IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 13 January 2025, accepted 20 January 2025, date of publication 23 January 2025, date of current version 29 January 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3533145

SURVEY

A Systematic Review of Access Control Models: Background, Existing Research, and Challenges

NASTARAN FARHADIGHALATI, LUIS A. ESTRADA-JIMENEZ, SANAZ NIKGHADAM-HOJJATI, (Member, IEEE), AND JOSE BARATA, (Member, IEEE)

NOVA School of Science and Technology, Center of Technology and Systems (UNINOVA-CTS), 2829-516 Lisbon, Portugal
Associated Lab of Intelligent Systems (LASI), NOVA University Lisbon, 2829-516 Lisbon, Portugal

Corresponding author: Nastaran Farhadighalati (nastaran.farhadi@uninova.pt)

This research was funded (in part) by the Portuguese FCT program, Center of Technology and Systems (CTS) CTS/00066.

ABSTRACT Data security has become paramount, especially with the exponential growth of data, the rise of cyber threats, and the increasing prevalence of remote work. Data confidentiality, integrity, and availability are crucial, particularly in sensitive domains like healthcare and cloud computing. While robust access control (AC) is essential, it must be balanced with maintaining operational efficiency. In access control models, there is a general lack of a comprehensive cross-domain overview, insufficient focus on evolving access control requirements, and inadequate analysis of challenges and issues. This paper comprehensively analyzes access control models (ACMs) through a two-pronged approach. First, we conduct a Narrative Literature Review(NLR) to classify traditional ACMs, evaluating their security strengths and weaknesses and compatible security protocols. Second, we perform a Systematic Literature Review (SLR) of emerging ACMs developed over the past decade across various domains. This systematic review has three primary objectives: (1) to introduce and analyze these emerging ACMs, (2) to present their current technological status, and (3) to identify key challenges and promising research directions. By combining these approaches, this paper offers a comprehensive overview of ACM applications and techniques, identifies existing challenges, and explores future research directions to guide advancements in access control.

INDEX TERMS Access control (AC), access control model (ACM), security, data, requirements.

GLOSSARY

AAA	Authentication,Authorization,Accountability.
ABAC	Attribute-Based Access Control.
ABE	Attribute-Based Encryption.
ABSC	Attribute-Based SignCryption.
AC	Access Control.
ACL	Access Control list.
ACM	Access Control Model.
ARBAC	Administration Role-Based Access Control.
BBAC	Behavior-Based Access Control.
BLP	Bell-LaPadula.
BMA	British Medical Association.
C-TMAC	Collaborative Team-Based Access Control.
CA-TMAC	Context-Aware Team-Based Access Control.
CC	Cloud Computing.
CL	Capability List.
D-TMAC	Dynamic Team-Based Access Control.
DAC	Discretionary Access Control.
E-BAC	Emotion-based Access Control.
EHR	Electronic Health Record.
EMR	Electronic Medical Record.
EnBAC	Entity-Based Access Control.
HBAC	History-based Access Control.
HE	Homomorphic Encryption.
ICN	Information-Centric Networking.
ID	Identity.
IoT	Internet of Thing.

The associate editor coordinating the review of this manuscript and approving it for publication was Martin Reisslein.

MAC	Mandatory Access Control.
MFA	Multi-Factor Authentication.
ML	Machine Learning.
MLS	Multilevel Security Model.
NLR	Narrative Literature Review.
OrBAC	Organization-Based Access Control.
OSN	Online Social Network.
OWL	Web Ontology Language.
PHR	Patient Health Record.
RAdAC	Risk-Adaptive Access Control.
RBAC	Role-Based Access Control.
RBAC0	Flat RBAC.
RBAC1	Hierarchical RBAC.
RBAC2	Constrained RBAC.
RBAC3	Symmetric RBAC.
ReBAC	Relation-Based Access Control.
RiskBAC	Risk-Based Access Control.
RQ	Research Question.
RuBAC	Rule-Based Access Control.
SDN	Software-Defined Networking.
SLR	Systematic Literature Review.
SVM	Support Vector Machine.
TBAC	Task-Based Access Control.
TmBAC	Team-Based Access Control.
TOMCAC	Task-Oriented Multilevel Cooperative Access Control.
TR-DSAC	Task-Role Based Dual System Access Control.
UCON	Usage-based Access Control.
VBAC	View-Based Access Control.
XACML	eXtensible Access Control Markup Language.

I. INTRODUCTION

Data is a crucial resource that requires robust security measures. With the increasing volume of data, rising cyber threats, and the shift to remote work, effective data protection is more important than ever. Ensuring the confidentiality, integrity, and availability of data is essential to prevent unauthorized access and maintain information reliability [1]. Although strict "access control(AC)" laws are critical, it is equally important to keep these processes efficient. AC processes should be efficient with minimal delays and structured to minimize false negatives. Moving towards automation and reducing false positives can help organizations streamline employee access while upholding strong security measures.

AC is fundamental to data security, regulating how users and systems access data and resources. Over the past decade, the significant increase in AC research underscores the growing importance of securing digital systems and data. The line graph reveals a steady upward trend in the number of published access control papers (Fig. 1).

Its importance is evident in its widespread use across distributed systems and its critical role in today's interconnected, data-driven world. AC ensures that only authorized personnel within an organization can access resources. As a

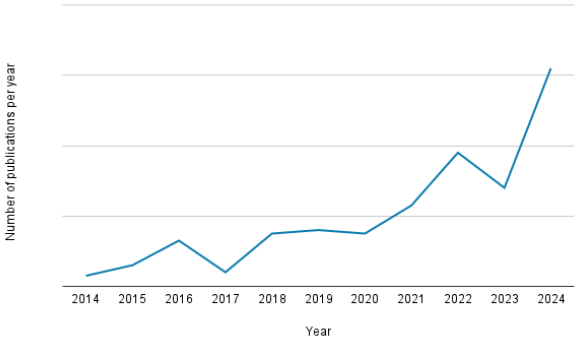

FIGURE 1. Distribution of published articles in the field of access control.

fundamental mechanism in data security, access control defines who is allowed to access or perform actions on objects within a computing environment and the specific conditions under which this access is granted. AC regulates permissions based on user privilege levels, allowing access after successful authentication. As Coronado et al. defined, "access control" refers to [2]:

> *"The prevention of unauthorized use of a resource, including the prevention of the use of a resource in an unauthorized manner."*

Without access control, sensitive data could be exposed to unauthorized users, leading to privacy violations and security risks. Such a lack of control undermines data protection and compromises organizational security. For example, in 2024, several banks faced significant fines due to unauthorized access to customer data. Santander Bank Polska S.A. was fined €326,000 for insufficient data security, while UniCredit S.p.A. incurred a €2.8 million fine for similar violations [3].

To mitigate these risks, organizations must implement robust AC strategies. Effective information security systems are essential for protecting data from unauthorized access and malicious activities while maintaining data availability. Despite the importance of robust AC strategies, many companies struggle with data security.

A major challenge in AC is developing a unified access control model (ACM) that combines features from existing, often incompatible frameworks [4](In *Subsection* VI-C, this issue will also be discussed, with a focus on identifying the key requirements for effective access control). Traditional models address various aspects such as adaptability, context awareness, flexibility, and scalability. However, new ACMs are being developed to meet essential security requirements. Categorizing these models helps organizations choose the most appropriate one for their needs. Understanding key AC requirements is crucial for building effective access control systems in today's complex environment.

This review paper examines traditional ACMs, discussing their advantages and disadvantages in detail. We investigate the challenges associated with these models, focusing on the technologies involved and the fundamental requirements

for implementing effective security measures. By analyzing these aspects, we aim to highlight current access control practices' limitations and their implications for system security. Our goal is to provide insights that will help researchers design improved access control models that not only enhance security but also address the evolving needs of modern systems. Taking a close look at this topic, we hope to emphasize the challenges, requirements, and technologies that can better safeguard sensitive information in digital environments that are becoming increasingly complex.

A. MOTIVATION OF THIS WORK

Several researchers have conducted surveys on ACMs, assessing authentication, access control, and privacy across different domains (see Table. 1). These studies share three main goals: reviewing traditional ACMs, identifying challenges in their specific areas, and evaluating current solutions. While some studies investigate how ACM has evolved, others focus on the latest approaches. All aim to identify gaps and propose improvements in AC systems.

Many papers review traditional ACMs, highlighting their benefits and drawbacks in various contexts, such as the Internet of Things (IoT) [5], Software-Defined Networking (SDN) [6], and Electronic Health Records (EHRs) [5]. They assess the effectiveness of these models, particularly in IoT systems, where multiple devices require different levels of security.

Other studies explore the applications of the ACMs [7], the areas that are covered, and the specific security needs they address [8]. These works identify gaps and predict future trends, illustrating how various ACMs address distinct security requirements and emphasizing the importance of updating access control as security needs evolve.

These papers employ different methodologies to examine ACMs across various domains. Although they all focus on AC, each study provides unique insights into the development and functionality of models in specific contexts. These studies provide a detailed analysis of ACM challenges, as a guide for future security enhancements.

To the best of our knowledge, no comprehensive review has provided a general overview of ACMs. This review is intended for researchers interested in gaining a broad understanding of ACMs before delving into specific domains. Additionally, existing studies have not sufficiently addressed AC requirements for data or highlighted the most critical ones over an extended period. Such a review is essential for understanding key recurring requirements and guiding the development of new ACMs. By identifying current gaps and inconsistencies, this work aims to direct future research and contribute to the creation of more effective and adaptable access control solutions.

Specifically, this research is motivated by the following key needs and gaps:

- Lack of a comprehensive cross-Domain Overview: While existing literature examines ACMs in specific contexts, a holistic review offering a broad understanding across various domains is missing. This paper aims to fill this void, providing a foundational understanding for researchers before they explore domain-specific analyses.
- Insufficient focus on evolving access control requirements: Current studies have not adequately addressed the changing access control requirements, especially concerning data privacy and the most critical needs over time. This review analyzes recurring requirements to guide the development of future ACMs.
- Need for a clear categorization and taxonomy: A comprehensive categorization of traditional ACMs, including their strengths and limitations, is necessary. Furthermore, a taxonomy of application domains and technologies used to implement emerging ACMs while preserving data privacy is required.
- Inadequate analysis of challenges and issues: An in-depth review of the challenges and issues discussed in existing literature is needed to identify inconsistencies and direct future research.

Therefore, this paper aims to:

- Provide a comprehensive categorization of traditional ACMs, highlighting their strengths and limitations.
- Develop a taxonomy of application domains and technologies used in emerging ACMs, with a focus on preserving data privacy.
- Analyze access control requirements in emerging ACMs.
- Conduct an in-depth review of the challenges and issues discussed in the existing literature.

B. PURPOSE, SCOPE, AND CONTRIBUTIONS OF THE CURRENT WORK

This section highlights the key contributions and scope of our review, emphasizing its comprehensive approach and relevance to the field. Our study uses a well-structured methodology, following systematic guidelines to identify, categorize, and analyze the literature on ACMs. The objectives and contributions of this work include:

- Comprehensive Categorization of ACMs: This paper provides a detailed classification of traditional ACMss, summarizing their key strengths, limitations, and contexts of use.
- Systematic Literature Review (SLR) Methodology: We follow SLR [12] guidelines to select relevant research articles and use both mechanical and machine learning methods to improve the accuracy of paper selection.
- Temporal Scope: The review focuses on studies from the past ten years to ensure the analysis captures the most up-to-date advancements in ACMs.
- Identification of Access Control Challenges and Requirements: Key challenges in implementing ACMs are explored, alongside a thorough analysis of critical security requirements for enhancing security in complex and dynamic environments.

TABLE 1. Existing review papers about access control model (ACM).

Ref	Main focus
[8] 2024	- Evaluate the current state of research on authorization and ACMs for various database models. - Identify five key requirements: granularity, content-based authorizations, context-based authorizations, custom authorizations, and separation of concerns.
[9] 2023	- State-of-the-art ACM techniques. - Recent research trends in CC, blockchain, IoT, and SDN. - Challenges and opportunities in these technologies.
[7] 2022	- Analysis of traditional ACMs. - Compare strengths, weaknesses, and applications. - Explain gaps in foundational models and emerging trends, particularly in IoT and CC.
[6] 2020	- Detailed review of ACMs. - Cover conventional approaches and those adapted for OSN and IoT. - Compare models and assess strengths, weaknesses, and challenges of ACMs. - Discuss potential solutions for these systems.
[10] 2019	- Comprehensive review of authentication methods for securing IoT. - Compare existing mechanisms and identify areas for further research. - Offer guidance for developing secure IoT authentication schemes.
[11] 2017	- Overview of different AC solutions in IoT. - Outline strengths and weaknesses of traditional and modern ACMs and protocols in IoT.
[5] 2015	- Identify key technical features for security and privacy in EHR systems. - Develop a template for implementing these measures through a systematic literature review.

- Analysis of Domains and Techniques: This study focus on identifying and categorizing the areas covered and the technical methods used in ACMs studies.

Therefore, the key Research Questions (RQs) addressed in this review are summarized as follows:

What are the most common traditional ACMs used to ensure data security? What are their key components, advantages, and limitations?

What emerging ACMs are built on traditional models, and what are their key features?

To address these questions, *Section* III provides an overview of traditional ACMs, while *Sections* V, and VI delve into the details of emerging ACMs and their key features.

In this regard, the structure of this review is organized as follows: Section II provides a comprehensive overview of the definition, key concepts, and principles of ACM. Section III includes a classification of traditional ACMs, their essential components, and an analysis of the strengths and weaknesses of each model. *Section* IV outlines the methodology used for this literature review. *Section* V presents the results derived from the analysis conducted throughout the review. *Section* VI discusses the findings, and provides an in-depth analysis of the reviewed studies, including future directions and challenges of the examined works. *Section* VII discusses the limitations of the literature review methodology, while *Section* VIII provides the conclusions of this study.

II. ACCESS CONTROL MODEL FOUNDATIONS: KEY CONCEPTS, ELEMENTS, AND PRINCIPLES

A. ACCESS CONTROL MODEL DEFINITION AND ELEMENTS

Access Control Models (ACMs) are designed to enforce policies that determine who can access specific data or systems, under what conditions, and how permissions are managed. Various scholars have defined ACMs from differing perspectives, emphasizing distinct aspects of these frameworks.

ACM comprises several key elements that regulate access to sensitive resources. Understanding these components is essential for implementing effective access control strategies that ensure data security and compliance within an organization. The primary elements include the "subject", which is the entity requesting access; the "object", representing the data resource being targeted; the "operation", defining the action the subject intends to perform on the object; "access rights or permissions", specifying the allowed actions; "and access policies or rules", outlining the conditions under which access is granted or denied. These components work together to enforce consistent access control mechanisms across the organization. For a visual representation, (Fig. 2), which illustrates the access control elements [13].

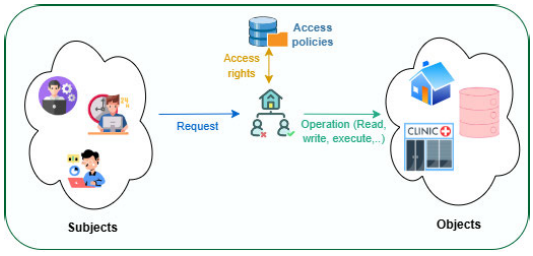

FIGURE 2. Access control elements (Adapted from [14]).

B. ACCESS CONTROL MODEL PRINCIPLES

By defining who can access what, under which conditions, and what actions they can perform, these models help organizations maintain robust security postures. They ensure that access is granted based on predefined criteria, such

FIGURE 3. Taxonomy of access control model (ACM).

as user roles, attributes, or specific conditions, thereby minimizing the risk of unauthorized access and potential security breaches [4].

ACM designs involve key questions: "Who" defines authorized users or groups, "What" specifies the resource being accessed, "When" sets time constraints for access, "Where" identifies allowed physical or network locations, "Why" justifies access based on needs or sensitivity, and "How" determines the methods and permissions for granting access.

III. CONVENTIONAL ACCESS CONTROL MODELS

In this section, we will explore each traditional ACMs in detail, highlighting their advantages and limitations.

A. TAXONOMY OF TRADITIONAL ACCESS CONTROL MODELS

In this part, we provide a review of conventional ACMs and discuss their evolution over time. Additionally, we present a taxonomy of these models, as illustrated in Fig. 3. To achieve this, we adopt a Narrative Literature Review (NLR) approach, which provides a comprehensive, critical, and subjective summary of the existing literature [15]. This methodology allows for a flexible and less structured exploration of the topic, enabling the integration of diverse sources and perspectives. While this approach offers a broad view of the subject, it also relies on the interpretation and selection of literature, making it susceptible to bias [16].

1) IDENTITY-CENTRIC ACCESS CONTROL MODEL

This approach uses verified credentials like usernames to confirm identity, offering a simple method for access management in systems requiring user verification.

- *Discretionary Access Control (DAC)*

DAC (Fig. 4) allows resource owners, typically the creators, to grant access based on user identity, offering flexibility. However, DAC alone cannot ensure system security and is often combined with MAC or other models for enhanced protection [17].

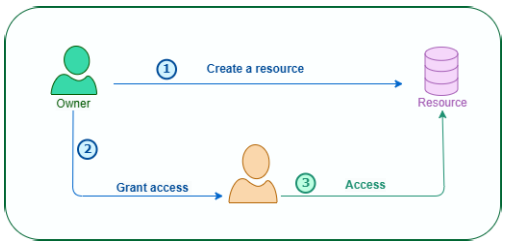

FIGURE 4. DAC (Adapted from [18]).

2) MATRIX-CENTRIC ACCESS CONTROL MODEL

Matrix-centric access control assigns permissions directly to users for specific resources, providing a structured and transparent method ideal for systems with stable users and resources.

- *Access Control List (ACL)*

ACL (Fig. 5) manage data access in shared systems by listing subjects and their authorized operations on objects, presenting the access matrix from a column perspective [19].

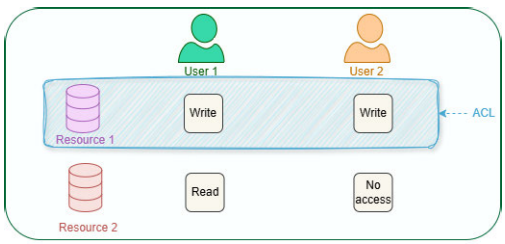

FIGURE 5. ACL (Adapted from [19]).

- *Capability List (CL)*

The CL (Fig. 6) is an alternative to ACL, focusing on subjects and specifying which objects they can access,

whereas ACL associates with objects and defines which subjects can access them [20].

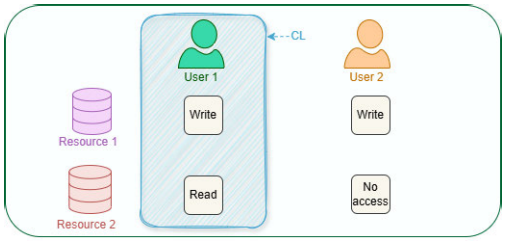

FIGURE 6. CL (Adapted from [20]).

• *View-Based Access Control (VBAC)*

VBAC (Fig. 7) is a database model that uses views and virtual tables to provide customized data access. It allows users to interact with specific subsets of data without exposing the entire database. Database administrators define views through queries, assign access privileges, and restrict users to these predefined views, ensuring controlled data interaction [21].

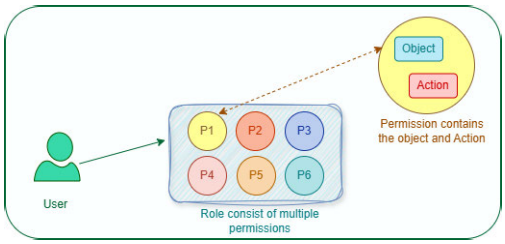

FIGURE 7. VBAC (Adopted from [21]).

3) RULE-CENTRIC ACCESS CONTROL MODEL

Some ACMs use predefined rules to determine access, applying them uniformly to all users without considering individual identities. These rules set the conditions for user-resource interactions.

• *Mandatory Access Model (MAC)*

MAC (Fig. 8), also known as Lattice-based Access Control, is a stricter alternative to DAC. In MAC, access policies are centrally managed, and users cannot modify their own permissions. It enforces strict security protocols, ensuring users can only access resources at the same or lower security levels, with classifications like *Top Secret (TS)*, *Secret (S)*, *Confidential (C)*, and *Unclassified (U)* indicating varying levels of risk associated with unauthorized access [18].

• *Multilevel Security Model (MLS)*

MLS is particularly relevant in Cross-Domain Systems (CDS), where data must be securely shared across different security domains (e.g., between government agencies, healthcare organizations, or military branches). MLS ensures that sensitive information is protected even when accessed by users from different domains, by enforcing strict access

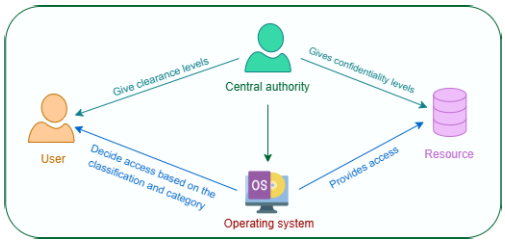

FIGURE 8. MAC (Adapted from [18]).

controls based on hierarchical security levels. For example, in a military CDS, a user with a confidential clearance can not access top secret documents, even if they are part of a shared cross-domain system [22].

The following are some well-known approaches to MLS:

- Bell-LaPadula (BLP): The BLP model is designed to protect information confidentiality, particularly in government and military settings. It classifies data and users into security levels, with users assigned clearance to access data. The model enforces two key rules: the Simple Security Property ("No Read Up"), which prevents users from reading higher-classified data, and the *Star Property* (*No Write Down*), which restricts writing to lower-classified data. The "Strong Star Property" further limits both reading and writing to the same security level for enhanced security [23].
- Biba: The Biba model focuses on data integrity by controlling information flow and preventing unauthorized changes. It assigns integrity labels to both users and data, ensuring users cannot alter higher integrity data or be influenced by lower integrity data. Unlike the BLP model, which emphasizes confidentiality, Biba prioritizes integrity. It enforces three key rules: the "Simple Integrity Rule" (prevents reading lower integrity data), the "Star Integrity Rule" (prevents writing to higher integrity levels), and the "Invocation Property" (restricts access from lower integrity levels) [24].

• *Multilateral Security*

Multilateral security differs from traditional hierarchical models by managing lateral information flows rather than focusing solely on security levels between entities. It enables secure sharing of sensitive information across competing or compartmentalized groups, such as healthcare providers sharing medical records, while maintaining necessary restrictions to protect confidentiality. ACMs based on Multilateral Security principles include [25]:

- Chinese wall policy: The Chinese Wall policy is a security model that prevents conflicts of interest by restricting access to sensitive information in organizations handling data from competing companies. It applies two main rules: the "Simple Security Rule", which prevents users from accessing data from different groups after interacting with one, and the "Property Rule", which restricts writing data to other groups. This model ensures confidentiality, particularly in industries

like financial services and consulting, and enhances security in shared cloud environments.

- British Medical Association (BMA): The BMA model includes various frameworks and tools designed to improve healthcare delivery and governance. It is essential not only for professional medical associations but also serves as a benchmark for other organizations. A key feature of the BMA model is its governance structure, which follows a clear system that encourages effective communication and consensus-building among its members.

• *Rule-Based Access Control (RuBAC) Model*

The RuBAC (Fig. 9) model uses rules to determine who can access specific resources, offering flexibility in managing access permissions based on attributes like user roles, job titles, location, and time of day. This adaptability allows RuBAC to handle complex rules and changing conditions. It provides benefits like granular control and efficiency, automating many access control tasks. Common use cases include OSN, CC, and enterprise applications, where it regulates access to profiles, content, resources, and sensitive information [26].

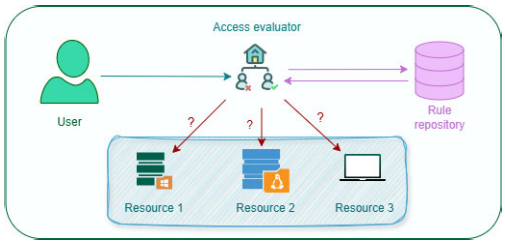

FIGURE 9. RuBAC (Adapted from [26]).

4) ROLE-CENTRIC ACCESS CONTROL MODEL

This approach simplifies management by assigning permissions to roles rather than individual users, making it easier to adapt to organizational changes.

• *Role-Based Access Control (RBAC) Model*

The RBAC (Fig. 10) framework simplifies access management by assigning permissions based on user roles, reducing administrative tasks, and enhancing security. It organizes access control around roles, permissions, and users, ensuring efficient management and protecting sensitive information [18].

RBAC comes in several variations, each offering different levels of complexity and functionality. "Flat RBAC (RBAC0)" is a basic model where roles are not hierarchical, and permissions are directly assigned to roles. "Hierarchical RBAC (RBAC1)" organizes roles hierarchically, allowing permission inheritance, aligning with organizational structures. "Constrained RBAC (RBAC2)" adds restrictions on role assignments and activation periods, incorporating Separation of Duty (SoD) to prevent conflicts of interest. "Symmetric RBAC (RBAC3)" is the most advanced model, including periodic permission-role reviews for dynamic, flexible permission management.

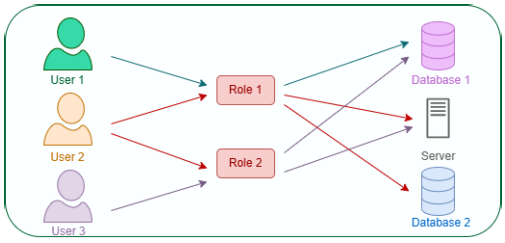

FIGURE 10. RBAC(Adapted from [18]).

• *Administration Role-Based Access Control (ARBAC) Model*

ARBAC (Fig. 11) extends RBAC by adding administrative roles to manage access policies, enhancing security and organization. It includes components like User-Role Assignment (URA), Permission-Role Assignment (PRA), and Role-Role Assignment (RRA) to efficiently manage user roles and permissions. This model allows for better separation of administrative duties and access control management.

The sub-branch of ARBAC includes "RBAC97", which introduces key components of role-based access control with decentralized, flexible role management. "ARBAC99" extends RBAC97 by improving the management of mobile and immobile users and their permissions. Building on ARBAC99, it "RBAC02" addresses multi-step user assignments and duplicate permission-role assignments [27].

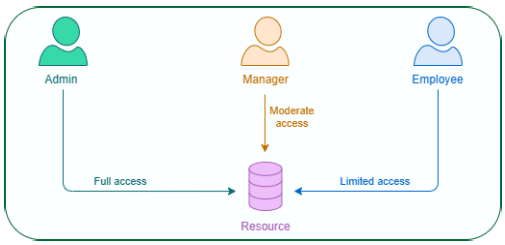

FIGURE 11. ARBAC.

• *Organization-Based Access Control (OrBAC) Model*

OrBAC (Fig. 12) is a model that structures access control policies based on an organization's hierarchy, defining roles for user responsibilities, activities for actions they can perform, and views for objects they can access. It uses ternary relationships to link these components, allowing for flexible and context-aware access control. Additionally, OrBAC supports the use of contextual policies that adapt to dynamic factors like time or location, providing a more adaptive approach to managing access within organizations [18].

The OrBAC model has various extensions, including "AdOr-BAC", which enhances OrBAC by adding administrative capabilities for managing dynamic roles and adapting to organizational changes. "Contextual OrBAC" integrates situational context, such as time and location, into access policies, enabling more adaptive and secure control. Additionally,

"OrBAC with Obligations" expands OrBAC by incorporating required or prohibited actions based on specific conditions.

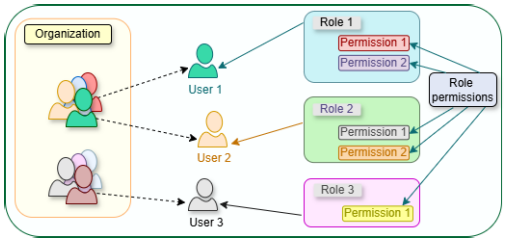

FIGURE 12. OrBAC (Adapted from [28]).

• *Team-Based Access Control (TmBAC) Model*

The TmBAC model (Fig. 13) builds on RBAC by incorporating teams, roles, and permissions, allowing access based on both individual roles and team memberships [29].

Its variants include "Collaborative Team-Based Access Control (C-TMAC)", which manages roles, users, contexts, permissions, and sessions, influenced by factors like time and location. "Context-Aware Team-Based Access Control (CA-TMAC)" assigns roles and permissions with access decisions based on contextual factors such as time and location. "Dynamic Team-Based Access Control (D-TMAC)" allows dynamic updates to team memberships, role assignments, and access rights without disrupting operations.

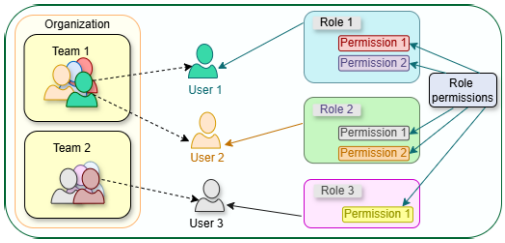

FIGURE 13. TmBAC (Adapted from [29]).

• *Role-Based Access Control Model Extensions*

Traditional RBAC models are evolving to address new demands by incorporating contextual information into access decisions. These extensions enhance RBAC by adding features that make it more flexible and effective in different scenarios. Some key types of RBAC include [30]:

- Temporal RBAC (T-RBAC): Restricts role permissions to specific timeframes, activating or deactivating roles based on time.
- GEO-RBAC: enables access based on a user's location within a designated geographic area.
- Tie-RBAC: tailors RBAC for social networks, granting access based on social relationships.

5) CONTENT-CENTRIC ACCESS CONTROL MODEL

Content-centric access control uses resource attributes to enable flexible, fine-grained permissions, reducing administrative effort and supporting dynamic environments.

• *Attribute-Based Access Control (ABAC) Model*

ABAC (Fig. 14) is a flexible access control model that evaluates attributes of users, resources, and environmental factors to make dynamic access decisions. This makes it more detailed and context-aware compared to traditional models like RBAC [18].

There are several variants of ABAC, including $ABAC_a$, a foundational model that supports MAC, DAC, and RBAC features, enabling dynamic access control, and $ABAC_b$, which extends $ABAC_a$ by incorporating constraint attributes for more complex and precise access decisions.

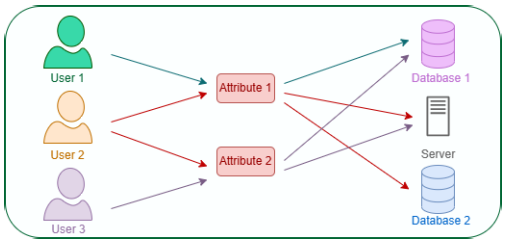

FIGURE 14. ABAC (Adapted from [18]).

• *Task-Based Access Control (TBAC) Model*

TBAC (Fig. 15) grants permissions based on tasks rather than user identities or attributes, ensuring users have the necessary access to complete specific responsibilities. This model provides fine-grained control, adaptability to dynamic environments, and enhanced security by limiting access to task-relevant resources.

Several variations of TBAC have emerged to address specific needs [31], including Task-Role Based Dual System Access Control (TR-DSAC), which integrates TBAC and RBAC to grant access based on task sequences and user roles, and Task-Oriented Multilevel Cooperative Access Control (TOMCAC), a workflow-based model tailored for CC environments, aligning access with task execution.

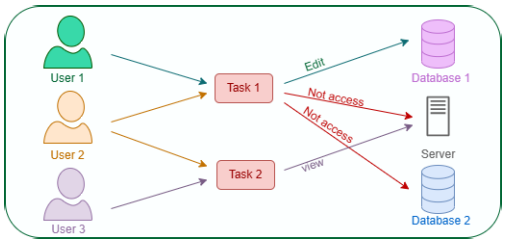

FIGURE 15. TBAC (Adapted from [31]).

• *Relation-Based Access Control (ReBAC) Model*

ReBAC (Fig. 16) leverages social connections and interactions within networks to make dynamic access decisions. Unlike static models, it adapts permissions based on trust levels, user closeness, and past interactions. This personalized approach enhances security by aligning access rights with the evolving social context of relationships [32].

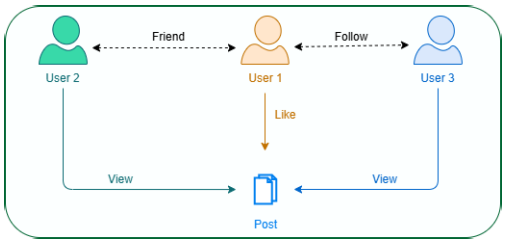

FIGURE 16. ReBAC.

• *Entity-Based Access Control (EnBAC) Model*

The EnBAC (Fig. 17) is a security model that evaluates access control policies by considering both attributes and relationships using the concept of entities. EnBAC uses an Entity-Relationship (ER) model and entity graph to define complex, fine-grained access policies. It excels in managing permissions for systems with detailed hierarchies and evolving relationships, offering flexibility for diverse scenarios [33].

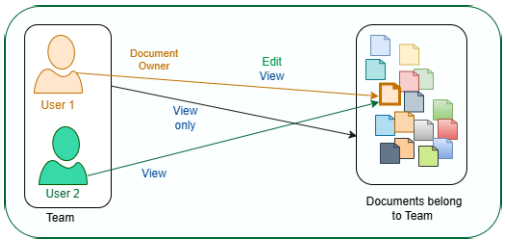

FIGURE 17. EnBAC (Adapted from [33]).

6) CONTEXT-CENTRIC ACCESS CONTROL MODEL

Context-centric access control determines permissions based on contextual factors like action sequences, time, location, and interaction history.

• *Risk-Based Access Control (RiskBAC) Model*

RiskBAC (Fig. 18) manages access by assessing risks in real-time, considering factors beyond standard permissions. It evaluates security risks associated with access requests, compares them to policies, and is particularly suited for dynamic systems like IoT, CC, and sectors requiring quick data access [34].

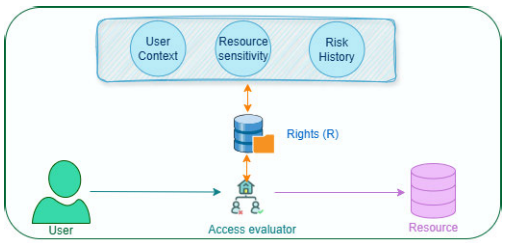

FIGURE 18. RiskBAC (Adapted from [34]).

• *History-based Access Control (HBAC) Model*

HBAC (Fig. 19) enforces access control policies by tracking a program's execution history. It distinguishes between "static rights", the initial permissions granted, and "current rights", which evolve as the program executes. "Access decisions" are based on the program's current rights, updated based on its actions, like accessing specific resources. The system continuously evaluates whether a program's behavior aligns with its permissions and adjusts accordingly. This model ensures dynamic and context-sensitive access control, reflecting the program's actions over time [35].

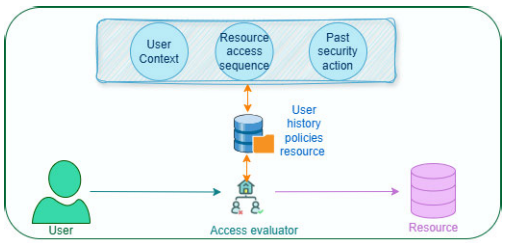

FIGURE 19. HBAC (Adapted from [35]).

• *Emotion-Based Access Control(E-BAC) Model*

E-BAC (Fig. 20) combines emotional recognition with traditional access control to enhance security. It uses emotion detection methods, like facial recognition or behavior analysis, to assess a user's emotional state and adjust access permissions. For example, one system merges iris recognition with emotion detection for smart home environments, while another identifies emotional inconsistencies to trigger security responses. This approach strengthens user authentication by factoring in emotional states alongside standard access controls [36].

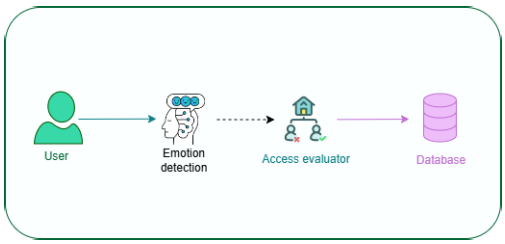

FIGURE 20. E-BAC (Adapted from [36]).

• *Usage-based Access Control (UCON)*

UCON is an advanced access control model that incorporates continuous *Authorization* (A), *oBligation* (B), and *Condition*(C) to dynamically adjust access based on real-time user behavior and context. It emphasizes the ongoing assessment of user permissions throughout the lifecycle of resource usage, allowing for flexible and adaptive security measures. There are several variations of the UCON model, such as UCON_{abc}, which includes all three components, and others like UCON*preA* and UCON*postA*, which focus on authorization before or after access, respectively. Similarly, UCON*preB* and UCON*postB* address obligations before and after access, while UCON*preC* and UCON*postC* deal with conditions evaluated before or after access [37].

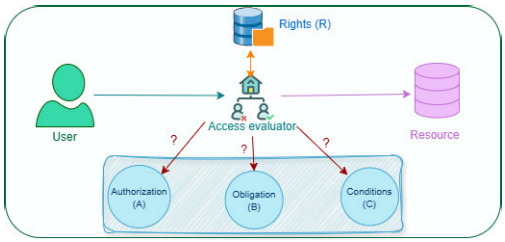

FIGURE 21. UCON (Adapted from [37]).

• *Behavior-Based Access Control (BBAC) Model*

The BBAC (Fig. 22) model manages user access by analyzing behavioral patterns, focusing on "behavior analysis", "dynamic adaptation", and "risk management". It monitors user interactions with software resources, identifying suspicious patterns and adapting access permissions in real-time, particularly in dynamic environments like the IoT. By evaluating historical and current user behavior, it assesses the risk of unauthorized access, strengthening system security. In data-sharing and microservice architectures, BBAC adjusts access based on user behavior and environmental changes, offering enhanced resilience against unauthorized access [38].

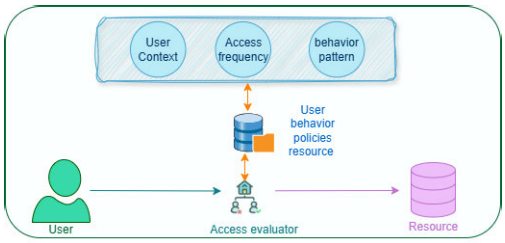

FIGURE 22. BBAC (Adapted from [38]).

B. ANALYSIS OF ACCESS CONTROL MODELS

1) STRENGTHS, AND LIMITATIONS OF TRADITIONAL ACMs

To facilitate a better understanding of the features of each ACM, Table. 2 below offers a clear comparison, highlighting their key characteristics, strengths, and limitations.

2) COMPATIBLE PROTOCOLS OF TRADITIONAL ACMs

Establishing secure access control requires a multi-faceted approach, with security protocols playing a vital role in orchestrating the interconnected processes of authentication, authorization, and auditing (AAA). This section will examine the key security protocols that support these processes and their combined contribution to different traditional access control models (Table. 3).

- Kerberos: A network authentication protocol using secret-key cryptography, relying on a trusted third-party for secure user and service authentication over insecure networks [59].
- IPSec (Internet Protocol Security): A suite of protocols securing IP communications by authenticating and encrypting each packet, ensuring confidentiality, integrity, and authenticity [60].
- TLS/SSL (Transport Layer Security/Secure Sockets Layer): Cryptographic protocols enabling secure communication over networks, with SSL being the predecessor of TLS, commonly used for securing websites [61].
- OAuth 2.0: An authorization framework allowing third-party applications to access user data without exposing credentials, using access tokens [62].
- Zero Trust: It assumes that every user or device, inside or outside the network, should be treated as untrusted until they can prove their legitimacy [63].
- RADIUS/TACACS+ (Remote Authentication Dial-In User Service/Terminal Access Controller Access-Control System Plus): Both are protocols used for network access control. RADIUS is used for authentication and authorization, while TACACS+ provides more granular control and separation between AAA [64].
- LDAP (Lightweight Directory Access Protocol): A protocol for accessing and maintaining distributed directory information services, widely used for authentication and authorization in enterprise environments [65].
- OpenID Connect: An authentication protocol built on OAuth 2.0, enabling single sign-on (SSO) and providing identity information through an ID token [66].
- 802.1X: A network access control protocol for securing wired and wireless networks by ensuring device authorization before access [67].
- MQTT (Message Queuing Telemetry Transport): A lightweight, publish-subscribe messaging protocol designed for low-bandwidth, high-latency, or unreliable networks, used in IoT applications.
- Blockchain: A distributed ledger technology ensuring secure, transparent, and immutable data storage, used in applications like cryptocurrency and decentralized apps.
- AMQP (Advanced Message Queuing Protocol): A message-oriented middleware protocol supporting secure, reliable, and asynchronous messaging, guaranteeing message delivery even during network failures [68].

IV. METHODOLOGY

In this study, we conducted a Systematic Literature Review (SLR) to thoroughly examine major AC requirements. As described in [12], SLR offers the following contributions:

- Clear Methodology: Our well-defined SLR protocol ensures replicable and verifiable findings.
- Comprehensive Review: As a part of this paper, we present an extensive overview of the literature relating to the ACM domains, techniques, and requirements, incorporating multiple perspectives and methodologies.
- Identification of Knowledge Gaps: Systematic analysis of current research identifies emerging trends, challenges, and opportunities in access control.

TABLE 2. Components, strengths, and limitations of ACMs.

ACM Type	Access Control Model	Components	Strengths	Limitations
Identity-centric ACM	DAC [17]	Resource ownership	User empowerment, Flexibility in delegation, Decentralized control [13]	Costly updates, Static management, inefficient for government use, Challenging maintenance [13]
Matrix-centric ACM	ACL [19]	User ID, Access table	Clarity in decision-making, Centralized management [39]	Complexity in large organizations, Potential for misuse, Scalability issues [39]
	CL [20]	User ID, Resource access token	Multidimensional framework, Practical applications [40]	Definitional challenges, Redundant rules [40]
	VBAC [21]	User ID, Resource view	Implementation ease, Flexibility [41]	Complexity in dynamic environments, Interoperability issues [42]
Rule-centric ACM	MAC [18]	User ID, Security label	Strict compliance, Centralized control, reduced risk of data leakage [43]	Lacks fine-grained control, Costly and complex deployment [43]
	MLS [22]	User ID, Classification security level	Controlled access, Enhanced data integrity [22]	Complex implementation, Performance overhead [44]
	Multilateral Security [25]	User ID, Trust relationship	Enhanced cooperation, Legitimacy and influence , Burden sharing [45]	Decision-making delays, Loss of sovereignty , Complexity in coordination [45]
	RuBAC [26]	User ID, Access rule	Simplicity in implementation, Consistency, and adaptability [46]	Scalability issues, Limited flexibility [46]
Role-centric ACM	RBAC [18]	User ID, Role	Centralized management, Adaptability, Enables duty separation [47]	Scalability challenges, Interoperability challenges in collaborative environments, Poor support for dynamic attributes [48]
	ARBAC [27]	Administrative role, Role hierarchy, Role assignment	Scalability, Flexibility [49]	Complexity in management, Potential for centralization [49]
	OrBAC [28]	User ID, Ternary relationships, Context information	Context awareness, Abstract entities, Flexibility in policy specification [50]	Non-adaptive nature, Limited cross-domain support [50]
	TmBAC [29]	User ID, Role, Team, Team membership	Enhanced collaboration, Dynamic management [51]	Complexity in management, Potential security risks [52]
Content-centric ACM	ABAC [18]	User ID, Environmental conditions	Fine-grained access control, Dynamic attribute management, Context-sensitive [18]	Policy Management complexity, High computational resources [18]
	TBAC [31]	User ID, Task attribute, Contextual attributes	Minimizes unauthorized exposure, Flexibility, and improved management [53]	Complex implementation,Performance overhead [31]
	ReBAC [32]	User ID, Relationship	Contextual access control, Flexibility [54]	Complexity in management, Scalability issues [54]
	EnBAC [33]	User ID, Entity attributes	Flexibility, Privacy preservation [55]	Complex implementation, Performance Overhead [33]
Context-centric ACM	RiskBAC [34]	Risk factor, Risk assessment criteria	Dynamic adaptability, Quantitative risk assessment [56]	Complex implementation , Potential for over-restriction [56]
	HBAC [35]	User ID, Behavioral history	Real-time decision making, Scalability, Fine-grained control, Compliance with regulations [57]	Complexity in implementation, Potential for bias, Concurrency challenges [57]
	E-BAC [36]	User ID, Emotional state, Contextual factor	Contextual decision-making , Behavioral analysis , Reduced cognitive load [36]	Accuracy challenges, Complex implementation, Data interpretation challenges [36]
	UCON [37]	User behavior, Contextual factor	Dynamic permission, Obligation management [58]	Complexity, Implementation challenges, Real-time monitoring [58]
	BBAC [38]	Behavior profile, Contextual information	Dynamic risk assessment , Improved accuracy [38]	Data dependency, False positives, Complex implementation [38]

SLR are essential for producing rigorous and credible review papers. By following a structured methodology, SLRs ensure comprehensive and transparent coverage of relevant studies, minimizing bias and enhancing reliability [79]. They focus on specific research questions, enabling consistent evaluation, objective comparisons, and the identification of key themes, trends, and knowledge gaps. SLRs combine quantitative and qualitative insights, often using protocols like PRISMA to improve reproducibility and reliability. This approach integrates studies from multiple fields, offering a holistic understanding of complex topics and uncovering future research opportunities. Widely applicable and highly cited, SLRs provide actionable insights that benefit researchers, practitioners, and policymakers, making them invaluable for impactful academic contributions [80], [81], [82], [83].

This approach provides a comprehensive understanding of ACM, and valuable insights into current knowledge and is especially helpful for researchers gaining an initial understanding of the topic, requirements, and challenges. By focusing on frequently discussed subjects and identifying current research gaps, our review highlights developing trends and opens up opportunities for further study.

We present all phases and stages involved in the SLR process in Fig. 23, as shown in the following steps:

(A) Planning: Defining research questions, developing a search strategy, and establishing study inclusion and exclusion criteria.
(B) Conducting: Identifying relevant studies, assessing their quality, extracting data, and synthesizing findings.
(C) Discussion: Reporting the results clearly and concisely, ensuring transparency and reproducibility.

ACM have been widely studied over the years, driven by advancing technologies and increasing security and privacy concerns. Research efforts continue to adapt these models to address emerging data-related challenges.

This study is significant as it explores AC techniques within data security, aiming to identify key challenges and technological trends that could shape future developments. Through a thorough review of the current landscape, this analysis highlights critical AC requirements and provides insights to guide future research directions.

TABLE 3. Compatible protocol with access control models.

Access control models	Compatible Security Protocols	Why Compatible
DAC	Kerberos, TLS/SSL [59]	Manages discretionary user-defined permissions with strong authentication and secure communications.
ACL	IPSec, 802.1X, RADIUS/TACACS+ [60]	Enforces static access rules effectively at the network or device level.
CL	Kerberos, OAuth 2.0	Supports delegation and token-based resource access while maintaining security.
VBAC	ABAC-compatible protocols (e.g., OAuth 2.0, Zero Trust)	Dynamically evaluates values (e.g., attributes) for conditional access.
MAC	IPSec, TLS/SSL [61]	Enforces rigid, policy-driven access rules to secure sensitive environments.
MLS	IPSec, Kerberos [69]	Ensures hierarchical access based on security levels, especially in classified systems.
Multilateral Security	IPSec, Zero Trust [69]	Ensures secure communications between independent entities or organizations.
RuBAC	OAuth 2.0, Zero Trust, TLS/SSL [62]	Enforces dynamic policies based on predefined rules, ideal for modern applications.
RBAC	Kerberos, RADIUS/TACACS+, LDAP [65]	Assigns permissions based on roles, ensuring centralized authentication and authorization.
ARBAC	OAuth 2.0, OpenID Connect [66]	Combines attributes with roles for fine-grained access control.
OrBAC	Zero Trust, OAuth 2.0 [70]	Supports organization-defined policies and dynamic access control.
TmBAC	Kerberos, OAuth 2.0 [71]	Facilitates team-oriented access with shared credentials and role mappings.
ABAC	OAuth 2.0, Zero Trust, OpenID Connect [72]	Dynamically enforces attribute-based conditions, essential for modern, scalable environments.
TBAC	OAuth 2.0, Kerberos [73]	Assigns access based on task execution and delegation requirements.
ReBAC	OpenID Connect, Zero Trust [63]	Manages access based on dynamic relationships between entities, ideal for social or collaborative environments.
EnBAC	Zero Trust, OAuth 2.0 [74]	Evaluates environmental factors (e.g., location, device) to allow or deny access.
RiskBAC	Zero Trust, ABAC-compatible protocols [75]	Dynamically adjusts access permissions based on calculated risk levels.
HBAC	Blockchain, Kerberos [76]	Tracks historical access and enforces decisions based on past activities.
E-BAC	Event-driven protocols (e.g., MQTT, AMQP)	Triggers access control decisions based on system events or real-time conditions.
UCON	Zero Trust, OAuth 2.0 [77]	Combines traditional access control with ongoing usage monitoring for dynamic policy enforcement.
BBAC	Machine learning-enhanced Zero Trust [78]	Monitors behavior patterns and enforces access decisions based on detected anomalies or normal patterns.

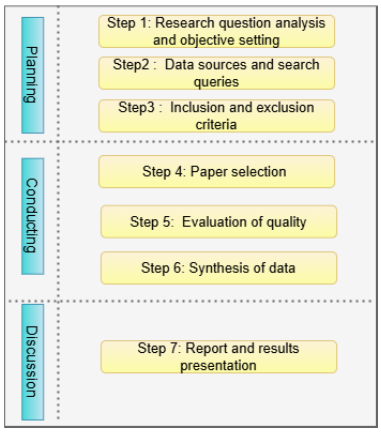

FIGURE 23. Phases and stages of SLR.

A. PLANING

This section outlines the tasks completed during the Planning phase of our SLR, detailing the activities involved in developing our review framework.

1) RESEARCH QUESTION ANALYSIS AND OBJECTIVE SETTING

The first step in conducting a SLR is identifying the study's need. This corresponds to Stage 1 of the SLR process, as shown in Fig. 23. In this case, the need was established by identifying gaps and emerging trends related to ACM regarding the security of data.

To address this need, clear Research Questions (RQs) must be formulated to guide the analysis of relevant studies. For this SLR on ACM, the RQs and their corresponding goals are outlined in Table. 4.

2) DATA SOURCES AND SEARCH QUERIES

As shown in Fig. 23, Step 2 of the systematic literature review (SLR) process focuses on selecting appropriate source databases and crafting effective search strings. This step is essential to ensure the review is both comprehensive and methodologically sound.

For this review, we selected two leading scientific databases: **Web of Science (WOS)** (https://www.

TABLE 4. Research questions (RQs).

	Research questions	Goals
RQ1	What are the applications and security techniques that address data security in the emerging access control studies?	The goal is to provide an overview of the emerging techniques and applications proposed for enhancing data security in AC systems.
RQ2	What are the trending AC requirements in data AC?	The aim is to review the requirements highlighted by recent research in AC and identify key requirements that should be addressed for future advancements in data security.
RQ3	What are the trends and gaps concerning AC data security?	The objective is to pinpoint emerging trends and identify current gaps in data AC.

(webofscience.com/) and **Scopus** (https://www.scopus.com). These databases were chosen for their extensive and reputable coverage in fields such as computer science, engineering, and related disciplines. Web of Science is known for its multidisciplinary research scope and citation tracking capabilities, while Scopus offers a broad and detailed collection of peer-reviewed literature. Together, their complementary strengths make them crucial resources for conducting a high-quality review.

The search strategy involved designing a search string aligned with the research objectives. The search terms were divided into two categories: Group 1, which included terms like "Access control", "Privacy", and "Security" and Group 2, which focused on terms like "Data" and "Database". As shown in Table. 5, these groups were combined using the logical operator "AND" to ensure that the results addressed both aspects. Within each group, terms were linked with "OR" to account for variations and synonyms, broadening the search and reducing the risk of missing relevant studies.

TABLE 5. General string to be adapted for the repository.

Group 1	Group 2
"Access control*"	"Information"
"Privacy"	"Data"
"Security"	"Database"

3) INCLUSION AND EXCLUSION CRITERIA

After the initial selection of studies from the database search, the next steps involve screening these studies and choosing those relevant for more detailed analysis. According to the SLR methodology, it is crucial to establish inclusion and exclusion criteria. The specific criteria used in this paper are outlined in Tables 6 and 7.

TABLE 6. Inclusion criteria.

IC	Inclusion criteria
IC1:	This study discusses emerging ACMs, data protection techniques, opportunities, or challenges.
IC2:	This study discusses AC and data protection requirements.

B. CONDUCTING

The following section includes additional details about how the protocol is applied. The following stages will be discussed: identifying research sources, selecting papers, evaluating quality, and extracting and synthesizing data.

TABLE 7. Exclusion criteria.

EC	Exclusion criteria
EC1: Year	Articles published after 2014.
*EC2:*Subject area	Limited to "Computer science" and "Engineering".
EC3: Document type	Limited to "Article" and "Conference paper".
EC4: Source type	Limited to "Journal" and "Conference proceeding".
EC5: Language	Limited to "English".
*EC6:*Open access	Limited to "Open access".

1) PAPER SELECTION

This step corresponds to Stage 4 of the SLR process, as illustrated in Fig. 23. To analyze and decide which studies to include, we extracted key information from the selected studies. In the results table, the following fields were included:

- Database, Author, Title, Year, Keywords, URL, Abstract, Publisher, and DOI

2) EVALUATION OF QUALITY

Stage 5 of the SLR process (Fig. 24) evaluates study quality, starting with 2,400 potential studies. Strict inclusion criteria reduced this to 307 articles, further refined to 222 unique entries using Machine Learning (ML) techniques and human review (Pandas Library and Scikit-Learn Preprocessing Module in Python). After assessing titles and abstracts for relevance to RQs, 162 articles were shortlisted. A detailed review excluded conceptual-only studies, resulting in 50 selected articles.

3) SYNTHESIS OF DATA

Following the selection of the 50 primary studies, Stage 6 of the SLR (Fig. 23) involves data extraction and progress monitoring. The information from these papers was organized into a data extraction table for the next steps in the process. The attributes included in this data extraction table are outlined below:

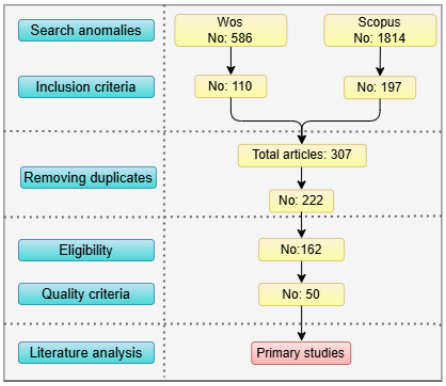

FIGURE 24. Methodology for the literature review.

- Paper title, Year, Basic ACMs, Summary of the paper, App domains, Access Control techniques, Access control requirements

The results of this step, which involves synthesizing data from the primary studies, will be described in detail in *Section* .

C. DISCUSSION

Finally, the last stage of the SLR is Stage 7 – report and results presentation. This stage involves preparing reports and presenting the results in a clear format. In this section, we outline the objectives of the RQs and highlight the gaps and requirements of various data ACMs. The results are presented in Section VI.

V. RESULTS

This section reviews various studies on ACMs tailored to different environments. Some models extend traditional frameworks, while others are adapted or newly developed to meet specific contextual needs. This highlights the ongoing need to refine ACMs in response to technological advancements. By combining new elements with existing models, these approaches contribute to more adaptable and comprehensive access control policies. A total of 50 relevant studies were analyzed, and their contributions, application domains, and techniques are summarized in Table. 11 in the Appendix.

VI. DISCUSSION

This section outlines the objectives of the RQs, identifies gaps in data ACMs, and conducts a quantitative analysis of key studies, focusing on publication trends, application domains, security techniques, and challenges to highlight current trends and future research directions.

A. DISTRIBUTION OVER THE YEARS

Fig. 25 presents a histogram showing the distribution of studies on access control models, with a clear upward trend from 2014 to 2020, peaking in 2020. A slight decline in 2021, potentially due to global events, is noted, but the overall trend has remained upward since then.

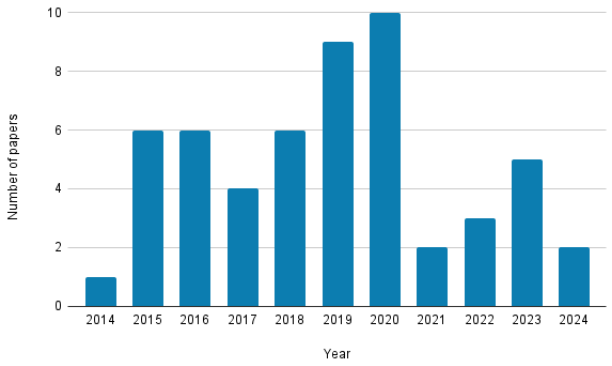

FIGURE 25. Distribution of works over the past 10 years considered in the review.

B. APPLICATION DOMAIN

Fig. 26 demonstrates the widespread concern AC across various application domains. Healthcare stands out as a primary focus (54%), reflecting the sensitive nature of patient data and the increasing reliance on technology in this sector. Other industries, such as education, social media, and government, also prioritize access control due to the handling of sensitive information. This underscores the universal need for robust ACM to protect data integrity and privacy across diverse fields.

Although healthcare dominates the attention, data security challenges in other sectors highlight the broader importance of this issue. Therefore, developing adaptable access control solutions is essential to meet the evolving needs of different industries.

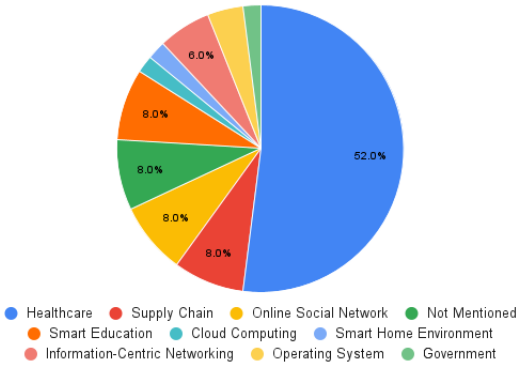

FIGURE 26. General application domain (The unlabeled pie slice represents 1%).

A summary of the classification of the application domain based on the analysis papers can be seen in Table 8.

C. ACCESS CONTROL MODELS: TECHNIQUES AND APPROACHES

In the modern digital era, safeguarding sensitive information is a priority. Organizations must implement effective privacy-preserving techniques to safeguard data while enabling its use for decision-making [130]. As part of this section,

TABLE 8. Application domain classification based on the analysis of the works.

Application domain	References
Healthcare	[84] , [85], [86], [87] , [88] , [89] , [90], [91] , [92] , [93] , [94] , [95], [96] , [97], [98] , [99] , [100] , [101] , [102] , [103] , [104], [105] , [106] , [107], [108] , [109] , [110] .
Supply chain	[111], [112], [113].
Online Social Network	[114], [115], [116], [117], [118].
Smart education	[119], [120], [121] .
Cloud computing	[122].
Smart home environment	[123] .
Information-centric network	[124], [125], [126].
Operating system	[127], [128] .
Government	[129].

TABLE 9. Techniques in access control models used in the works analyzed.

Application domain	References
Blockchain	- Smart contract: [85], [95], [96] , [101], [131]. - Hyperledger Fabric: [112], [89], [119], [94]. - Access levels: [87]
Encryption/Decryption	-Attribute-Based Encryption (ABE) : [88] -Cryptographic methods: [93] , [97] - Homomorphic Encryption(HE): [102] -signatures through Attribute-Based Signcryption (ABSC) : [98] -Proxy re-encryption: [101], [103]
Machine learning	-Support Vector Machine (SVM) : [116] -fuzzy Logic techniques: [90], [132] .
Anonymity	-k-anonymity: [120], [113] .
Access control language	-Hybrid Logic : [114] -Web Ontology Language(OWL): [123], [108] -eXtensible Access Control Markup Language(XACML) : [93], [94], [100], [121] . -OAuth 2.0: [94]
Zero trust	-Principle of least privilege: [107], [107] -Multi-Factor Authentication (MFA) : [86] -Access policy aggregation: [133] [110], [110].
Graph-based framework	-SQL query translation : [127] -Graph data structures : [118] -Topic models: [99].

we examine the various techniques used to implement ACM (Fig. 27).

A summary of the classification of the works based on the techniques in access control models can be seen in Table 9.

Based on our literature review, the privacy-preserving techniques used in review papers can be classified into the following categories:

- **Blockchain:** Blockchain technology improves ACM in fields like healthcare, big data, and IoT by offering a decentralized, secure, and tamper-proof system to protect sensitive data and prevent unauthorized access [134], [135], [136].
  Smart contracts, which automate and enforce access control policies, play a vital role in these systems. In healthcare, for example, smart contracts secure medical data access and monitor user behavior in IoT environments [85], [101]. *Hyperledger Fabric* provides a secure, decentralized method for managing permissions, with solutions like AccessChain [112] and MyBlockEHR [89] using blockchain to offer fine-grained control in business contracts and healthcare. Additionally, integrating *access levels* through permission and consensus protocols enhances security and efficiency in managing sensitive data [87].
- **Encryption/Decryption:** Encryption is a vital component of AC, particularly for protecting sensitive data in outsourced environments like CC [137]. By ensuring that only users with the correct decryption keys can access data, encryption safeguards both security and privacy [138], [139]. Advanced techniques like *Attribute-Based Encryption (ABE)* link data access to user attributes, enabling fine-grained control, such as managing genomic data in Data Networking [88]. *Cryptographic methods* are widely used to secure EHRs in cloud systems [93], with approaches like *Homomorphic Encryption (HE)* allowing computations on encrypted data without decryption, further enhancing security [102]. Additionally, frameworks combining encryption with digital signatures, such as *digital signatures through Attribute-Based Signcryption (ABSC)*, enable fine-grained control by restricting data access to authorized individuals based on specific attributes [98].
- **Machine learning (ML):** ML techniques enhance access control systems by improving adaptability, accuracy, and efficiency. Unlike traditional models like RBAC and ABAC, ML algorithms automate decision-making, detect real-time anomalies, and bolster security measures [140]. For example, *Support Vector Machine (SVM)* classifies and predicts user behavior based on historical data, identifying anomalies to detect potential threats and unauthorized access [116]. In healthcare, *fuzzy Logic techniques* is applied to RBAC, enabling precise access decisions by assessing safety risks and evaluating risk factors [90]. These approaches adapt access control policies to different contexts, offering flexible and robust security solutions [132].
- **Anonymity:** Anonymity in AC is used to enhance privacy protection while maintaining data usability. The Role-task conditional-purpose policy model integrates anonymity techniques, such as *k-anonymity*, to ensure

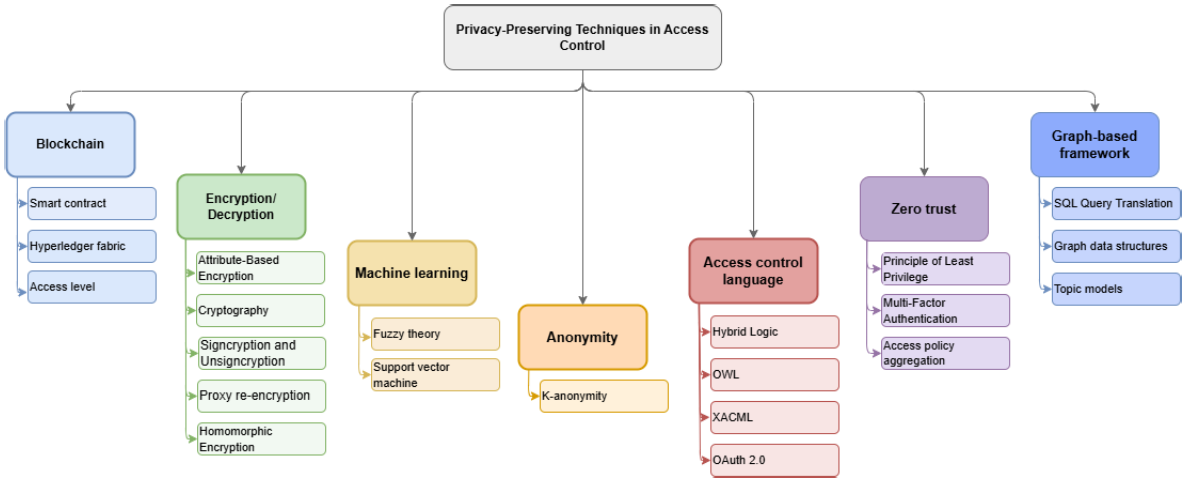

FIGURE 27. Privacy preservation techniques.

that data remains usable while protecting individual privacy. This model allows for flexible AC, where users can access anonymized data based on specific purposes and privacy levels, thus balancing data utility and privacy requirements [120]. Furthermore, the (k,n,m) anonymity approach enhances traditional k-anonymity by automating the selection of quasi-identifiers, allowing for tailored anonymity levels based on sensitivity and exposure [113].

- **Access control language:** Access control languages are crucial in defining and enforcing policies that determine who can access specific data and under what conditions. To enhance both security and flexibility, several advanced languages and frameworks have been developed [141].
  For example, *Hybrid Logic* enables the creation of complex, context-aware access control policies, allowing dynamic and fine-grained management that can adapt to changing requirements [114]. Similarly, *Web Ontology Language(OWL)* is used to represent semantically and reason about access control policies, simplifying the definition of relationships and rules across different systems [123]. Additionally, *eXtensible Access Control Markup Language(XACML)* is a widely-used standard for specifying access control policies in XML format, supporting fine-grained control by defining rules based on user, resource, and action attributes [93], [121].
  Complementing these, *OAuth 2.0* is an open-standard authorization framework that allows third-party applications to access resources on behalf of users without sharing credentials [94]. While OAuth focuses on delegated access (who can access what), XACML enforces detailed access rules (under what conditions access is granted or denied). Together, OAuth and XACML can work in tandem, with OAuth managing token issuance and XACML providing policy enforcement, enhancing both security and flexibility in access control systems.
- **Zero trust:** Zero Trust is a cybersecurity model emphasizing continuous verification and strict access controls, fundamentally shifting from traditional trust-based security paradigms. It operates on the principle of "never trust, always verify," ensuring that no user or device is inherently trusted, regardless of their location within or outside the network perimeter [115].
  In [107], the *principle of least privilege* is used to ensure that users have only the minimum necessary access to perform their tasks, thereby enhancing the security and privacy of EHRs. Additionally, the paper [86] *Multi-Factor Authentication (MFA)* enhances security by requiring multiple forms of verification before granting access to sensitive health data.
- **Graph-based framework:** Graph-based frameworks enhance AC by modeling relationships between users, data, and resources as a graph, enabling efficient policy enforcement, fine-grained control, and dynamic adaptability. The process involves modeling entities and their relationships, constructing graphs with nodes and edges, defining policies using query languages, evaluating access by traversing the graph, and maintaining updates to reflect organizational changes.
  In healthcare, graph-based models track user interactions and data access, ensuring accountability and compliance with privacy regulations [110]. For example, RuBAC frameworks use *SQL query translation* to optimize rule management and scalability, while ReBAC frameworks model user-resource relationships in real time, providing context-aware and adaptive access decisions [127]. Additionally, integrating graph-based frameworks with topic models enhances privacy-aware and risk-adaptive systems, particularly in managing sensitive health data securely [99].

D. EVALUATION OF PRIMARY ACCESS CONTROL REQUIREMENTS

Understanding AC requirements is crucial for developing effective security models in various domains. Table 10 presents a comparative analysis of the AC features addressed

TABLE 10. Comparison of the literature papers in terms of access control requirements.

Ref	Adaptability	Context-aware	Distributed	Dynamic	Fine-grained	Flexibility	Granularity	Interoperability	Light weight	Real time	Scalability	Usability
[84]	✓	✓	×	✓	×	✓	×	×	×	×	×	×
[85]	✓	×	✓	✓	×	×	×	×	×	×	×	×
[86]	✓	×	×	✓	✓	✓	×	✓	×	×	×	×
[111]	✓	✓	×	✓	✓	×	×	×	×	×	✓	×
[112]	✓	×	✓	✓	✓	✓	×	×	×	✓	×	×
[87]	✓	×	✓	✓	✓	✓	×	×	×	✓	×	×
[114]	×	✓	×	×	✓	✓	×	×	×	×	×	×
[115]	✓	✓	×	✓	✓	✓	×	×	×	✓	✓	×
[116]	×	✓	×	✓	✓	✓	×	×	✓	✓	×	×
[88]	×	×	✓	✓	✓	✓	×	×	×	×	×	×
[89]	×	×	✓	✓	✓	✓	×	×	×	✓	×	✓
[133]	×	×	✓	✓	×	×	×	×	×	✓	×	×
[90]	×	×	×	×	×	✓	×	✓	×	✓	×	×
[91]	✓	✓	×	×	✓	×	✓	×	×	×	×	×
[119]	×	×	✓	×	×	✓	×	×	×	✓	×	×
[122]	×	×	×	✓	✓	✓	×	×	✓	✓	×	✓
[123]	✓	✓	×	✓	×	✓	✓	×	×	✓	×	×
[132]	✓	×	×	✓	✓	✓	×	×	×	✓	×	×
[124]	×	×	✓	✓	✓	✓	×	×	×	×	×	×
[120]	×	✓	×	✓	✓	✓	×	×	×	✓	×	×
[125]	×	✓	×	✓	✓	✓	×	×	×	✓	×	×
[92]	×	✓	×	✓	✓	✓	×	×	×	✓	×	×
[93]	×	✓	×	✓	✓	✓	×	×	×	×	×	×
[126]	×	×	×	✓	✓	✓	×	×	×	✓	×	×
[94]	×	×	×	✓	✓	✓	×	×	×	×	×	×
[95]	×	×	✓	✓	✓	×	×	×	×	✓	×	×
[96]	×	×	✓	✓	✓	×	×	×	×	✓	×	×
[97]	×	×	✓	✓	✓	✓	×	×	×	✓	×	×
[117]	×	×	×	✓	✓	✓	×	×	×	×	×	×
[98]	×	×	×	✓	✓	✓	×	×	×	✓	×	×
[99]	✓	✓	×	✓	✓	✓	×	×	×	✓	×	×
[100]	×	×	×	✓	✓	✓	×	×	×	✓	×	×
[101]	×	×	✓	✓	✓	✓	×	×	×	×	×	×
[142]	×	×	×	✓	✓	✓	✓	×	×	×	×	×
[102]	×	×	×	✓	✓	✓	×	×	×	×	×	×
[131]	✓	✓	×	✓	×	×	×	×	✓	×	✓	×
[103]	×	✓	×	✓	×	✓	×	×	×	✓	×	×
[113]	×	✓	×	✓	✓	✓	×	×	×	×	×	×
[104]	×	×	✓	✓	×	×	×	×	×	✓	×	×
[127]	✓	×	×	×	✓	✓	×	×	×	✓	×	×
[128]	×	×	✓	×	×	×	×	×	×	×	×	×
[129]	✓	✓	×	✓	×	×	×	×	×	✓	✓	×
[121]	×	✓	×	✓	×	✓	×	×	×	✓	×	×
[105]	×	✓	×	✓	✓	✓	×	×	×	✓	×	×
[106]	✓	✓	×	×	✓	✓	✓	✓	×	✓	×	×
[107]	✓	✓	×	✓	✓	✓	✓	×	×	×	×	×
[118]	×	✓	×	✓	✓	✓	×	×	×	×	×	×
[108]	✓	✓	×	×	✓	✓	×	×	×	×	×	×
[109]	✓	✓	×	×	✓	✓	×	×	×	×	×	×
[110]	✓	✓	×	×	×	✓	×	×	×	×	×	×

End of Table

in the selected studies, using simple symbols (✓, ×) to indicate the presence or absence of each feature.

The AC requirements addressed in Table. 10 are defined as follows:

- **Adaptability:** "*Adaptability*" in access control refers to the dynamic adjustment of security measures based on contextual factors and user characteristics, such as profiles, preferences, habits, and health states [143]. This concept ensures personalized service delivery and a positive user experience in interconnected systems. It is particularly important in smart environments, where systems must accommodate evolving constraints and requirements while integrating multiple devices and services [131].

Adaptability enhances traditional static approaches, like role-based or policy-based access control, enabling dynamic and context-aware responses [143]. However, achieving adaptability presents challenges, including complex system design [144], performance overheads [145], privacy concerns [145], and the difficulty of maintaining consistent policies in large-scale environments [146]. Despite these hurdles, adaptability remains essential for effective service delivery and security in dynamic systems.

- **Context-awareness:** "*Context-aware*" systems dynamically adapt their behavior based on the user's current situation, activities, and environment [147], [148]. These systems utilize contextual information, such as location, time, and activity, to deliver relevant services tailored to the user's tasks and surroundings [6], [131], [143]. This adaptability enhances flexibility and precision in system functionality.
  In the realm of access control, context-aware models leverage real-time context data to assign permissions dynamically, ensuring secure and appropriate data sharing [145]. By continuously adjusting to changes in context, these models improve the granularity and responsiveness of access control mechanisms [143].
- **Distributed:** "*Distributed*" in the context of access control refers to the management and enforcement of access control policies across multiple, often geographically dispersed, systems or domains. This is particularly relevant in environments where data is shared across different organizations or locations, such as in CC, IoT, or cross-organizational collaborations [149].
  Distributed access control involves decentralized decision-making, allowing access control decisions to be made and enforced across different components of a system rather than at a central point. This approach can improve system performance and scalability, especially in environments with large numbers of users, devices, and data points.
- **Dynamic access control policies:** "*Dynamic access control policies*" use real-time contextual information–such as trust, risk, and operational needs–to determine access rights, moving beyond static, predefined rules [150], [151]. These models integrate past and future context, enabling flexible, context-aware decision-making that adapts to diverse environments like IoT systems [131].
  In e-health, dynamic access control is particularly valuable, as it adjusts to changing roles, contexts, and risks in real time. Factors like time, location, and user behavior are considered to ensure appropriate access, such as granting a doctor full access during emergencies but limited access in routine scenarios. These policies continuously assess risks, enforce rules during active sessions, and help prevent insider threats [152].
- **Fine-grained:** "*Fine-grained access control*" is critical for safeguarding sensitive data, such as EHR, by restricting access based on roles, responsibilities, and other attributes. This approach ensures that individuals can only access the specific information necessary for their functions, aligning with the principle of least privilege [153].
  Unlike traditional models like RBAC, which provide broad access based on roles, fine-grained control leverages ABAC to define access policies using detailed attributes and contextual factors. This allows for more precise and flexible access management, addressing complex scenarios and evolving organizational needs RBAC.
  Fine-grained access control is particularly significant in healthcare, CC, and virtual organizations, where secure and regulated data sharing is essential. By managing access at a granular level, it enhances security, supports compliance, and protects sensitive information [154].
- **Flexibility:** "*Flexibility*" in access control refers to the ability to dynamically adjust permissions for users and data in response to evolving needs, enabling responsive and adaptable access management [155]. This capability is particularly crucial for protecting EHR in the ever-changing healthcare environment [156].
  Flexible access control systems ensure appropriate access by adapting policies based on roles, collaborations, and data requirements [156]. Traditional rigid models often fall short in dynamic settings, while more adaptable approaches, such as DAC, RBAC, and ABAC, provide the necessary flexibility through dynamic, role-based, and attribute-driven decision-making [157].
- **Granularity:** "*Granularity*" in access control refers to the level of detail in defining access rules. Higher granularity allows for more specific and flexible control over permissions, aligning access policies with diverse information needs [158].
  For example, the UCON model offers high expressiveness and adaptability, enabling fine-grained access control policies that adjust dynamically to changing conditions. This approach enhances traditional methods by incorporating open and closed authorizations for precise control, such as managing XML-like documents [159].
  However, while increased granularity improves the enforcement of regulations and policies, it also introduces challenges, including higher implementation complexity and potential trade-offs between security benefits and costs [160].
- **Interoperability:** "Interoperability" in ACM is the capacity for diverse systems and platforms to share and manage data seamlessly. This is achieved by harmonizing user identities, translating security levels, and granting appropriate access to resources, facilitating collaboration across various environments. Data

interoperability provides comprehensive, contextual information that enhances data analysis and decision-making, particularly when organizations maintain distinct access control policies [161].

In CC, interoperability is especially critical, as ACM must transfer user credentials across various layers and address challenges from service heterogeneity and differing access policies. Effective interoperability thus strengthens security and usability, allowing access control systems to adapt to varied contexts and user requirements [162], [163]

- **Light weight:** In the context of ACM for data, "*lightweight*" refers to solutions designed to operate efficiently within the limited resources [131]. Lightweight access control in data management involves efficient and flexible mechanisms for protecting sensitive information while minimizing computational overhead. These models aim to ensure security and privacy while reducing resource demands, making them suitable for mobile cloud environments [157]. Lightweight access control often incorporates flexible and fine-grained mechanisms that enable privacy-aware data sharing, thereby lowering the costs associated with data re-encryption and decryption. Additionally, lightweight solutions are characterized by their ability to adapt dynamically to changing contexts, ensuring that access control policies remain effective without placing a heavy burden on constrained devices [6], [131].
- **Real-time:** In the context of access control, "*real-time*" refers to the immediate assessment of contextual features at the moment an access request is made. This allows for adaptive decision-making based on current conditions, especially in dynamic environments like edge computing and IoT, where user behavior and context can change rapidly. It involves evaluating factors such as user actions, resource sensitivity, action severity, and historical risk data to assess the security risk associated with each request [131], [164].

  Unlike traditional static models that rely on predefined policies, real-time access control models use these contextual inputs to provide flexible and context-sensitive access decisions. This enhances security in environments like the IoT [6], [164]. This approach ensures that access permissions can adapt to changing circumstances, improving the overall security posture of the system [131].
- **Scalability:** "*Scalability*" in data access control refers to a system's ability to efficiently handle increasing numbers of users, data, and access requests without compromising performance or security. Key features of scalable access control systems include their ability to efficiently manage large volumes of data and requests [131], [165], [166].

  For instance, Google's Zanzibar system exemplifies this capability, handling trillions of access control lists and processing millions of authorization requests per second [141]. Additionally, scalable systems are designed to maintain high performance even under heavy workloads. Another important aspect is consistent security enforcement; these systems can effectively manage complex access control policies, ensuring that all user actions follow a well-defined order.
- **Usability:** "*Usability*" in access control refers to how easily access control models can be managed, understood, and updated, ensuring that users and devices can interact with the system efficiently [131].

  Usability is particularly important in data access control, especially in sectors like healthcare [167]. Key aspects include user-friendliness, where the interface is easy to navigate with minimal learning required and efficiency, allowing users to perform tasks like logging in or managing permissions quickly and without unnecessary steps [164]. Additionally, the system should emphasize error prevention by guiding users to avoid mistakes and providing clear instructions for recovery when errors do occur [168], [169].

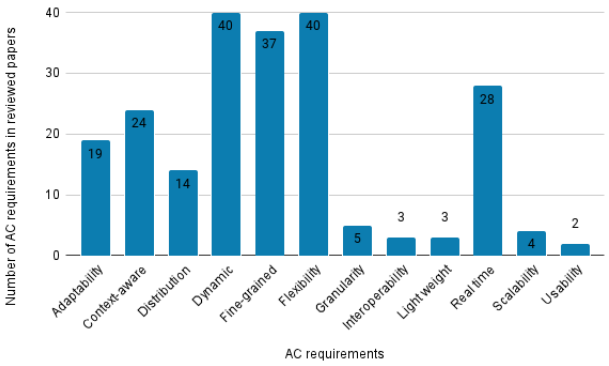

FIGURE 28. Frequency of AC requirements in reviewed studies.

Fig. 28 visualizes the frequency of AC requirements discussed in the reviewed papers (Table. 10). It appears that "Dynamic", "Flexibility", and "Fine-grained" are the most frequently discussed requirements, with many studies highlighting their importance. In the second tier, "Real-time", "Adaptability", and "Context-awareness" are the most demanding requirements. This suggests that researchers and practitioners are increasingly recognizing the need for access control systems that can adapt to changing environments, consider contextual factors, and offer detailed control over access permissions.

E. SUMMARY OF CHALLENGES AND DIRECTIONS FOR FUTURE WORK

Implementing an effective AC system involves a variety of challenges, from accurately identifying authorized individuals to ensuring seamless resource access. This section delves into each category, highlighting the complexities and obstacles that organizations face in securing their systems and data (Fig. 29).

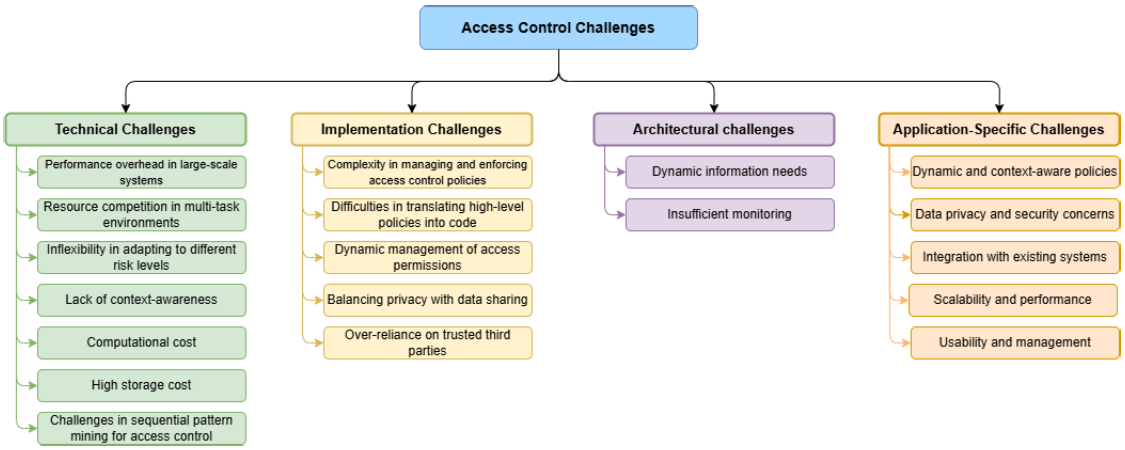

FIGURE 29. Access control challenges.

1) TECHNICAL CHALLENGES

- **Performance overhead in large-scale systems:** Performance overhead refers to the additional computational and resource burden that AC mechanisms impose as a system scales. This challenge arises from processing numerous access requests, evaluating complex policies, and managing extensive role-permission relationships. As users, roles, and access requests increase, more computational power and memory are needed. [92] addresses this issue by proposing dynamic segregation of duty to streamline role management, reducing overhead and improving system performance in critical healthcare scenarios.
- **Resource Competition in Multi-Task Environments:** Resource competition in multi-task environments occurs when multiple tasks require the same limited resources simultaneously, creating access control challenges. Spatial resource limitations can also lead to deadlocks and increased system overhead. The MT-RBAC model addresses these issues by incorporating spatio-temporal awareness in access decisions and dynamically adjusting roles based on task context, time, and location. This optimizes resource allocation, minimizes conflicts, and enhances system performance through predictive resource management [142].
- **Inflexibility in adapting to different risk levels:** Traditional models rely on pre-defined access requests, operating under the assumption that all potential needs can be anticipated. This strict adherence to pre-defined rules can impede emergency care, leading to critical data delays and increasing risks during emergencies. To address this, the proposed solution includes introducing a "situation control policy" and creating a "Special-Access-Zone" for emergencies. This approach enables controlled access during emergencies while maintaining security, ensuring that critical data can be accessed promptly when needed most [105].
- **Lack of context-awareness:** The lack of context awareness in AC systems can lead to several critical issues. First, it often results in overprivileged users and applications, as access rights are assigned without considering the specific context of the request, granting excessive capabilities. This can compromise security and privacy, as permissions are not dynamically adjusted based on factors like location, time, or user activity. Consequently, access control systems become static and inflexible, unable to adapt to changing conditions or enforce fine-grained policies. In healthcare, particularly in telehealthcare, the absence of context awareness hinders the development of personalized and adaptive care models, limiting their ability to meet individual patient needs effectively. [123].
- **Computational cost:** Computational cost in access control refers to the processing power and time required to execute mechanisms such as authentication, authorization, and policy evaluation, and it varies depending on factors like the complexity of the ACM, the number of policies, and the cryptographic algorithms involved. Sophisticated models with fine-grained controls generally require more processing power than simpler ones. Similarly, a large number of policies or complex policy logic increases the system's computational burden, as it must evaluate multiple conditions before making an access decision [98]. Systems that incorporate context awareness, which relies on real-time data such as location or user behavior, further increase computational costs due to the need for retrieving and processing this information [106]. With an increasing number of users and devices, especially in IoT environments, computational demands increase.
- **High storage cost:** Storage challenges in AC systems are significant, particularly due to data volume issues. The healthcare system contains large amounts of data, including images and test results, that are difficult to

manage. Additionally, blockchain technology requires storing all historical transactions, further complicating storage needs. To address these challenges, data storage optimization techniques are proposed, such as storing only metadata on the blockchain and using off-chain storage for the actual medical data [96].

- **Challenges in sequential pattern mining for access control:** Traditional sequential pattern mining struggles with the complexity of behavioral data in AC systems, which involve multiple elements like subject, action, resource, and context. These systems face challenges in handling complex relationships and the semantic meaning of behavioral items. Specialized algorithms and techniques, such as graph-based representations and semantic analysis [118], are being developed to address these issues.

2) IMPLEMENTATION CHALLENGES

- **Complexity in managing and enforcing access control policies:** Access control policy management faces several challenges, particularly in complex, dynamic, and privacy-sensitive environments like healthcare and CC [112], [123]. Dynamic environments require adaptable ACM that can respond to changing conditions and user behavior, while privacy concerns necessitate balancing data accessibility with privacy preservation. To address these challenges, solutions include adopting fine-grained access control models like ABAC for more flexible and context-aware decisions [118], incorporating context-aware and dynamic policies to adapt to changing situations [123], and leveraging blockchain technology for enhanced security, transparency, and decentralization [96]. Many proposed AC frameworks are conceptual and have not been implemented in real-world settings. This lack of practical implementation and validation makes it difficult to assess whether they meet the requirements for real-world deployment, such as scalability and performance.
- **Difficulties in translating high-level policies into code:** Translating high-level policies into code presents significant challenges, primarily due to the gap between abstraction and implementation. High-level policies often express security goals abstractly, making it difficult to translate them into concrete, enforceable code due to semantic differences and contextual dependencies. Traditional ACMs like RBAC are often too rigid and lack the expressiveness needed for fine-grained, context-aware policies. To address these challenges, more expressive models like ABAC and ReBAC are advocated, offering greater flexibility and granularity. To bridge this gap, formal policy languages can be a useful tool in providing structured, precise ways of expressing policies, helping to automate reasoning for consistency and conflict detection. Dynamic policy evaluation and context-aware enforcement are also emphasized, allowing systems to adapt to changing conditions in real time. Hybrid approaches, such as extending RBAC with context awareness or combining ABAC and ReBAC, are suggested to create more comprehensive and flexible AC solutions.
- **Dynamic management of access permissions:** Dynamic management of access permissions faces challenges in multi-task environments, where access permissions must adapt to varying tasks, resources, and user roles. Traditional models like RBAC struggle in these scenarios, prompting the development of enhanced models such as MT-RBAC, which incorporates spatio-temporal factors like time and location for more precise control [142]. In healthcare systems, managing access to sensitive EHRs requires balancing data availability with patient privacy. Advanced approaches like LW-C-CP-ARBE [108] and VBAC [122] offer fine-grained permissions, enabling dynamic and secure management of EHR data.
- **Balancing privacy with data sharing:** Balancing privacy with data sharing is a significant challenge in AC implementation across various sectors. In supply chains, the increasing complexity demands greater transparency and data sharing among stakeholders, which must be balanced with the need to protect sensitive business information. If data on a blockchain is not properly secured, it can jeopardize a company's competitive advantage and financial standing. Therefore, it is crucial to find a balance between data accessibility and privacy to ensure secure information exchange [112].
  In healthcare, the sensitivity of personal health information necessitates preventing its misuse or unauthorized disclosure. While sharing EHRs can enhance healthcare delivery, research, and AI-driven health analysis, it must be managed carefully to protect patient privacy [85]. Methods for preserving privacy while enabling data sharing include data desensitization, which involves removing or altering identifying information [90]. Additional methods such as anonymization and encryption help protect patient data [90]. Robust access control mechanisms also ensure that only authorized individuals can access specific information within EHRs [98], [170].
- **Over-reliance on trusted third parties:** Trust models often rely on third parties, which poses challenges for ensuring the security of trust data and accurately predicting trust levels. The challenges of EHR interoperability, focus on the risks of centralized approaches that rely on third-party cloud providers [161]. Concerns include potential data breaches, security vulnerabilities, and the susceptibility of centralized systems to attacks, performance issues, and single points of failure. Similarly, in Information-Centric Networking (ICN), centralized access control schemes, while effective in managing content access, pose risks by depending on a central authority or third party, creating a single point of failure if compromised [124].

3) ARCHITECTURAL CHALLENGES

- **Dynamic information needs:** Traditional AC systems often struggle to meet the evolving needs of medical professionals, leading to delays in accessing critical information. There is a particular difficulty in using static access control models for EHR systems in hybrid cloud environments. To address this, a ''dynamic access-control policy'' transformation approach enables real-time adjustments to access policies during data transfers between private and public clouds, thereby accommodating diverse user privileges [104]. Additionally, a ''dynamic risk-adaptive access control model'' leverages topic models to assess the risks associated with user access behaviors, periodically updating risk scores and access thresholds. Together, these strategies underscore the necessity for adaptive access control mechanisms to effectively manage dynamic information needs while ensuring robust security in healthcare [93].
- **Insufficient monitoring:** In healthcare systems, simply preventing unauthorized access is insufficient. Effective data governance requires monitoring how information is accessed and used. This involves tracking data access and utilization to ensure appropriate use, not just whether access is granted [85].

  A significant challenge is the insufficient monitoring of data access and usage. ACMs must evolve beyond static policies to adapt to user behavior, necessitating continuous monitoring for effective adaptations. One approach is "Information Accountability" which implements transparent audit processes to log all transactions, creating a comprehensive record for analyzing information usage [93].

  Additionally, a dynamic risk-adaptive access control model quantifies the risk associated with user access requests and adjusts permissions accordingly. By continuously monitoring user behavior and updating risk scores, this model enhances the system's ability to detect and respond to potential threats, emphasizing the need for robust monitoring mechanisms in managing data security effectively [99].

4) APPLICATION-SPECIFIC CHALLENGES

- **Dynamic and context-aware policies:** Many sources highlight the need for adaptive access control policies that account for changing situations, user contexts, and environmental factors. Traditional models like RBAC often struggle to address the dynamic nature of modern applications. For instance, in healthcare, emergencies may require bypassing access control rules ("break the glass") [142], while in supply chains, access requirements can change as products move through various stages and involve different stakeholders [122]. To meet these challenges, developing context-aware models like ABAC is essential. These models consider factors such as user roles, locations, device types, and the purpose of access to enable more flexible and informed access decisions [85], [90], [105].
- **Data Privacy and Security Concerns:** Protecting sensitive data is critical in applications handling personal or confidential information. In healthcare, there is a constant challenge to balance patient privacy with the need for data accessibility to support effective treatment and research [112]. Similarly, supply chain applications must safeguard business-sensitive data while enabling efficient collaboration among stakeholders [112]. Online social networks also present significant risks, as users often share personal information without fully understanding the potential privacy implications [120]. Addressing these challenges requires robust access control policies, secure storage mechanisms, and the use of privacy-enhancing technologies such as encryption, anonymization, and blockchain to prevent unauthorized access and ensure data protection [88], [93], [108].
- **Integration with existing systems:** Integrating new access control models into existing IT infrastructure presents significant challenges [90]. In healthcare, organizations often operate with complex and heterogeneous systems, making it difficult to enforce consistent access control policies across various platforms [104]. Similarly, supply chain systems frequently involve legacy systems and diverse technologies, requiring considerable effort to adapt and integrate new access control mechanisms [112]. Legacy access control systems, in particular, often lack the flexibility and granularity needed for modern applications, necessitating either extensive modifications or the creation of entirely new systems to meet current demands [90].
- **Scalability and performance:** As data volumes increase and applications grow more complex, ensuring the scalability and performance of access control mechanisms becomes essential. Blockchain-based solutions provide benefits such as decentralization and tamper-proof data management but face scalability challenges, especially when handling large-scale transactions [97], [101]. Similarly, complex access control policies, such as those based on attributes or relationships, can introduce significant computational overhead, affecting application performance. To address these issues, optimizing access control algorithms, utilizing efficient data structures, and implementing techniques like sharding in blockchain systems can improve scalability and enhance overall performance [112].
- **Usability and management:** Designing user-friendly and manageable access control systems is crucial for successful implementation, as complex policies often lead to misconfigurations and security risks. In applications like healthcare and supply chains, poor usability can cause errors, such as excessive access rights, compromising security and efficiency [118]. Manageable systems with intuitive tools are essential for

TABLE 11. Summary of references considered.

Ref	Basic ACM	Domain	Techniques	Summary
[84] 2024	RiskBAC	Healthcare (EHR)	Not Mentioned	Introduces a three-dimensional framework comprising risk and utility factors, data access scenarios, and roles and Evaluating against use cases and 25 criteria.
[85] 2024	RiskBAC	Healthcare (EHR)	Blockchain (Smart Contracts)	Evaluates access requests based on the current and past behavior, denying access. The model achieves an accuracy exceeding 90% in distinguishing between honest and malicious doctors.
[86] 2023	RBAC	Healthcare (EHR)	MFA	A system integrating a trust-based mechanism, dynamically evaluates user trust based on behavior. This approach has led to an 80% improvement in security and a 40.38% reduction in unauthorized activities.
[111] 2023	ABAC, TBAC, RBAC	Supply Chain	Zero Trust	Presents a zero-trust ACM for rail transit data platforms, continuously assessing trust in real-time based on dynamic user behavior and system interactions.
[112] 2023	ABAC	Supply Chain	Blockchain (Hyperledger fabric)	Combines ABAC with a multi-ledger blockchain to enhance trust and transparency, reducing the risks of unauthorized access and breaches. It supports a high throughput of 42 transactions per second (tps) in large-scale environments.
[87] 2023	ABAC	Healthcare	Blockchain (Access level)	Uses blockchain to improve data management and security. It features a permission-level system and a state machine to ensure transparency in access control, granting access only to authorized personnel. The system creates new hashes in 32.5 microseconds, boosting security.
[114] 2023	ABAC, ReBAC	OSN	Hybrid Logic	Introduces a new ARBAC model tailored for OSN. Unlike traditional methods like RBAC, which are not well-suited for the complex relationships and data-sharing practices in OSNs, this model offers more flexible and context-aware access control.
[115] 2022	RBAC, ABAC, TBAC	Transport System	Zero Trust	Enhances security for rail transit data platforms by continuously evaluating trust and dynamically adjusting permissions.
[116] 2022	Multiparty AC	OSN	ML (SVM)	Addresses privacy, and security issues in multi-user data transmission with the NA3P framework, which uses machine learning to enhance security and predict access control policies for shared content.
[88] 2022	ABAC	Healthcare	Encryption and Decryption	Investigate an ABAC for genomics data. This work builds on top of a Named Data Networking (NDN) and explores how attribute ebased encryption can be used to provide access control.
[89] 2021	Trust-BAC	Healthcare (EHR)	Blockchain (Hyperledger fabric)	The proposed framework combines on-chain and off-chain storage to enhance performance and ensure valid data retrieval. This approach reduces response times significantly, with a 50% decrease in response time for test cases involving large amounts of data compared to storing all data on-chain.
[133] 2021	RuBAC	Not Mentioned	Access Policies Aggregation	Introduces a semantics framework based on condition minterms to evaluate and compare the expressiveness of RuBAC. This approach aids security practitioners in making informed decisions regarding the selection, balancing expressiveness and complexity.
[90] 2020	RiskBAC	Healthcare	Decentralized Identifiers, Fuzzy Theory	uses RiskBAC with fuzzy logic to assess privacy leakage risks. The results demonstrate that the model effectively evaluates safety risks and predicts various risk factors, achieving a prediction accuracy of over 90%.
[91] 2020	Not Mentioned	Healthcare (PHR)	Privacy Rating (PR)	Enhances privacy and security in cloud-based healthcare systems by addressing concerns about sensitive patient data on third-party servers. For instance, if a user's PR value (6.7) is higher than the data's PR value (3.2), the system grants access to only a limited portion of the data.
[119] 2020	ABAC	Smart Education	Blockchain (Hyperledger fabric)	Propose a framework for secure cross-organization identity management that integrates Self-Sovereign Identity principles with blockchain. A prototype processed 55,000 access control requests per second with 3-second latency.
[122] 2020	ABAC,RBAC	CC	Encryption	Reduces costs for mobile users and ensures minimal overhead for devices while allowing secure policy sharing for data updates. Scheme improves decryption efficiency on the mobile client side, as even with 64 attributes, the decryption time remains under 1.5 seconds.
[123] 2020	ABAC	Smart Home Environment	OWL	Proposes the PALS system, which enhances ABAC. The system makes dynamic access decisions and includes an intrusion detection subsystem for smart home systems.
[132] 2020	RiskBAC	Not Mentioned	Fuzzy theory	Proposes using fuzzy inference to build flexible RBAC to provide solutions to challenges such as mitigating damage from malicious users and addressing scalability concerns. For example, processing 1,600 requests took 14.37 seconds, while 3,200 requests took 29.5 seconds.
[124] 2020	Not Mentioned	ICN	Blockchain	Introduces a matching-based access control model for hierarchical access and a blockchain-based access token mechanism. The longest process time is under 0.4 ms for 200 sub-types of user attributes, which exceeds practical requirements.

TABLE 11. *(Continued.)* **Summary of references considered.**

Ref	Basic ACM	Domain	Techniques	Summary
[120] 2020	Not Mentioned	Smart Education	k-Anonymity	Proposes a dynamic, semantic-aware access control model that combines purpose-based access control with k-anonymity to protect personal information in cyber-physical systems.
[125] 2020	Not Mentioned	ICN	Anomaly detection mechanisms	The proposed dynamic model protects privacy in multi-datacenter environments using a semantic dynamic authorization strategy based on anomaly assessments of user behavior. The DSAAC algorithm achieves about 93% accuracy.
[92] 2019	RBAC	Healthcare (EHR)	Encryption and Decryption	Combines RBAC and ABE to enhance the privacy and security of EHRs in the cloud, providing secure access through multiple encryption and verification layers. It improves PHR efficiency by 34.79% in encryption, decryption.
[93] 2019	ABAC, ReBAC	Healthcare (EHR)	Cryptography, XACML	Combines relationship and ABAC and integrates advanced cryptographic techniques to enhance key management, allowing more granular control over data access while maintaining user privacy.
[126] 2019	RBAC	ICN	Encryption and Decryption	Presents a system for managing access control and data privacy using cryptographic keys within a hierarchical structure.
[94] 2019	RuBAC	Healthcare	Blockchain(Hyperledger Fabric), XACML	Proposes an access control framework extending XACML for General Data Protection Regulation (GDPR) compliance, using a semantic model to manage user consent.
[95] 2019	RBAC	Healthcare (EMR)	Blockchain (Smart contract)	Proposes a blockchain-based scheme for access control in Electronic Medical Records (EMRs) to address user privacy leakage. It utilizes RBAC and information entropy technology to enhance data utilization and security.
[96] 2019	Not Mentioned	Healthcare (EHR)	Blockchain (Smart Contract)	Enhances privacy and security of large-scale health data using blockchain and encryption, ensuring transparency, and fine-grained access control. It is scalable for health data, with encryption and decryption times of 0.4 ms for IoT data and 0.2 ms for diagnoses.
[97] 2019	RBAC	Healthcare (EMR)	Blockchain, Cryptography	The blockchain-based access control scheme for EMRs enhances data sharing, security, and privacy by preventing tampering. The block creation time of 8 minutes is considered acceptable for PHR access.
[117] 2019	ReBAC	OSN	Graph based representation	Argues that ReBAC has broader applications in OSNs and personalized healthcare, emphasizing the need for models that capture complex relationships. It also addresses challenges in formalizing REBAC models and resolving conflicts in access control policies.
[98] 2018	ABAC	Healthcare(EHR)	Signcryption and Unsigncryption	Uses attribute-based encryption and cuckoo filters to enhance privacy and security in EHR systems while minimizing communication and computation costs.
[99] 2018	RiskBAC	Healthcare	Topic Models	The proposed RAdAC for health information systems uses topic models and dynamic risk-based access permissions, achieving an F1 score of 79%.
[100] 2018	ABAC	Healthcare	XACML, Encryption	Proposes a secure cloud-based EHR system using ABAC with XACML, partial encryption, and electronic signatures to efficiently transmit necessary data to authorized requesters.
[101] 2018	Not mentioned	Healthcare(EHR)	Blockchain(smart contract), Proxy re-encryption	a blockchain-based framework for secure, interoperable access to EHRs, balancing privacy and accessibility using smart contracts and cryptographic techniques.
[142] 2018	RBAC	Not mentioned	Spatio-temporal Correlation	MT-RBAC enhances traditional RBAC by adding spatio-temporal constraints and resource control to prevent task failures, particularly in high spatio-temporal correlation applications like aerospace.
[102] 2017	ABAC	Healthcare	HE	Enables privacy-preserving data processing with encrypted data computations and flexible access control.
[131] 2017	RiskBAC	Not mentioned	Blockchain (Smart contracts)	Enhances IoT device security by using real-time risk assessment and adaptive features to monitor user behavior and adjust access permissions.
[103] 2017	RBAC, MAC	Healthcare(EHR)	Proxy re-encryption searchable encryption	combines RBAC and MAC with a "break-the-glass" feature, using a Special-Access-Zone and situation control policy to enable secure, justified access to sensitive healthcare data during emergencies.
[113] 2017	RBAC , TBAC	Supply chain	k-anonymity	Integrates access controls and anonymization to safeguard data from insider threats and ensure protection during publication.
[104] 2016	RBAC	Healthcare(EHR)	Encryption	Proposes a ACM for secure and privacy-preserving data sharing in EHR systems across hybrid clouds. It addresses security and privacy issues by transforming access-control policies between private and public clouds.
[127] 2016	RuBAC, ABAC	Operating System	SQL Query Translation	Evaluates a RuBAC that dynamically translates access rules into SQL queries. It uses heuristics to minimize database workload induced by access control checks, aiming to improve performance and efficiency.
[128] 2016	RBAC	Operating System	Obligations Integration	Introduces ARBAC through administrative obligations, which is essential for cloud and mobile applications in organizations.

TABLE 11. *(Continued.)* **Summary of references considered.**

Ref	Basic ACM	Domain	Techniques	Summary
[129] 2016	MAC,ABAC	Government	Not Mentioned	Presents a RiskBAC address security challenges from the growing number of interconnected IoT devices. This model dynamically assesses the risk of each access request in real-time, considering factors like user context and resource sensitivity.
[121] 2016	RBAC,OrBAC,TBAC	Smart Education	Multi-agent systems, XACML	Presents the Trust-ORBAC Model, an AC framework for e-learning platforms that combines elements from OrBAC and dynamic RBAC to enhance security. It introduces a "trust level" layer and evaluates the model's effectiveness and limitations using the "MotOrbac" tool in practical scenarios.
[105] 2016	RBAC, MAC	Healthcare(EHR)	Multi-level data flow, Break-the-glass	Presents a security model for EHR systems that combines RBAC and MAC policies to enhance security and flexible emergency access through Special-Access-Zone. It also proposes centralized cloud storage to provide authorized users with anytime access to comprehensive medical histories, addressing issues of siloed data.
[106] 2015	RBAC	Healthcare, Smart Education	Ontology-Based	Introduces a framework that enhances access management for software services by considering user intentions and situational context, addressing the limitations of traditional models like RBAC and ABAC.
[107] 2015	VBAC	Healthcare(EHR)	Principle of Least Privilege	Presents a VBAC for EHR systems aimed at enhancing security and patient privacy. It introduces "views" that enable patients to control which parts of their health information can be accessed by different users, allowing for more granular access management.
[118] 2015	ReBAC	OSN, Healthcare	Graph data structures	Focuses on addressing the complexities of ReBAC in OSN by emphasizing the limitations of traditional ACMs. It introduces a formal ReBAC framework to better capture the relationship dynamics, operations, and access privileges in OSN.
[108] 2015	Not mentioned	Healthcare	OWL	Presents an ontology-based access control model to enhance the security and privacy of healthcare systems in CC. It leverages semantic web technologies to manage complex and distributed data efficiently.
[109] 2015	Not mentioned	Healthcare	Not Mentioned	Introduces a model that enhances flexibility by considering relationships between users, resources, and entities, overcoming the limgdpritations of traditional access control models like RBAC and ABAC.
[110] 2014	Not mentioned	Healthcare	Access policies aggregation	Introduces a system that combines patient privacy preferences with healthcare professionals' information needs. It integrates accountability mechanisms to ensure responsible data use, allowing patients to set access policies and track patients, and healthcare professionals' actions.

consistent policy enforcement in dynamic environments [104], [132].

VII. LIMITATIONS

The exclusion criteria applied during this literature review may have overlooked some important publications. This is partly due to the significant variability in keywords generated within the context of data access control and its associated applications. Nevertheless, the number of works analyzed and their distribution over a decade provides a representative sample of the research conducted. To mitigate this limitation, two important databases were included.

Additionally, it is important to note that articles not published in English were excluded, which may have resulted in some relevant works being omitted from the analysis.

Several sections of the review analyze empirical evidence found in the literature, such as technological enablers, application contexts, and the categorization of traditional access control methods and their requirements. These sections offer a comprehensive overview of the field, highlighting core representative elements and clusters. Future work should focus on developing a conceptual framework that addresses specific challenges, limitations, and requirements of access control that have not been widely considered.

Lastly, given the rapid evolution of this research area, particularly concerning technological enablers and access control models, it is likely that the findings presented in this work may change over time.

VIII. CONCLUSION AND FUTURE WORK

ACMs are essential for securing data across various applications, especially as digital environments become increasingly complex and interconnected. In the first part of this study, we reviewed conventional ACMs, highlighting their strengths and limitations. These traditional models are widely adopted due to their simplicity and ease of management but face limitations in modern applications such as CC and the IoTs.

Emerging ACMs offer more adaptive and granular approaches, yet they introduce new challenges, including higher complexity and increased resource demands. Our SLR, which included 50 selected studies, identified recurring requirements for ACMs, such as adaptability, context awareness, and real-time responsiveness. The study also reveals significant challenges, including cross-domain compatibility, effective privacy management, and the integration of ML to support real-time decision-making. These factors are critical as organizations strive to enhance security processes without compromising data protection.

Additionally, our review discusses emerging techniques and technologies supporting ACMs development, with ML, blockchain, and graph-based frameworks being some of the most influential.

The findings suggest a need for a unified ACM framework that combines the strengths of both traditional and emerging models to achieve robustness and flexibility. Future research should focus on developing models that balance complexity

with usability while addressing key challenges such as interoperability, automated policy enforcement, and privacy-aware access mechanisms. A key gap in current research is the lack of actionable implementation guidelines for ACM. Research should aim to provide detailed frameworks, best practices, and practical tools to help practitioners overcome challenges in system integration and access policy management.

Another area needing attention is the limited empirical validation of ACMs in diverse contexts. Future work should deploy and evaluate these models in real-world settings such as healthcare, finance, and industrial control systems to assess their performance and security under varying conditions. Additionally, current studies often neglect the usability and human factors of ACMs. Research should explore ways to design models that are secure, user-friendly, and efficient, focusing on aspects like cognitive load, error prevention, and user acceptance.

Finally, the lack of standardized evaluation metrics is another challenge. Future research should prioritize developing metrics that evaluate security, performance, usability, and cost. Standardizing these metrics will allow for better comparisons of ACMs and help practitioners make informed decisions.

This review serves as a resource for academics and industry practitioners by clarifying the current ACM landscape and highlighting areas for further exploration. Addressing the identified gaps and challenges will foster the development of more effective, resilient, and adaptable ACMs, strengthening data security and integrity in dynamic and distributed digital systems.

APPENDIX

Table 11 presents a summary of the work obtained from the systematic review of the literature.

ACKNOWLEDGMENT

The icons used in certain figures were provided by (www.flaticon.com) and made by Freepik, ioKanda, Creative_Captain, dreaming, and bukeicon.

REFERENCES

[1] C. Kar Yee and M. F. Zolkipli, "Review on confidentiality, integrity and availability in information security," *J. ICT Educ.*, vol. 8, no. 2, pp. 34–42, Jul. 2021.
[2] Adolfo S. Coronado, *Computer Security: Principles and Practice*. Indiana Univ., Purdue Univ. Fort, 2013.
[3] E. de Chazal. (2024). *Biggest Gdpr Fines of 2024*. [Online]. Available: https://www.skillcast.com/blog/biggest-gdpr-fines-2024
[4] B. S. Radhika, N. Kumar, and R. K. Shyamasundar, "Samyukta: A unified access control model using roles, labels, and attributes," in *Proc. Int. Conf. Inf. Syst. Secur.* Cham, Switzerland: Springer, Jan. 2022, pp. 84–102.
[5] F. Rezaeibagha, K. T. Win, and W. Susilo, "A systematic literature review on security and privacy of electronic health record systems: Technical perspectives," *Health Inf. Manage. J.*, vol. 44, no. 3, pp. 23–38, Oct. 2015.
[6] A. K. Malik, N. Emmanuel, S. Zafar, H. A. Khattak, B. Raza, S. Khan, A. H. Al-Bayatti, M. O. Alassafi, A. S. Alfakeeh, and M. A. Alqarni, "From conventional to state-of-the-art IoT access control models," *Electronics*, vol. 9, no. 10, p. 1693, Oct. 2020.
[7] M. U. Aftab, A. Hamza, A. Oluwasanmi, X. Nie, M. S. Sarfraz, D. Shehzad, Z. Qin, and A. Rafiq, "Traditional and hybrid access control models: A detailed survey," *Secur. Commun. Netw.*, vol. 2022, pp. 1–12, Feb. 2022.
[8] A. K. Y. S. Mohamed, D. Auer, D. Hofer, and J. Küng, "A systematic literature review of authorization and access control requirements and current state of the art for different database models," *Int. J. Web Inf. Syst.*, vol. 20, no. 1, pp. 1–23, Feb. 2024.
[9] L. Golightly, P. Modesti, R. Garcia, and V. Chang, "Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN," *Cyber Secur. Appl.*, vol. 1, Dec. 2023, Art. no. 100015.
[10] S. Kavianpour, B. Shanmugam, S. Azam, M. Zamani, G. N. Samy, and F. De Boer, "A systematic literature review of authentication in Internet of Things for heterogeneous devices," *J. Comput. Netw. Commun.*, vol. 2019, pp. 1–14, Aug. 2019.
[11] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, "Access control in the Internet of Things: Big challenges and new opportunities," *Comput. Netw.*, vol. 112, pp. 237–262, Jan. 2017.
[12] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering—A systematic literature review," *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, Jan. 2009.
[13] S. Parkinson and S. Khan, "A survey on empirical security analysis of access-control systems: A real-world perspective," *ACM Comput. Surveys*, vol. 55, no. 6, pp. 1–28, Jul. 2023.
[14] C. D. P. K. Ramli, "Modelling and analysing access control policies in xacml 3.0," Tech. Univ. Denmark, Tech. Rep. 364, 2015.
[15] R. Ferrari, "Writing narrative style literature reviews," *Med. Writing*, vol. 24, no. 4, pp. 230–235, Dec. 2015.
[16] J. Sukhera, "Narrative reviews: Flexible, rigorous, and practical," *J. Graduate Med. Educ.*, vol. 14, no. 4, pp. 414–417, Aug. 2022.
[17] *Trusted Computer System Evaluation Criteria (tcsec)*, Dept. Defence, New Delhi, India, 1985.
[18] N. Kashmar, M. Adda, and M. Atieh, "From access control models to access control metamodels: A survey," in *Proc. Future Inf. Commun. Conf. (FICC)*, vol. 2. Cham, Switzerland: Springer, Feb. 2019, pp. 892–911.
[19] M. Petkovic and W. Jonker, *Security Privacy and Trust in Modern Data Management*. Cham, Switzerland: Springer, 2007.
[20] J. Barkley, "Comparing simple role based access control models and access control lists," in *Proc. 2nd ACM Workshop Role-Based Access Control*, 1997, pp. 127–132.
[21] Y. Liang, "Study on view-based security model for database," in *Proc. Sun Yatsen Univ. Forum*, vol. 3, 2005, pp. 134–137.
[22] E. Bertino and R. Sandhu, "Database security-concepts, approaches, and challenges," *IEEE Trans. Dependable Secure Comput.*, vol. 2, no. 1, pp. 2–19, Jan. 2005.
[23] D. Bell and L. La Padula, "Secure computer system: Unified exposition and multics interpretation," MITRE Corp., Bedford, MA, USA, Tech. Rep. ESD-TR-75-306, 1976.
[24] M. Benantar, *Access Control Systems: Security, Identity Management and Trust Models*. Cham, Switzerland: Springer, 2005.
[25] R. Tomasic, "Chinese walls, legal principle and commercial reality in multi-service professional firms," *UNSWLJ*, vol. 14, p. 46, Jan. 1991.
[26] J. Cruz. (2016). *Rule-set-based Access Control*. [Online]. Available: https://www.linkedin.com/pulse/rule-set-based-access-control-jos
[27] R. Sandhu, V. Bhamidipati, and Q. Munawer, "The ARBAC97 model for role-based administration of roles," *ACM Trans. Inf. Syst. Secur.*, vol. 2, no. 1, pp. 105–135, Feb. 1999.
[28] A. A. E. Kalam, R. E. Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miège, C. Saurel, and G. Trouessin, "Organization based access control," in *Proc. IEEE 4th Int. Workshop Policies Distrib. Syst. Netw.*, Mar. 2004, pp. 120–131.
[29] R. K. Thomas, "Team-based access control (TMAC): A primitive for applying role-based access controls in collaborative environments," in *Proc. 2nd ACM Workshop Role-Based Access Control (RBAC)*, 1997, pp. 13–19.
[30] A. Tapiador, D. Carrera, and J. Salvachúa, "Tie-RBAC: An application of RBAC to social networks," 2012, *arXiv:1205.5720*.
[31] J. Dong, H. Zhu, C. Song, Q. Li, and R. Xiao, "Task-oriented multilevel cooperative access control scheme for environment with virtualization and IoT," *Wireless Commun. Mobile Comput.*, vol. 2018, no. 1, Jan. 2018, Art. no. 5938152.

[32] Y. Cheng, J.-H. Park, and R. Sandhu, "A user-to-user relationship-based access control model for online social networks," in *Proc. IFIP Annu. Conf. Data Appl. Secur. Privacy*, Paris, France. Cham, Switzerland: Springer, Jan. 2012, pp. 8–24.

[33] S. A. Afonin and A. Bonushkina, "Validation of safety-like properties for entity-based access control policies," in *Proc. Adv. Soft Hard Comput.* Cham, Switzerland: Springer, Dec. 2018, pp. 259–271.

[34] R. Aluvalu, K. K. Chennam, M. A. Jabbar, and S. S. Ahamed, "Risk aware access control model for trust based collaborative organizations in cloud," *Int. J. Eng. Technol.*, vol. 7, no. 4, pp. 49–52, Sep. 2018.

[35] H. F. Atlam, R. J. Walters, G. B. Wills, and J. Daniel, "Fuzzy logic with expert judgment to implement an adaptive risk-based access control model for IoT," *Mobile Netw. Appl.*, vol. 26, no. 6, pp. 2545–2557, Dec. 2021.

[36] P. Ghadekar, M. Ranjan Pradhan, D. Swain, and B. Acharya, "EmoSecure: Enhancing smart home security with FisherFace emotion recognition and biometric access control," *IEEE Access*, vol. 12, pp. 93133–93144, 2024.

[37] A. Hariri, A. Ibrahim, B. Alangot, S. Bandopadhyay, A. L. Marra, A. Rosetti, H. Joumaa, and T. Dimitrakos, "Ucon+: Comprehensive model, architecture and implementation for usage control and continuous authorization," in *Collaborative Approaches for Cyber Security in Cyber-Physical Systems*. Cham, Switzerland: Springer, 2023, pp. 209–226.

[38] X. Zhang, "Dynamic access control model based on user access behavior in the Internet of Things environment," in *Proc. 4th Int. Conf. Frontiers Technol. Inf. Comput. (ICFTIC)*, Dec. 2022, pp. 1020–1023.

[39] D. H. Freed, "Creating a table of authorization to empower staff," *J. Healthcare Financial Manage. Assoc.*, vol. 51, no. 11, pp. 4–33, Nov. 1997.

[40] T. Burchardt and R. Hick, "Inequality, advantage and the capability approach," *J. Hum. Develop. Capabilities*, vol. 19, no. 1, pp. 38–52, Jan. 2018.

[41] P. Tsankov, S. Marinovic, M. T. Dashti, and D. Basin, "Decentralized composite access control," in *Proc. Int. Conf. Princ. Secur. Trust*, Grenoble, France. Cham, Switzerland: Springer, Jan. 2014, pp. 245–264.

[42] J. Lina, Y. Fanga, B. Chena, and P. Wua, "A institute of remote sensing and geographic information system," Peking Univ. Beijing, Beijing, China, 2008.

[43] R. El Sibai, N. Gemayel, J. Bou Abdo, and J. Demerjian, "A survey on access control mechanisms for cloud computing," *Trans. Emerg. Telecommun. Technol.*, vol. 31, no. 2, p. 3720, Feb. 2020.

[44] S. D. C. De Vimercati, "Access control policies, models, and mechanisms," in *Proc. Int. School Found. Secur. Anal. Design*. Cham, Switzerland: Springer, Jan. 2000, pp. 137–196.

[45] C. Bueger, T. Edmunds, and B. J. Ryan, "Maritime security: The uncharted politics of the global sea," *Int. Affairs*, vol. 95, no. 5, pp. 971–978, Sep. 2019.

[46] K. Srivastava and N. Shekokar, "Design of machine learning and rule based access control system with respect to adaptability and genuineness of the requester," *EAI Endorsed Trans. Pervasive Health Technol.*, vol. 6, no. 24, pp. 1–12, Sep. 2020.

[47] Z. Asaf, M. Asad, S. Ahmed, W. Rasheed, and T. Bashir, "Role based access control architectural design issues in large organizations," in *Proc. Int. Conf. Open Source Syst. Technol.*, Dec. 2014, pp. 197–205.

[48] R. S. Sandhu, "Role-based access control," in *Advances in Computers*, vol. 46. Amsterdam, The Netherlands: Elsevier, 1998, pp. 237–286.

[49] M. P. Singh, S. Sudharsan, and M. P. Vani, "ARBAC: Attribute-enabled role based access control model," in *Proc. Int. Conf. Secur. Privacy*, Jaipur, India. Cham, Switzerland: Springer, Jan. 2019, pp. 97–111.

[50] M. Gotaishi and S. Tsujii, "Organizational cryptography for access control," *Cryptol. ePrint Arch.*, vol. 2018, p. 1120, Jan. 2018.

[51] F. Abbasi, A. Mesbahi, J. M. Velni, and C. Li, "Team-based coverage control of moving sensor networks with uncertain measurements," in *Proc. Annu. Amer. Control Conf. (ACC)*, Jun. 2018, pp. 852–857.

[52] M. F. F. Khan and K. Sakamura, "Context-aware access control for clinical information systems," in *Proc. Int. Conf. Innov. Inf. Technol. (IIT)*, Mar. 2012, pp. 123–128.

[53] R. Basnet, "Integration of task-attribute based access control model for mobile workflow authorization and management," Master's thesis, Dept. Comput. Sci., Colorado State Univ., Fort Collins, CO, USA, 2019.

[54] T. Bui, S. D. Stoller, and H. Le, "Efficient and extensible policy mining for relationship-based access control," in *Proc. 24th ACM Symp. Access Control Models Technol.*, May 2019, pp. 161–172.

[55] B. Zhao, G. Zheng, Y. Gao, and Y. Zhao, "Access-control model of super business system based on business entity," *Electronics*, vol. 11, no. 19, p. 3073, Sep. 2022.

[56] R. Jiang, X. Chen, Y. Yu, Y. Zhang, and W. Ding, "Risk and UCON-based access control model for healthcare big data," *J. Big Data*, vol. 10, no. 1, p. 104, Jun. 2023.

[57] L. Tandon, P. W. L. Fong, and R. Safavi-Naini, "HCAP: A history-based capability system for IoT devices," in *Proc. 23nd ACM Symp. Access Control Models Technol.*, Jun. 2018, pp. 247–258.

[58] B. Serra, D. Evangelista, and F. Lima, "Controle de acesso para condomínios residenciais," in *Proc. Anais da VIII Escola Regional de Computação do Ceará, Maranhão e Piauí*, Sep. 2020, pp. 109–116.

[59] M. Bugliesi, D. Colazzo, S. Crafa, and D. Macedonio, "A type system for discretionary access control," *Math. Struct. Comput. Sci.*, vol. 19, no. 4, pp. 839–875, Aug. 2009.

[60] M. R. Uddin, N. A. Evan, M. R. Alam, and M. T. Arefin, "Analysis of generic routing encapsulation (GRE) over IP security (IPSec) VPN tunneling in IPv6 network," in *Proc. 4th EAI Int. Conf. Ubiquitous Commun. Netw. Computing (UBICNE)*. Cham, Switzerland: Springer, Jan. 2021, pp. 3–15.

[61] R. Oppliger, *SSL and TLS: Theory and Practice*. Norwood, MA, USA: Artech House, 2023.

[62] A. Gabillon, R. Gallier, and E. Bruno, "Access controls for IoT networks," *Social Netw. Comput. Sci.*, vol. 1, no. 1, p. 24, Jan. 2020.

[63] P. García-Teodoro, J. Camacho, G. Maciá-Fernández, J. A. Gómez-Hernández, and V. J. López-Marín, "A novel zero-trust network access control scheme based on the security profile of devices and users," *Comput. Netw.*, vol. 212, Jul. 2022, Art. no. 109068.

[64] A. Pratap and P. Saxena, "An analytical and experimental study of AAA model with special reference to RADIUS and TACACS+," *Int. J. Comput. Appl.*, vol. 169, no. 9, pp. 6–10, Jul. 2017.

[65] K. I. C. Quiroz, V. A. P. Fernaindez, G. C. Barco, D. J. F. AdrianzeÌn, A. H. D. Chavarri, and R. M. Y. Arteaga "Control de acceso a redes inalaì mbricas por medio de protocolos de," in *Proc. Biblioteca Colloq.*, 2022, pp. 1–12.

[66] S. Thorgersen and P. I. Silva, *Keycloak-identity and Access Management for Modern Applications: Harness the Power of Keycloak, OpenID Connect, and OAuth 2.0 Protocols To Secure Applications*. Birmingham, U.K.: Packt Publishing Ltd, 2021.

[67] T. Fathima and S. M. Vennila, "Emphasizing a productive and protective access control to improve authentication using 802.1x with software-defined networks," in *Proc. Int. Conf. Comput., Commun., Elect. Biomed. Syst.* Cham, Switzerland: Springer, 2022, pp. 181–197.

[68] S. Mohanty, S. Sharma, and V. Vishal, "MQTT—Messaging queue telemetry transport IoT based messaging protocol," *Int. Res. J. Eng. Technol. (IRJET)*, vol. 2016, pp. 1–8, Sep. 2016.

[69] A. Luntovskyy, J. Spillner, A. Luntovskyy, and J. Spillner, "Security in distributed systems," *Architectural Transformations Netw. Services Distrib. Syst.*, vol. 2017, pp. 247–308, Jul. 2017.

[70] H. Zhang, W. Wu, and Z. Li, "Open social based group access control framework for e-Science data infrastructure," in *Proc. IEEE 8th Int. Conf. E-Sci.*, Oct. 2012, pp. 1–8.

[71] S. N. Kazmi, "Access control process for a saas provider," Master's thesis, Dept. Future Technol., Univ. Twente, Enschede, The Netherlands, 2019.

[72] M. Lodder, "Token based authentication and authorization with zero-knowledge proofs for enhancing Web API security and privacy," Masters thesis, 2023. [Online]. Available: https://scholar.dsu.edu/theses/425

[73] B. S. Egala and A. K. Paradhan, "Access control and authentication in IoT," in *Internet of Things: Security and Privacy in Cyberspace*. Cham, Switzerland: Springer, 2022, pp. 37–54.

[74] S. Pal and Z. Jadidi, "Protocol-based and hybrid access control for the IoT: Approaches and research opportunities," *Sensors*, vol. 21, no. 20, p. 6832, Oct. 2021.

[75] S. Poduvu, S. M. Saghaian, E. Ufuktepe, A. E. Morel, and P. Calyam, "Risk-based zero trust scale for tactical edge network environments," in *Proc. 8th ACM/IEEE Symp. Edge Comput.*, Dec. 2023, pp. 306–312.

[76] A. M. Tall and C. C. Zou, "A framework for attribute-based access control in processing big data with multiple sensitivities," *Appl. Sci.*, vol. 13, no. 2, p. 1183, Jan. 2023.

[77] M. James, T. Newe, D. O'Shea, and G. D. O'Mahony, "Authentication and authorization in zero trust IoT: A survey," in *Proc. 35th Irish Signals Syst. Conf. (ISSC)*, Jun. 2024, pp. 1–7.

[78] C. P. Kaliappan, K. Palaniappan, D. Ananthavadivel, and U. Subramanian, "Advancing IoT security: A comprehensive AI-based trust framework for intrusion detection," *Peer-to-Peer Netw. Appl.*, vol. 17, no. 5, pp. 2737–2757, Sep. 2024.

[79] G. Lame, "Systematic literature reviews: An introduction," in *Proc. Design Soc., Int. Conf. Eng. Design*. Cambridge, U.K.: Cambridge Univ. Press, Jul. 2019, vol. 1, no. 1, pp. 1633–1642.

[80] P. V. Torres-Carrión, C. S. González-González, S. Aciar, and G. Rodríguez-Morales, "Methodology for systematic literature review applied to engineering and education," in *Proc. IEEE Global Eng. Educ. Conf. (EDUCON)*, Apr. 2018, pp. 1364–1373.

[81] Y. Xiao and M. Watson, "Guidance on conducting a systematic literature review," *J. Planning Educ. Res.*, vol. 39, no. 1, pp. 93–112, Mar. 2019.

[82] R. Boelens, B. De Wever, and M. Voet, "Four key challenges to the design of blended learning: A systematic literature review," *Educ. Res. Rev.*, vol. 22, pp. 1–18, Nov. 2017.

[83] M. J. Page et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *Bmj*, vol. 372, p. 71, Mar. 2021.

[84] P. Churi and A. Pawar, "RUBAC: Proposed access control for flexible utility–privacy model in healthcare," *Social Netw. Comput. Sci.*, vol. 5, no. 3, p. 297, Feb. 2024.

[85] X. Pu, R. Jiang, Z. Song, Z. Liang, and L. Yang, "A medical big data access control model based on smart contracts and risk in the blockchain environment," *Frontiers Public Health*, vol. 12, Mar. 2024, Art. no. 1358184.

[86] A. U. R. Butt, T. Mahmood, T. Saba, S. A. O. Bahaj, F. S. Alamri, M. W. Iqbal, and A. R. Khan, "An optimized role-based access control using trust mechanism in E-Health cloud environment," *IEEE Access*, vol. 11, pp. 138813–138826, 2023.

[87] P. Arora, A. Bhagat, and M. Kumar, "Attribute-based access control model in healthcare systems with blockchain technology," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 5, pp. 1–11, 2023.

[88] D. Reddick, F. A. Feltus, and S. Shannigrahi, "Case study of attribute based access control for genomics data using named data networking," in *Proc. IEEE 19th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2022, pp. 715–716.

[89] R. G. Sonkamble, S. P. Phansalkar, V. M. Potdar, and A. M. Bongale, "Survey of interoperability in electronic health records management and proposed blockchain based framework: MyBlockEHR," *IEEE Access*, vol. 9, pp. 158367–158401, 2021.

[90] M. Shi, R. Jiang, X. Hu, and J. Shang, "A privacy protection method for health care big data management based on risk access control," *Health Care Manage. Sci.*, vol. 23, no. 3, pp. 427–442, Sep. 2020.

[91] P. B. Prince and S. P. J. Lovesum, "Privacy enforced access control model for secured data handling in cloud-based pervasive health care system," *Social Netw. Comput. Sci.*, vol. 1, no. 5, p. 239, Sep. 2020.

[92] A. Tembhare, S. Sibi Chakkaravarthy, D. Sangeetha, V. Vaidehi, and M. Venkata Rathnam, "Role-based policy to maintain privacy of patient health records in cloud," *J. Supercomput.*, vol. 75, no. 9, pp. 5866–5881, Sep. 2019.

[93] T. Kanwal, A. A. Jabbar, A. Anjum, S. U. R. Malik, A. Khan, N. Ahmad, U. Manzoor, M. N. Shahzad, and M. Balubaid, "Privacy-aware relationship semantics-based XACML access control model for electronic health records in hybrid cloud," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 6, pp. 1–24, Jun. 2019.

[94] M. Davari and E. Bertino, "Access control model extensions to support data privacy protection based on GDPR," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2019, pp. 4017–4024.

[95] Y. Zhao, M. Cui, L. Zheng, R. Zhang, L. Meng, D. Gao, and Y. Zhang, "Research on electronic medical record access control based on blockchain," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 11, Nov. 2019, Art. no. 155014771988933.

[96] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, and N. Yu, "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8770–8781, Oct. 2019.

[97] T. T. Thwin and S. Vasupongayya, "Blockchain-based access control model to preserve privacy for personal health record systems," *Secur. Commun. Netw.*, vol. 2019, pp. 1–15, Jun. 2019.

[98] Y. Ming and T. Zhang, "Efficient privacy-preserving access control scheme in electronic health records system," *Sensors*, vol. 18, no. 10, p. 3520, Oct. 2018.

[99] W. Zhang, H. Li, M. Zhang, and Z. Lv, "Privacy-aware risk-adaptive access control in health information systems using topic models," in *Proc. 23nd ACM Symp. Access Control Models Technol.*, Jun. 2018, pp. 61–67.

[100] K. Seol, Y.-G. Kim, E. Lee, Y.-D. Seo, and D.-K. Baik, "Privacy-preserving attribute-based access control model for XML-based electronic health record system," *IEEE Access*, vol. 6, pp. 9114–9128, 2018.

[101] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustain. Cities Soc.*, vol. 39, pp. 283–297, May 2018.

[102] W. Ding, Z. Yan, and R. H. Deng, "Privacy-preserving data processing with flexible access control," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 2, pp. 363–376, Mar. 2020.

[103] C. Kalpana and S. Revathy, "Analysis of time bound collaborative access control delegation model in electronic health records," in *Proc. Int. Conf. Comput. Methodologies Commun. (ICCMC)*, Jul. 2017, pp. 424–429.

[104] F. Rezaeibagha and Y. Mu, "Distributed clinical data sharing via dynamic access-control policy transformation," *Int. J. Med. Informat.*, vol. 89, pp. 25–31, May 2016.

[105] P. Gope and R. Amin, "A novel reference security model with the situation based access policy for accessing EPHR data," *J. Med. Syst.*, vol. 40, no. 11, pp. 1–14, Nov. 2016.

[106] A. S. M. Kayes, J. Han, and A. Colman, "An ontological framework for situation-aware access control of software services," *Inf. Syst.*, vol. 53, pp. 253–277, Oct. 2015.

[107] M. Sicuranza, A. Esposito, and M. Ciampi, "A view-based acces control model for EHR systems," in *Intelligent Distributed Computing VIII*. Cham, Switzerland: Springer, 2015, pp. 443–452.

[108] K. Mohan and M. Aramudhan, "Ontology based access control model for healthcare system in cloud computing," *Indian J. Sci. Technol.*, vol. 8, no. S9, p. 218, May 2015.

[109] J. Bogaerts, M. Decat, B. Lagaisse, and W. Joosen, "Entity-based access control: Supporting more expressive access control policies," in *Proc. 31st Annu. Comput. Secur. Appl. Conf.*, Dec. 2015, pp. 291–300.

[110] D. Grunwell, R. Gajanayake, and T. Sahama, "Demonstrating accountable-eHealth systems," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 4258–4263.

[111] W. Yu, L. Zhang, and Q. Xu, "Real-time reliability access control based on rail traffic data platform," *Electronics*, vol. 12, no. 5, p. 1105, Feb. 2023.

[112] A. Sarfaraz, R. K. Chakrabortty, and D. L. Essam, "AccessChain: An access control framework to protect data access in blockchain enabled supply chain," *Future Gener. Comput. Syst.*, vol. 148, pp. 380–394, Nov. 2023.

[113] R. Elgendy, A. Morad, H. G. Elmongui, A. Khalafallah, and M. S. Abougabal, "Role-task conditional-purpose policy model for privacy preserving data publishing," *Alexandria Eng. J.*, vol. 56, no. 4, pp. 459–468, Dec. 2017.

[114] F. Nazerian and H. Motameni, "New attribute relation-based access control system via hybrid logic," *J. Comput. Secur.*, vol. 10, no. 2, pp. 1–12, 2023.

[115] W. Yu and L. Zhang, "Research on zero trust access control model and formalization based on rail transit data platform," in *Proc. IEEE 10th Int. Conf. Inf., Commun. Netw. (ICICN)*, Aug. 2022, pp. 689–695.

[116] M. Nakerekanti and D. V. B. Narsimha, "Secured multiparty access control model for online social networking using machine learning," *ECS Trans.*, vol. 107, no. 1, pp. 9359–9372, Apr. 2022.

[117] J. Lobo, "Relationship-based access control: More than a social network access control model," *WIREs Data Mining Knowl. Discovery*, vol. 9, no. 2, p. 1282, Mar. 2019.

[118] P. Bennett, I. Ray, and R. France, "Analysis of a relationship based access control model," in *Proc. 8th Int. Conf. Comput. Sci. Softw. Eng.*, 2008, pp. 1–8.

[119] R. Belchior, B. Putz, G. Pernul, M. Correia, A. Vasconcelos, and S. Guerreiro, "SSIBAC: Self-sovereign identity based access control," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Dec. 2020, pp. 1935–1943.

[120] T. Sharma, J. C. Bambenek, and M. Bashir, "Preserving privacy in cyber-physical-social systems: An anonymity and access control approach," Jan. 2020.

[121] K. Asmaa and E. Najib, "Encoding a T-RBAC model for E-learning platform on ORBAC model," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 8, pp. 1–9, 2016.

[122] S. Fugkeaw, "A fine-grained and lightweight data access control model for mobile cloud computing," *IEEE Access*, vol. 9, pp. 836–848, 2021.

[123] S. Dutta, S. S. L. Chukkapalli, M. Sulgekar, S. Krithivasan, P. K. Das, and A. Joshi, "Context sensitive access control in smart home environments," in *Proc. IEEE IEEE 6th Intl Conf. Big Data Secur. Cloud (BigDataSecurity) Intl Conf. High Perform. Smart Comput., (HPSC) IEEE Intl Conf. Intell. Data Secur. (IDS)*, May 2020, pp. 35–41.

[124] Q. Lyu, Y. Qi, X. Zhang, H. Liu, Q. Wang, and N. Zheng, "SBAC: A secure blockchain-based access control framework for information-centric networking," *J. Netw. Comput. Appl.*, vol. 149, Jan. 2020, Art. no. 102444.

[125] A. Chen, G. Lu, H. Xing, Y. Xie, and S. Yuan, "Dynamic and semantic-aware access-control model for privacy preservation in multiple data center environments," *Int. J. Distrib. Sensor Netw.*, vol. 16, no. 5, May 2020, Art. no. 155014772092177.

[126] T. Phillips, X. Yu, B. Haakenson, and X. Zou, "Design and implementation of privacy-preserving, flexible and scalable role-based hierarchical access control," in *Proc. 1st IEEE Int. Conf. Trust, Privacy Secur. Intell. Syst. Appl. (TPS-ISA)*, Dec. 2019, pp. 46–55.

[127] S. A. Afonin, "Performance evaluation of a rule-based access control framework," in *Proc. 2016 39th Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO)*, 2016, pp. 1414–1418.

[128] P. V. Rajkumar and R. Sandhu, "POSTER: Security enhanced administrative role based access control models," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 1802–1804.

[129] L. Kerr and J. Alves-Foss, "Combining mandatory and attribute-based access control," in *Proc. 49th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2016, pp. 2616–2623.

[130] S. Raza Bashir, S. Raza, and V. Misic, "A narrative review of identity, data, and location privacy techniques in edge computing and mobile crowdsourcing," 2024, *arXiv:2401.11305*.

[131] H. F. Atlam, A. Alenezi, R. J. Walters, G. B. Wills, and J. Daniel, "Developing an adaptive risk-based access control model for the Internet of Things," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jun. 2017, pp. 655–661.

[132] Q. Ni, E. Bertino, and J. Lobo, "Risk-based access control systems built on fuzzy inferences," in *Proc. 5th ACM Symp. Inf., Comput. Commun. Secur.*, Apr. 2010, pp. 250–260.

[133] A. Masoumzadeh, P. Narendran, and P. Iyer, "Towards a theory for semantics and expressiveness analysis of rule-based access control models," in *Proc. 26th ACM Symp. Access Control Models Technol.*, Jun. 2021, pp. 33–43.

[134] H. Guo, W. Li, M. Nejad, and C.-C. Shen, "Access control for electronic health records with hybrid blockchain-edge architecture," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 44–51.

[135] S. Villata, N. Delaforge, F. Gandon, and A. Gyrard, "An access control model for linked data," in *Proc. Move to Meaningful Internet Systems: OTM Workshops*. Cham, Switzerland: Springer, Jan. 2011, pp. 454–463.

[136] S. Pal, A. Dorri, and R. Jurdak, "Blockchain for IoT access control: Recent trends and future research directions," *J. Netw. Comput. Appl.*, vol. 203, Jul. 2022, Art. no. 103371.

[137] U. Dowerah, S. Dutta, F. Hartmann, A. Mitrokotsa, S. Mukherjee, and T. Pal, "SACfe: Secure access control in functional encryption with unbounded data," in *Proc. IEEE 9th Eur. Symp. Secur. Privacy*, Jul. 2024, pp. 860–882.

[138] Y. Cai and M. Feng, "A time-bound data access control scheme based on attribute-based encryption," in *Proc. 8th Int. Conf. Cyber Secur. Inf. Eng.*, Sep. 2023, pp. 52–56.

[139] S. Ahmed, A. Dubey, A. Rasool, and M. Gyanchandani, "Access control and encryption techniques during big data accessing stage," in *Proc. 14th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, Jul. 2023, pp. 1–7.

[140] A. S. Chauhan, "Leveraging machine learning to improve access control mechanisms in data warehousing," *Afr. J. Biol. Sci.*, vol. 6, no. 12, pp. 2650–2658, Jul. 2024.

[141] P. Colombo and E. Ferrari, "Access control technologies for big data management systems: Literature review and future trends," *Cybersecurity*, vol. 2, no. 1, p. 3, Dec. 2019.

[142] Z. Ying, X. Zhen, and C. Chi, "A RBAC-based multitask spatio-temporal access control model MT_RBAC," in *Proc. Int. Conf. Comput. Pattern Recognit.*, Jun. 2018, pp. 14–20.

[143] M. Zerkouk, P. Cavalcante, A. Mhamed, J. Boudy, and B. Messabih, "Behavior and capability based access control model for personalized TeleHealthCare assistance," *Mobile Netw. Appl.*, vol. 19, no. 3, pp. 392–403, Jun. 2014.

[144] S. Ravidas, A. Lekidis, F. Paci, and N. Zannone, "Access control in Internet-of-Things: A survey," *J. Netw. Comput. Appl.*, vol. 144, pp. 79–101, Jul. 2019.

[145] A. Alkhresheh, "Dynamic access control framework for Internet of Things," Ph.D. dissertation, School Comput., Queen's Univ., Kingston, ON, Canada, 2019.

[146] F. Lonetti and E. Marchetti, "Issues and challenges of access control in the cloud," in *Proc. 14th Int. Conf. Web Inf. Syst. Technol.*, 2018, pp. 261–268.

[147] K. K. Khedo, "Context-aware systems for mobile and ubiquitous networks," in *Proc. Int. Conf. Netw., Int. Conf. Syst. Int. Conf. Mobile Commun. Learn. Technol.*, p. 123.

[148] T. Chaari, F. Laforest, and A. Celentano "Service-oriented context-aware application design," in *Proc. MCMP@ MDM*, May 2005, pp. 1–10.

[149] J. Bacon and K. Moody, "Access control in distributed systems," in *Computer Systems: Theory, Technology, and Applications*. Cham, Switzerland: Springer, 2004, pp. 21–28.

[150] A. Khoumsi, "Automata-based study of dynamic access control policies," in *Proc. ICISSP*, Jan. 2023, pp. 218–227.

[151] S. Xu, G. Yang, Y. Mu, and R. H. Deng, "Secure fine-grained access control and data sharing for dynamic groups in the cloud," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 2101–2113, Aug. 2018.

[152] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, "Access control in IoT: Survey & state of the art," in *Proc. 5th Int. Conf. Multimedia Comput. Syst. (ICMCS)*, Sep. 2016, pp. 272–277.

[153] J. Shi and H. Zhu, "A fine-grained access control model for relational databases," *J. Zhejiang Univ. Sci. C*, vol. 11, no. 8, pp. 575–586, Aug. 2010.

[154] M. N. K. Odugu, "A fine-grained access control survey for the secure big data access," *Turkish J. Comput. Math. Educ. (TURCOMAT)*, vol. 12, no. 10, pp. 4180–4186, Apr. 2021.

[155] S. D. C. D. Vimercati, S. Foresti, P. Samarati, and S. Jajodia, "Access control policies and languages," *Int. J. Comput. Sci. Eng.*, vol. 3, no. 2, p. 94, 2007.

[156] M. Graube, P. Ortiz, M. Carnerero, O. Lázaro, M. Uriarte, and L. Urbas, "Flexibility vs. Security in linked enterprise data access control graphs," in *Proc. 9th Int. Conf. Inf. Assurance Secur. (IAS)*, Dec. 2013, pp. 13–18.

[157] M. Penelova, "Access control models," *Cybern. Inf. Technol.*, vol. 21, no. 4, pp. 77–104, 2021.

[158] A. K. Routh and P. Ranjan, "A comprehensive review on granularity perspective of the access control models in cloud computing," in *Proc. IEEE Int. Conf. Interdiscipl. Approaches Technol. Manage. Social Innov. (IATMSI)*, Mar. 2024, pp. 1–6.

[159] L. Rosero, M. Riguidel, and J. Aranda, "Granular: An access control model, and confia: Its software tool," in *Proc. XL Latin Amer. Comput. Conf. (CLEI)*, Sep. 2014, pp. 1–9.

[160] I. Molloy, M. Tripunitara, V. Lotz, M. Kuhlmann, C. Schaufler, and V. Atluri, "Panel on granularity in access control," in *Proc. 18th ACM Symp. Access Control Models Technol.*, Jun. 2013, pp. 85–86.

[161] R. G. K. Babu, A. Badirova, F. F. Moghaddam, P. Wieder, and R. Yahyapour, "Authorization and interoperability in access control systems," in *Proc. 14th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2023, pp. 672–674.

[162] J. Hoffmann and B. Gonzalez Otero, "Demystifying the role of data interoperability in the access and sharing debate," *SSRN Electron. J.*, vol. 11, p. 252, Jan. 2020.

[163] M. Lenzerini, "Direct and reverse rewriting in data interoperability," in *Proc. Int. Conf. Adv. Inf. Syst. Eng.* Cham, Switzerland: Springer, Jan. 2019, pp. 3–13.

[164] H. F. Atlam, A. Alenezi, R. Khalid Hussein, and G. B. Wills, "Validation of an adaptive risk-based access control model for the Internet of Things," *Int. J. Comput. Netw. Inf. Secur.*, vol. 10, no. 1, pp. 26–35, Jan. 2018.

[165] O. Ghandour, S. El Kafhali, and M. Hanini, "Computing resources scalability performance analysis in cloud computing data center," *J. Grid Comput.*, vol. 21, no. 4, p. 61, Dec. 2023.

[166] A. Endo, C. Lee, and S. Date, "Scalability evaluation of a per-user access control framework," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2021, pp. 1493–1499.

[167] B. Naqvi, A. Seffah, and C. Braz, "Adding measures to task models for usability inspection of the cloud access control services," in *Proc. 7th Human-Centered Softw. Eng.*, Sophia Antipolis, France. Cham, Switzerland: Springer, Dec. 2018, pp. 133–145.

[168] F. Di Nocera, G. Tempestini, and M. Orsini, "Usable security: A systematic literature review," *Information*, vol. 14, no. 12, p. 641, Nov. 2023.

[169] R. Harrison, D. Flood, and D. Duce, "Usability of mobile applications: Literature review and rationale for a new usability model," *J. Interact. Sci.*, vol. 1, no. 1, p. 1, 2013.
[170] R. Zhang, G. Liu, H. Kang, Q. Wang, B. Wan, and N. Luo, "Anonymity in attribute-based access control: Framework and metric," *IEEE Trans. Dependable Secure Comput.*, vol. 21, no. 1, pp. 463–475, Jan. 2023.

NASTARAN FARHADIGHALATI received the B.Sc. degree in electrical engineering from IAU, Iran, in 2005, and the M.Sc. degree in control engineering from the Ferdowsi University of Mashhad, Iran, in 2011. She is currently pursuing the Ph.D. degree in electrical and computer engineering with NOVA University, Lisbon, Portugal. She is currently a Researcher with the UNINOVA Research Institute. Her research interests include security and privacy testing, testing of access control systems, and data science.

LUIS A. ESTRADA-JIMENEZ received the B.Sc. degree in electronic and control engineering from the Escuela Politecnica Nacional, Ecuador, in 2016, and the M.Sc. degree in mechatronics engineering from the University of Oviedo, Spain, in 2019. He is currently pursuing the Ph.D. degree in electrical and computer engineering with the NOVA University of Lisbon, Portugal. His master's thesis was developed with the Department of Modular Automation, FESTO Company, Germany. He is currently with the UNINOVA Institute as a Researcher. His research interests include self-organization and automation in smart manufacturing systems and the application of artificial intelligence in industrial environments.

SANAZ NIKGHADAM-HOJJATI (Member, IEEE) received the Ph.D. degree in information technology management (business intelligence) from IAU, in 2017. She was a Postdoctoral Researcher with the NOVA School of Science and Technology, NOVA University of Lisbon, from 2018 to 2019, where she is currently a Senior Researcher with the UNINOVA Institute. Her research interests include computational creativity, affective computing, business intelligence, human behavior, emerging technologies, ICT, and innovation management. She has published several books and academic papers in a number of peer-reviewed journals and presented various academic papers at conferences. She has led and participated in several European Union projects and Portuguese and Iranian National projects. In addition, she was an University-Invited Professor. She is currently the Director of the Women in Science, Technology, Engineering, and Mathematics (WoSTEM) Program, UNINOVA.

JOSE BARATA (Member, IEEE) received the Ph.D. degree in robotics and integrated manufacturing from the NOVA University of Lisbon, in 2004. He is currently a Professor with the Department of Electrical Engineering, NOVA University of Lisbon, and a Senior Researcher with the UNINOVA—Instituto de Desenvolvimento de Novas Tecnologias. He has participated in more than 15 international research projects involving different programs, including NMP, IST, ITEA, and ESPRIT. Since 2004, he has been leading the UNINOVA participation in EU projects, namely, EUPASS, self-learning, IDEAS, PRIME, RIVERWATCH, ROBO-PARTNER, and PROSECO. In the last years, he has participated actively researching SOA-based approaches for the implementation of intelligent manufacturing devices, such as within the Inlife Project. He has authored or co-authored over 100 original papers in international journals and international conferences. His main research interest includes intelligent manufacturing, with an emphasis on complex adaptive systems, involving intelligent manufacturing devices. He is a member of the IEEE Technical Committee on Industrial Agents (IES), Self-Organization and Cybernetics for Informatics (SMC), and Education in Engineering and Industrial Technologies (IES).