEEE 19th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM), IEEE, 2018, pp. 588–599.

[73] Y. Zong, Y. Guo, X. Chen, Policy-based access control for robotic applications, in: 2019 IEEE International Conference on Service-Oriented System Engineering (SOSE), IEEE, 2019, pp. 368–3685.

[74] R. Mahajan, M. Mahajan, D. Singh, A novel access control model in cloud computing environment (par-ac), International Journal of Engineering & Technology 7 (3) (2018) 1795–1800.

[75] H. Shen, P. Dewan, Access control for collaborative environments, in: Proceedings of the 1992 ACM conference on Computer-supported cooperative work, 1992, pp. 51–58.

[76] I. M. Al Abdulmohsin, Techniques and algorithms for access control list optimization, Computers & electrical engineering 35 (4) (2009) 556–566.

[77] D. D. Downs, J. R. Rub, K. C. Kung, C. S. Jordan, Issues in discretionary access control, in: 1985 IEEE Symposium on Security and Privacy, IEEE, 1985, pp. 208–208.

[78] B. W. Lampson, Dynamic protection structures, in: Proceedings of the November 18-20, 1969, fall joint computer conference, 1969, pp. 27–38.

[79] B. W. Lampson, Protection, ACM SIGOPS Operating Systems Review 8 (1) (1974) 18–24.

[80] G. S. Graham, P. J. Denning, Protection: principles and practice, in: Proceedings of the May 16-18, 1972, spring joint computer conference, 1971, pp. 417–429.

[81] P. J. Denning, Third generation computer systems, ACM Computing Surveys (CSUR) 3 (4) (1971) 175–216.

[82] M. A. Harrison, W. L. Ruzzo, J. D. Ullman, Protection in operating systems, Communications of the ACM 19 (8) (1976) 461–471.

[83] Q.-h. Bai, Y. Zheng, Study on the access control model, in: Proceedings of 2011 Cross Strait Quad-Regional Radio Science and Wireless Technology Conference, Vol. 1, IEEE, 2011, pp. 830–834.

[84] E. Bertino, C. Bettini, E. Ferrari, P. Samarati, A temporal access control mechanism for database systems, IEEE Transactions on knowledge and data engineering 8 (1) (1996) 67–80.

[85] R. Zhang, G. Liu, H. Kang, Q. Wang, Y. Tian, C. Wang, Improved bell–lapadula model with break the glass mechanism, IEEE Transactions on Reliability 70 (3) (2021) 1232–1241.

[86] V. C. Hu, D. Ferraiolo, D. R. Kuhn, et al., Assessment of access control systems, US Department of Commerce, National Institute of Standards and Technology, 2006.

[87] Z. Lei, Z. Hongli, Y. Lihua, S. Xiajiong, A mandatory access control model based on concept lattice, in: 2011 International Conference on Network Computing and Information Security, Vol. 1, IEEE, 2011, pp. 8–12.

[88] G. D. Wurster, Security mechanisms and policy for mandatory access control in computer systems, Ph.D. thesis, Carleton University (2010).

[89] A. S. Coronado, Computer security: Principles and practice (2013).

[90] A. Yadav, R. Shah, Review on database access control mechanisms and models, International Journal of Computer Applications 120 (18).

[91] Y. Liu, Trust-based access control for collaborative system, in: 2008 ISECS International Colloquium on Computing, Communication, Control, and Management, Vol. 1, IEEE, 2008, pp. 444–448.

[92] Z. Xu, S. D. Stoller, Mining attribute-based access control policies from logs, in: Data and Applications Security and Privacy XXVIII: 28th Annual IFIP WG 11.3 Working Conference, DBSec 2014, Vienna, Austria, July 14-16, 2014. Proceedings 28, Springer, 2014, pp. 276–291.

[93] L. Karimi, M. Aldairi, J. Joshi, M. Abdelhakim, An automatic attribute-based access control policy extraction from access logs, IEEE Transactions on Dependable and Secure Computing 19 (4) (2021) 2304–2317.

[94] A. Stambouli, L. Logrippo, Data flow analysis from capability lists, with application to rbac, Information Processing Letters 141 (2019) 30–40.

[95] R. Sandhu, V. Bhamidipati, Q. Munawer, The arbac97 model for role-based administration of roles, ACM Transactions on Information and System Security (TISSEC) 2 (1) (1999) 105–135.

[96] Z. Chen, H. Shao, Y. Li, H. Lu, J. Jin, Policy-based access control system for delta lake, in: 2022 Tenth International Conference on Advanced Cloud and Big Data (CBD), IEEE, 2022, pp. 60–65.

[97] V. Grout, J. McGinn, Optimisation of policy-based internet routing using access control lists, in: Proceedings of the 9th IFIP/IEEE Symposium on Integrated Network Management, 2005.

[98] R. S. Sandhu, P. Samarati, Access control: principle and practice, IEEE communications magazine 32 (9) (1994) 40–48.

[99] A. O'Connor, R. Loomis, Economic analysis of role-based access control, Tech. rep., RTI International (2010).

[100] W. Shang, Q. Ding, A. Marianantoni, J. Burke, L. Zhang, Securing building management systems using named data networking, IEEE Network 28 (3) (2014) 50–56.

[101] H. F. Atlam, M. O. Alassafi, A. Alenezi, R. J. Walters, G. B. Wills, Xacml for building access control policies in internet of things., in: IoTBDS, 2018, pp. 253–260.

[102] T. Kalajainen, et al., An access control model in a semantic data structure: Case process modelling of a bleaching line, Department of Computer Science and Engineering.

[103] D. E. Bell, L. J. LaPadula, Secure computer systems: Mathematical foundations, Tech. rep., Mitre Corp (1973).

[104] K. Vijayalakshmi, V. Jayalakshmi, A study on current research and challenges in attribute-based access control model, Intelligent Data Communication Technologies and Internet of Things (2022) 17–31.

[105] W. Sun, H. Su, H. Xie, Policy-engineering optimization with visual representation and separation-of-duty constraints in attribute-based access control, Future Internet 12 (10) (2020) 164.

[106] G. J. Sahani, C. S. Thaker, S. M. Shah, Scalable rbac model for large-scale applications with automatic user-role assignment, International Journal of Communication Networks and Distributed Systems 28 (1) (2022) 76–102.

[107] B. K. Rai, T. Solanki, Access control mechanism in health care information system, in: Cybersecurity, CRC Press, 2021, pp. 149–160.

[108] R. Narasimman, I. Alsmadi, Rbac for healthcare-infrastructure and data storage, arXiv preprint arXiv:2010.11096.

[109] A. Walker, J. Svacina, J. Simmons, T. Cerny, On automated role-based access control assessment in enterprise systems, in: Information Science and Applications: ICISA 2019, Springer, 2020, pp. 375–385.

[110] M. Gupta, S. Bhatt, A. H. Alshehri, R. Sandhu, Access control models in cloud iot services, in: Access Control Models and Architectures For IoT and Cyber Physical Systems, Springer, 2022, pp. 63–96.

[111] N. Saravanan, A. Umamakeswari, Lattice based access control for protecting user data in cloud environments with hybrid security, Computers & Security 100 (2021) 102074.

[112] J. R. Douceur, The sybil attack, in: International workshop on peer-to-peer systems, Springer, 2002, pp. 251–260.

[113] R. Xu, Y. Chen, E. Blasch, G. Chen, Blendcac: A blockchain-enabled decentralized capability-based access control for iots, in: 2018 IEEE International conference on Internet of Things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2018, pp. 1027–1034.

[114] A. Abboud, A. Lahmadi, M. Rusinowitch, M. Couceiro, A. Bouhoula, Poster : Minimizing range rules for packet filtering using a double mask representation, in: 2019 IFIP Networking Conference, Networking 2019, Warsaw, Poland, May 20-22, 2019, IEEE, 2019, pp. 1–2. doi:10.23919/IFIPNetworking46909.2019.8999466.

[115] N. Kang, Z. Liu, J. Rexford, D. Walker, Optimizing the "one big switch" abstraction in software-defined networks, in: K. C. Almeroth, L. Mathy, K. Papagiannaki, V. Misra (Eds.), Conference on emerging Networking Experiments and Technologies, CoNEXT '13, Santa Barbara, CA, USA, December 9-12, 2013, ACM, 2013, pp. 13–24. doi:10.1145/2535372.2535373.

[116] Y. Kanizo, D. Hay, I. Keslassy, Palette: Distributing tables in software-defined networks, in: Proceedings of the IEEE INFOCOM 2013, Turin, Italy, April 14-19, 2013, IEEE, 2013, pp. 545–549. doi:10.1109/INFCOM.2013.6566832.

[117] P. Chuprikov, K. Kogan, S. I. Nikolenko, How to implement complex policies on existing network infrastructure, in: Proceedings of the Symposium on SDN Research, SOSR 2018, Los Angeles, CA, USA, March 28-29, 2018, ACM, 2018, pp. 9:1–9:7. doi:10.1145/3185467.3185477.

[118] A. Abboud, R. Garcia, A. Lahmadi, M. Rusinowitch, A. Bouhoula, Efficient distribution of security policy filtering rules in software defined networks, in: 19th IEEE International Symposium on Network Computing and Applications, NCA 2020, Cambridge, MA, USA, November 24-27, 2020, IEEE, 2020, pp. 1–10. doi:10.1109/NCA51143.2020.9306746.

[119] A. Abboud, R. Garcia, A. Lahmadi, M. Rusinowitch, A. Bouhoula, M. Ayadi, Automatically distributing and updating in-network management rules for software defined networks, in: 2022 IEEE/IFIP Network Operations and Management Symposium, NOMS 2022, Budapest, Hungary, April 25-29, 2022, IEEE, 2022, pp. 1–9. doi:10.1109/NOMS54207.2022.9789807.

[120] Z. Tang, X. Ding, Y. Zhong, L. Yang, K. Li, A self-adaptive bell–lapadula model based on model training with historical access logs, IEEE Transactions on Information Forensics and Security 13 (8) (2018) 2047–2061.

[121] S. Xu, Y. Li, R. Deng, Y. Zhang, X. Luo, X. Liu, Lightweight and expressive fine-grained access control for healthcare internet-of-things, IEEE Transactions on Cloud Computing.

[122] S. Oh, S. Park, Task–role-based access control model, Information systems 28 (6) (2003) 533–562.

[123] S. Tanwar, K. Parekh, R. Evans, Blockchain-based electronic healthcare record system for healthcare 4.0 applications, Journal of Information Security and Applications 50 (2020) 102407.

[124] P. Chinnasamy, P. Deepalakshmi, Hcac-ehr: hybrid cryptographic access control for secure ehr retrieval in healthcare cloud, Journal of Ambient Intelligence and Humanized Computing 13 (2) (2022) 1001–1019.

[125] S. Figueroa, J. Añorga, S. Arrizabalaga, An attribute-based access control model in rfid systems based on blockchain decentralized applications for healthcare environments, Computers 8 (3) (2019) 57.

[126] B. S. Egala, A. K. Pradhan, V. Badarla, S. P. Mohanty, Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control, IEEE Internet of Things Journal 8 (14) (2021) 11717–11731.

[127] M. Y. Alshahrani, Implementation of a blockchain system using improved elliptic curve cryptography algorithm for the performance assessment of the students in the e-learning platform, Applied Sciences 12 (1) (2022) 74.

[128] C.-y. Li, Q. Zhao, N. Herencsar, G. Srivastava, The design of mobile distance online education resource sharing from the perspective of man-machine cooperation, Mobile Networks and Applications 26 (5) (2021) 2141–2152.

[129] S. Joseph, S. Karunan, A blockchain based decentralized transaction settlement system in banking sector, in: 2021 Fourth International Conference on Microelectronics, Signals & Systems (ICMSS), IEEE, 2021, pp. 1–6.

[130] 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.

[131] M. Auxilia, K. Raja, Knowledge based security model for banking in cloud, in: Proceedings of the International Conference on Informatics and Analytics, 2016, pp. 1–6.

[132] H. Guo, E. Meamari, C.-C. Shen, Multi-authority attribute-based access control with smart contract, in: Proceedings of the 2019 international conference on blockchain technology, 2019, pp. 6–11.

[133] X. Yu, Z. Shu, Q. Li, J. Huang, Bc-blpm: A multi-level security access control model based on blockchain technology, China Communications 18 (2) (2021) 110–135.

[134] I. A. Mohammed, Cloud identity and access management–a model proposal, International Journal of Innovations in Engineering Research and Technology 6 (10) (2019) 1–8.

[135] Y. Kawada, K. Yano, Y. Mizuno, T. Tsuchiya, Y. Fujisaki, Data access control for energy-related services in smart public infrastructures, Computers in Industry 88 (2017) 35–43.

[136] B. Fabian, S. Kunz, M. Konnegen, S. Müller, O. Günther, Access control for semantic data federations in industrial product-lifecycle management, Computers in Industry 63 (9) (2012) 930–940.

[137] T.-Y. Chen, Y.-M. Chen, H.-C. Chu, C.-B. Wang, Development of an access control model, system architecture and approaches for resource sharing in virtual enterprise, Computers in Industry 58 (1) (2007) 57–73.

[138] S. Daoudagh, E. Marchetti, M. Loreti, L. Spalazzi, A life cycle for authorization systems development in the GDPR perspective., in: ITASEC, 2020, pp. 128–140.

[139] E. F. Silva, D. C. Muchaluat-Saade, N. C. Fernandes, Across: A generic framework for attribute-based access control with distributed policies for virtual organizations, Future Generation Computer Systems 78 (2018) 1–17.

[140] P. T. Duy, H. Do Hoang, A. G.-T. Nguyen, V.-H. Pham, et al., B-dac: A decentralized access control framework on northbound interface for securing sdn using blockchain, Journal of Information Security and Applications 64 (2022) 103080.

[141] N. Deepa, Q.-V. Pham, D. C. Nguyen, S. Bhattacharya, B. Prabadevi, T. R. Gadekallu, P. K. R. Maddikunta, F. Fang, P. N. Pathirana, A survey on blockchain for big data: approaches, opportunities, and future directions, Future Generation Computer Systems.

[142] T.-Y. Chen, Knowledge sharing in virtual enterprises via an ontology-based access control approach, Computers in Industry 59 (5) (2008) 502–519.

[143] R. Jiang, Y. Xin, Z. Chen, Y. Zhang, A medical big data access control model based on fuzzy trust prediction and regression analysis, Applied Soft Computing 117 (2022) 108423.

[144] Z. Lian, Q. Zeng, W. Wang, T. R. Gadekallu, C. Su, Blockchain-based two-stage federated learning with non-iid data in iomt system, IEEE Transactions on Computational Social Systems.

[145] M. You, J. Yin, H. Wang, J. Cao, K. Wang, Y. Miao, E. Bertino, A knowledge graph empowered online learning framework for access control decision-making, World Wide Web (2022) 1–22.

[146] OASIS, Extensible access control markup language (xacml) version 3.0 (2013).
URL https://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

[147] N. Li, Q. Wang, W. H. Qardaji, E. Bertino, P. Rao, J. Lobo, D. Lin, Access control policy combining: theory meets practice, in: B. Carminati, J. Joshi (Eds.), 14th ACM Symposium on Access Control Models and Technologies, SACMAT 2009, Stresa, Italy, June 3-5, 2009, Proceedings, ACM, 2009, pp. 135–144. doi:10.1145/1542207.1542229.

[148] E. Bertino, B. Catania, E. Ferrari, P. Perlasca, A logical framework for reasoning about access control models, ACM Trans. Inf. Syst. Secur. 6 (1) (2003) 71–127. doi:10.1145/605434.605437.

[149] A. Jeffrey, T. Samak, Model checking firewall policy configurations, in: POLICY 2009, IEEE International Symposium on Policies for Distributed Systems and Networks, London, UK, 20-22 July 2009, IEEE Computer Society, 2009, pp. 60–67. doi:10.1109/POLICY.2009.32.

[150] G. Bruns, D. S. Dantas, M. Huth, A simple and expressive semantic framework for policy composition in access control, in: P. Ning, V. Atluri, V. D. Gligor, H. Mantel (Eds.), Proceedings of the 2007 ACM workshop on Formal methods in security engineering, FMSE 2007, Fairfax, VA, USA, November 2, 2007, ACM, 2007, pp. 12–21. doi:10.1145/1314436.1314439.

[151] S. Jha, N. Li, M. V. Tripunitara, Q. Wang, W. H. Winsborough, Towards formal verification of role-based access control policies, IEEE Trans. Dependable Secur. Comput. 5 (4) (2008) 242–255. doi:10.1109/TDSC.2007.70225.

[152] S. K. Lahiri, S. Chen, Y. Wang, I. Dillig, Formal specification and verification of smart contracts for azure blockchain, CoRR abs/1812.08829. arXiv:1812.08829.

[153] A. Saâdaoui, N. B. Y. B. Souayeh, A. Bouhoula, Automated and optimized formal approach to verify SDN access-control misconfigurations, in: H. Gao, Y. Yin, X. Yang, H. Miao (Eds.), Testbeds and Research Infrastructures for the Development of Networks and Communications - 13th EAI International Conference, TridentCom 2018, Shanghai, China, December 1-3, 2018, Proceedings, Vol. 270 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer, 2018, pp. 96–112. doi:10.1007/978-3-030-12971-2_6.

[154] P. Colombo, E. Ferrari, Access control in the era of big data: state of the art and research directions, in: Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies, 2018, pp. 185–192.

[155] I. H. Sarker, M. H. Furhad, R. Nowrozy, Ai-driven cybersecurity: an overview, security intelligence modeling and research directions, SN Computer Science 2 (3) (2021) 1–18.

[156] S. Daoudagh, E. Marchetti, The GDPR compliance and access control systems: Challenges and research opportunities.

Appendix A. List of Abbreviations

AA	Attribute Authorities
ABAC	Attribute Based Access Control
ABE	Attribute Based Encryption
ABS	Attribute-Based Signatures
ACL	Access Control List
AC	Access Control
AES	Advanced Encryption Standard
AWS	Amazon Web Services
B-DAC	Blockchain-based framework for Decentralized authentication and fine-grained Access Control
BacS	Blockchain-based access control Scheme
BC-BLPM	Blockchain-based Bell-LaPadula Model
BDSS-FA	Blockchain-Based Secure Data-sharing platform with Fine-grained Access Control
BlendCAC	Blockchain-enabled decentralized Capability-based Access Control
BSeIn	Blockchain-based Secure mutual authentication with fine-grained access control system for Industry
C-CP-ARBE	Collaborative-Ciphertext Policy-Attribute Role-Based Encryption
C-RBAC	Context-aware Role-based Access Control
CapBAC	Capability-based Access Control
CA	Certificate Authority
CBA	Capability Based Access
CL	Capability List
CP-ABE	Ciphertext-based Attribute Encryption
CSD	Critical Set Detection
DAC	Discretionary Access Control
DDoS	Distributed Denial of Service
DoS	Denial of Service
DS	Digital Signature
FADB	Fine-grained Access control scheme for VANET Data based on Blockchain

FlowNAC	Flow-based Network Access Control
GCP-IoTAC	Google Cloud Platform IoT Access Control
GDPR	General Data Protection Regulation
GP	Group Policy
HABE	Hierarchical Attribute Based Encryption
HASBE	Hierarchical Attribute - Set Based Encryption
IACAC	Identity Authentication and Capability-based Access Control
IoMT	Internet of Medical Things
IoT	Internet of Things
ISMS	Information Security Management System
KBAC	Knowledge Based Access Control
KBSM	Knowledge Based Security Model
KP-ABE	Key Policy Atribute Based Encryption
L-ABAC	Location-aware Attribute-based Access Control
LBAC	Lattice-based Access Control
LDAP	Lightweight Directory Access Protocol
LPAC	Lightweight Privacy-aware Access Control
LPM	Longest Prefix Match
MAC	Mandatory Access Control
MITM	Man-In-The-Middle
MRE	Multi-receiver Encryption
P2P	Peer-to-Peer
PAP	Policy Administration Point
PAR-AC	Policy based, Attribute based, Role based, Access Control
PBAC	Policy Based Access Control
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIP	Policy Information Point
PNAC	Port-based Access Control
PRA97	Permission-Role Assignment '97
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role Based Access Control
RDBMS	Relational Database Management System

RFID	Radio Frequency Identification
RMAC	Reference Monitoring Access Control
RRA97	Role-Role Assignment '97
RSA	Rivest-Shamir-Adleman
RuBAC	Rule Based Access Control
SaaS	Software-as-a-Service
SBAC	A Secure Blockchain-based Access Control
SCBAC	Smart-Contract based Access Control
SDN	Software Defined Networking
SEM-ACSIT	Secure and Efficient Multi-authority Access Control for IoT Cloud Storage
SEMAAC	Secure and Efficient Multi-Authority Access Control
SI Axiom	Simple Integrity Axiom
SLA	Service Level Agreements
SoD	Segregation of Duties
SRAC	Selective Ring-based Access Control
T-RBAC	Task Role-based Access Control
TBAC	Transactional-Based Access Control
TCAM	Ternary Content Addressable Memory
TCP	Transmission Control Protocol
UCON	Usage Control-based Access Control
UDP	User Datagram Protocol
URA97	User-Role Assignment '97
VANET	Vehicle Ad Hoc Network
XACML	eXtensible Access Control Markup Language

Declaration of interest statement

This is hereby certify that the paper is original, neither the paper nor a part of it is under consideration for publication anywhere else. Also, we have no conflicts of interest to disclose.

We confirm that the manuscript has been read and approved by all named authors.

Best Regards,
Authors