IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 25 April 2023, accepted 12 May 2023, date of publication 24 May 2023, date of current version 22 June 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3279492

TOPICAL REVIEW

A Survey on Identity and Access Management for Cross-Domain Dynamic Users: Issues, Solutions, and Challenges

AYTAJ BADIROVA, SHIRIN DABBAGHI, FARAZ FATEMI MOGHADDAM, PHILIPP WIEDER, AND RAMIN YAHYAPOUR

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG), 37075 Göttingen, Germany
Institute of Informatic, Georg August University of Göttingen, 37073 Göttingen, Germany

Corresponding authors: Aytaj Badirova (aytaj.badirova@gwdg.de), Shirin Dabbaghi (sdabbag@gwdg.de), Faraz Fatemi Moghaddam (ffatemi@gwdg.de), Philipp Wieder (philipp.wieder@gwdg.de), and Ramin Yahyapour (ramin.yahyapour@gwdg.de)

ABSTRACT Access control management in a heterogeneous cloud environment, where the number of users is growing, is a daunting task for service providers. Efficiency is heavily reliant on shared resources in a modern cloud computing culture. Although data or service sharing is highly appreciated for collaborative projects, preserving identity and access management security is challenging in this context. The difficulties encountered are diverse, including a single point of failure, incompatibility, dynamic user groups, trust establishment, and revocation. Despite extensive research, certain obstacles and issues need to be addressed. In this article, challenges in access management in centralized and decentralized identity governance are grouped into different categories and accompanied by background information on the topic. Studies and implemented projects have been evaluated regarding their value and flaws. Traditional approaches, such as centralized and federated identity, as well as more futuristic methods, such as blockchain-based decentralized identity, AI/ML access management, and ABE schema, have been investigated while writing this paper. A comparative evaluation of the proposed studies has been included, where the differences and similarities can be observed.

INDEX TERMS Access management, cloud computing, security and privacy.

I. INTRODUCTION

Cloud computing (CC) is a widely established technology in industry and academia due to its vast capabilities. Some of the benefits of this trend include on-demand services, flexible provisioning, and a wide range of functions. The ability to employ various services from different sources encourages businesses and individuals to follow suit. Many companies are quickly adopting this service model since it provides numerous economic opportunities, particularly regarding invested finances and human capital. Organizations tend to have less interest in investment in IT infrastructure since outsourcing them from cloud providers reduces hardware, software, and labor costs to maintain them. Leading CC companies, such as Google App Engine [1], Amazon EC2 [2], and Microsoft Azure [3], offer a wide range of services and pricing options that are widely used by interested businesses.

Aside from the public cloud companies listed previously, private and community cloud [4] options are also available. In the case of institutions and scientific organizations, the main objective is to maintain and distribute research data in the most secure way possible within collaborating parties. In such situations, private and community cloud alternatives become crucial.

Collaborative projects in research and development are widely facilitated, requiring the cooperation of various parties with data or services. Different architectures have been developed to manage user identity and access to services, where centralized, federated, and user-centered models are among the most adapted ones. Authentication and authorization are essential in any identity and access management (IAM) system. During the authentication procedure, the user logs

The associate editor coordinating the review of this manuscript and approving it for publication was Diana Gratiela Berbecaru.

in with credentials from their home organization. Even a good authentication technique needs an additional layer to ensure complete security. A reliable authorization strategy is a requirement to have a stable access control system. Whether sensitive data or a costly service is exchanged, each party requires some degree of security to access them. The security standards vary depending on the shared service or data. The security needs of the accessed data or service are defined by access control systems, which decide whether privileged users ensure the security requirements.

As technology advances, so do security risks. Since centralized user management creates a honeypot and introduces security and privacy vulnerabilities such as single point of failure and lack of user data control, the new focus is on decentralized identity systems, also known as self-sovereign identity (SSI). Even though there is no globally accepted definition of SSI, Christopher Allen, widely regarded as a pioneer in the field, proposed ten SSI principles in his article [5]. This new user management paradigm necessitates a new approach to access management strategies. SSI systems are relatively new and need more time to grow in various directions, from legal to technical. Therefore integrating SSI with access management is challenging for now. In general, identity and access management in a cloud environment require technical compatibility, interoperable architecture, security, and privacy management as basic requirements, regardless of being centralized or decentralized. The complexity of dealing with the difficulties mentioned above poses a barrier to cross-organizational (or cross-cloud) identity and access management, given that each company tends to design its own rules and architecture.

A. USER GROUP MANAGEMENT

Internal user groups are well-known, but cross-organizational user groups offer more advantages. Instead of providing permissions to each user individually, user groups allow managing access distribution in a batch manner. Role-Based access control (RBAC) is based on this principle. User groups, whether temporary or permanent, are inherently dynamic. It must be updated frequently when a new user joins or leaves.

1) DYNAMIC USER MANAGEMENT

One of the primary motivations for implementing identity federation is collaborative initiatives. Collaborative projects are dynamic and prone to constant changes. The project structure differs from the organizational structure when multiple organizations are involved. Hence, cross-organizational active user groups are well-known approaches. Regarding dynamic access in a federation, most studies focus on data sharing over the cloud [8], [9], [10], [11]. Although managing active user groups is challenging, the features are convenient for short-term collaborative projects. Within an organization or in cross-organizational projects, such groups can be adopted. Managing such user groups locally is relatively simple. When it comes to having them at the federation level, it becomes a pretty complicated job.

2) HIERARCHICAL USER GROUPS

Several studies have recommended hierarchical user groups because there are multiple groups with varied access types [23], [24], [25]. It can be described in two ways based on various approaches: internally as varied rights within a single group, and externally as different parent-child groupings.

3) INVOLVEMENT OF SSI

The incorporation of SSI in cross-domain access management significantly enhances flexibility and scalability. Because cryptographic technologies back it, its security (reliability) is greater than the legacy approaches. Furthermore, users manage their own identities, ensuring maximum and adjustable privacy. On the other hand, many IAM systems are unprepared for this new paradigm and face several obstacles. However, increasing interest in this field provides optimism for the foreseeable future.

More research needs to be done on the issues of cross-organizational access management and group administration, particularly in a cloud setting. Therefore this paper provides a comprehensive review of cross-organizational user and group management. The following is a list of the paper's efforts:

- cloud computing taxonomy that covers the access mechanisms, characteristics, and approaches
- challenges in cross-organizational centralized and decentralized identity-based access control, interoperability, distinct security requirements, access delegation, and revocation issues
- an exhaustive literature review on state-of-the-art, facilitated methods, contributions, and weaknesses of the current studies
- discussions in the direction of the future of IAM systems

In this work, different aspects of user and group management have been covered. TABLE 1 shows a comparison of this research to other surveys on the same issue. This report not only goes through the issues of earlier surveys in-depth, but also discusses new factors.

The rest of this document is laid out as follows: Section II establishes a foundation for comprehending the issue and briefly summarizes the key concepts. In Section III, the primary issues have been broken down into categories and subcategories. The current state of user management in a dynamic cloud environment is discussed in Section IV, which is followed by the section discussion and conclusion.

II. PRELIMINARIES

A. FEDERATED IDENTITY MANAGEMENT (FIdM)

In a federation environment, multiple services and identity providers participate in providing easily accessible services. In this scenario, identity providers are responsible for creating, managing, and verifying user identities, while service providers should handle the highly available services.

TABLE 1. Evaluation of this work in comparison to existing surveys.

P \ Tp	Tax.	COG	AE	DaM	HG	AI/ML	C	R	SSI
[26]	✓			✓	✓	✓			
[27]	✓		✓	✓	✓		✓	✓	
[28]	✓	✓	✓		✓		✓	✓	
[29]	✓	✓	✓				✓	✓	
This work	✓	✓	✓	✓	✓	✓	✓	✓	✓

Abbreviations: P:papers, Tp:researched topics, COG:cross-organizational groups, AE:attribute-based encryption, DaM:decentralized access management , HG:hierarchical user groups, AI/ML:AI/ML based user management in groups, C:comparison of different approaches, R:revocation, SSI:self-sovereign identity.

Identity federation and management is enabled by single sign-on, account linking, and session management, developed by current XML-based standards. It allows users to interact with other members of the network securely. To access a service or data in the federation, users need to log in once with any membership, then have privileges for multiple providers.

B. ACCESS CONTROL IN CLOUD

Organizational security concerns are addressed through access control systems. The fundamental goal is to secure services and resources from unauthorized, malicious users while allowing legal users to access them. Each access control system's primary qualities are limiting access rights and prohibiting outsiders. Each company has its access control system, detailed in its policy. However, there are just a few access control concepts - DAC, MAC, RBAC, ABAC, and so on. Because ABAC is the most recent and granular, it is briefly covered in this section.

1) ABAC [7]—ATTRIBUTE-BASED ACCESS CONTROL

In comparison to RBAC, ABAC is a relatively new solution that arose from the necessity for more granular access methods. Because permissions and privileges are granted depending on the attributes offered, the requirement for a distinct role is diminished. ABAC is more versatile than prior access control approaches. Based on their specified attributes, users can receive certain rights (or a collection of permissions). User group management is also straightforward with ABAC. Permissions are assigned to the chosen group, and people can be automatically added. In general, ABAC is a context-aware access control mechanism since it can differentiate between many identity providers, which is essential in a cloud environment.

C. ATTRIBUTE-BASED ENCRYPTION

Taking advantage of ABAC Attribute-based encryption (ABE) [30] is a secure way in granular access control systems. This encryption method is mainly used for data access. In traditional public-key encryption (PKI) systems, the access right is based on identity, known as identity-based encryption. (IDE) [31]. The required data must be encrypted with identity-based information, as expected. The public key of the receiver user is utilized in this step. It is quite particular and necessitates information on the recipient user, which may constitute a breach of privacy. ABE is based on attributes rather than specific user identities. Briefly, it is a one-to-many encryption schema. Only users whose keys match predefined attributes during the ciphertext generation can decrypt this ciphertext. It helps to maintain user anonymity while having security under control.

1) CIPHERTEXT-POLICY [32], [35]

With its logic, CP-ABE is similar to ABAC and RBAC schema. Under this encryption paradigm, the data provider should encrypt the data using a present access schema (policy). As a result, the access policy is a part of the final cyphertext. This access schema specifies the types of people who have access to the data. Users obtain private keys that match their sets of attributes from attribute authority. Users can only access and decrypt cyphertext if they can prove that they have the required attributes.

An example of such an access control schema has been demonstrated in Figure 1. The access tree is encrypted alongside the rest of the data in CP-ABE. Because *User3* has the required attribute in the access tree, can access and successfully decrypt the data. In CP-ABE, the data owner has complete control over the data and may change the access schema at any time.

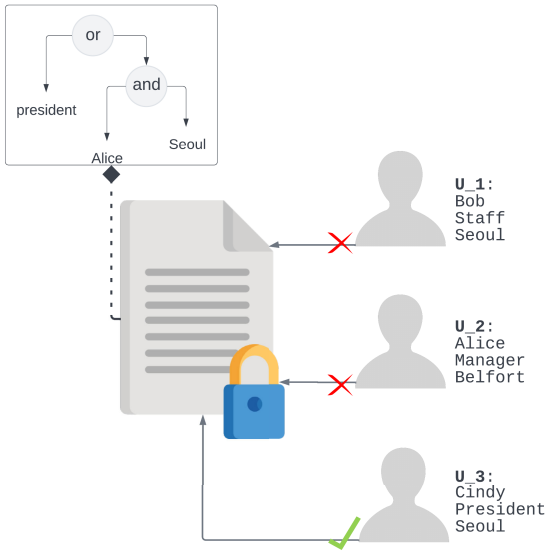

FIGURE 1. Ciphertext-Policy based ABE (CP-ABE) [33].

2) KEY-POLICY [30], [34]

In the KP-ABE model, the ciphertext sender identifies it with multiple informative attributes. The trusted attribute authority (or service provider (SP)) provides the user's private key, which contains the access structure (or access policy). This access structure determines the data types that the key can decode.

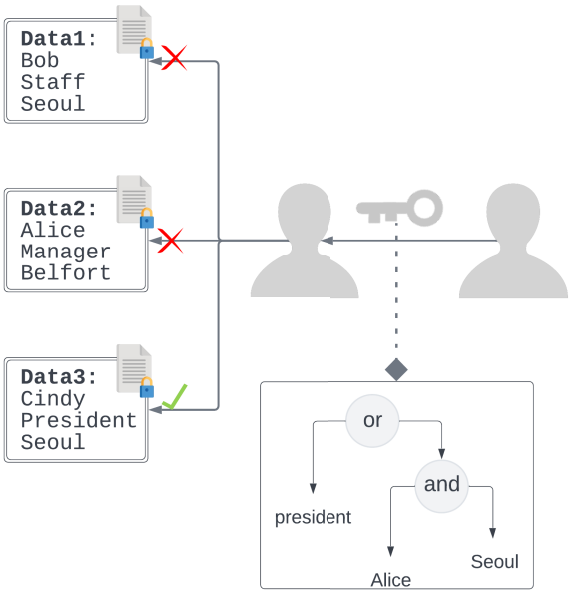

FIGURE 2. Key-Policy based ABE (KPB-ABE) [33].

In Figure 2, the sample of the KP-ABE schema has been presented. Each chunk of data has attributes (e.g., name, surname, location, position). The access tree is a part of the user key which differentiates the user attributes. The encrypted data can be decrypted by using the access tree only when it matches the attributes in the tree. In the given example, the user can access only the Data3 since it has *president* attribute, which satisfies the tree.

The control of data access is the fundamental difference between these two ABE schemas. The access schema tree is a part of the ciphertext in CP-ABE. It allows the owner to control data access. Nevertheless, because the access structure is a part of the provided private key, it is not the case with KP-ABE.

D. GROUP KEY MANAGEMENT

Handling users in groups instead of individually lessens the pressure on controlling access. Specifically, using groups for data access in the cloud is advantageous. Although there are multiple methods for managing groups in the cloud, a common approach is using group keys. Encrypting the data and distributing the key among users is a straightforward method. Since user groups are constantly changing, especially in the cloud, the management system should be flexible enough to handle security changes when a user is added or removed. [36], [37], [38]. There are several group key schemas, such as dynamic, static, or triple-party key agreement protocols, depending on the deployed system and service [26].

E. SELF-SOVEREIGN IDENTITY IN ACCESS CONTROL

A big part of existing access control solutions is based on centralized or federated identity models, in which the user has no control over their data. This architecture is reasonably simple to adopt, but security and privacy are difficult to maintain. Those necessities give rise to a sense of self-sovereign identity. Here, users retain control over their identities and provide data at their discretion under this strategy. In this situation, customers keep their data in their digital wallets instead of at an identity provider.

In the following subsection, the identity management procedure in the self-sovereign identity paradigm is explained. Before going into the workflow, it is necessary to explain core understandings of SSI.

Decentralized identity (DID) is a publicly accessible identifier for every subject (person, organization, device, item, etc.). The structure of DID is already standardized, and for more details, the W3 documentation can be referred to [12]. However, because the technology is new, there is no standard or direct way to use DID. Some projects support a single DID for all services, while others oppose it since it reduces privacy by increasing traceability. DID can be obtained from multiple organizations such as the sovrin foundation [13], the DID foundation [14], and others. In Figure 3, an example of DID structure has been presented. The first part shows the schema of the identity. The next part explains the origin of the DID (e.g., `sovr` indicates Sovrin). Then the last section is the method-specific identifier.

FIGURE 3. An example of DID structure.

Verifiable credential (VC) can be a certificate, diploma, license, or another type of document that can be verified for its legitimacy. The primary qualification of the VC is to be cryptographically secure, machine-readable, and privacy-preserving. The issuer signs the VC by using the issuer's private key. The public key is stored in the verifiable ledger (e.g., a public blockchain). These VCs are assigned to the user's DID and stored in the personal digital wallet of the subject (user). VC contains claims such as name, surname, date of birth, etc.

Whenever the user wants to use VC, they do not share the credential itself, but the presentation of it. Here the user can take advantage of the selective disclosure function of the SSI by sharing only the needed details (claims) without exposing more information.

Verifiable data registry is a blockchain-based ledger that stores various data such as DID, public keys, and schemas. However, because the ledger is public and non-modifiable, no user-specific data should be placed inside it.

Revocation registery plays a crucial role in maintaining security, particularly in access control. The verifier is reliant

on the credential given by the user. In the case of the VC's change (expiration or cancellation), the verifier should be able to verify this change. It is done by revocation registry. The revocation process must be fast and carried out without contacting the issuer in DID management. The revocation register should be able to guarantee the currency of the credential. Distributed ledgers follow similar policies in terms of revocation registry. Hyperledger Indy revocation registry can be taken as an example in this subject [22].

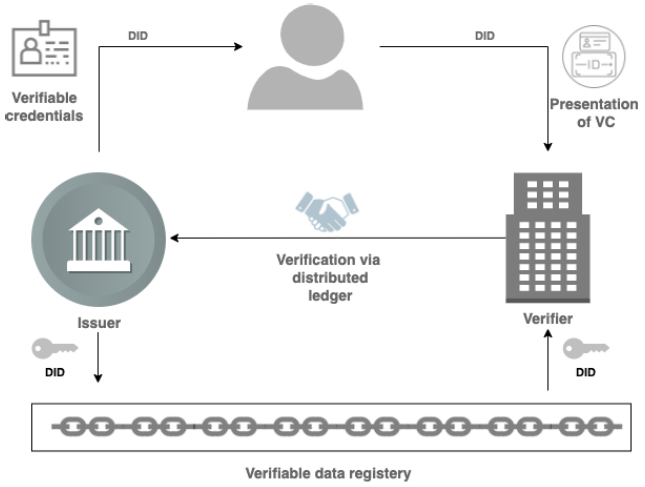

FIGURE 4. Self-sovereign identity.

In Figure 4, a simplified workflow is presented. The issuer (that might be a government or a private entity) signs the VC with its private key, stores the public key on the ledger, and transmits the VC to the holder (user). The VC is stored in the user's wallet. Whenever a user is required to present the credential, they share a presentation. The verifier (receiver of the presentation) can then use the public key in the distributed ledger to validate the legitimacy of the credential.

As discussed in this section, self-sovereign identity is a novel solution with a different workflow from traditional (centralized or federated) identity management systems. User identities in legacy models are not dynamic and are maintained by a single entity, making access control management relatively straightforward and static. With the development of SSI, this procedure necessitates compatible solutions.

III. CHALLENGES IN USER MANAGEMENT IN CLOUD

Cloud computing is becoming more frequently adopted by businesses as it provides a variety of benefits for them, ranging from outsourced data storage to computational and network services. Cloud-based services offer rapid and straightforward access for a large number of users, as well as high availability. When many people from various backgrounds want to access the same service or data, security, and privacy become a concern. The maintenance of access management in traditional systems is a relatively straightforward operation. It is different in the cloud, as the cloud provider determines the security. When many companies cooperate to share services in a federated environment, there is a trade-off between security and accessibility. When SSI is involved, access management systems face new issues. Controlling decentralized sovereign users differs from managing centralized local or federated users. This article discusses the critical issues in access management, regardless of whether centralized or decentralized identity models support the user. The challenges in both systems have been addressed in this section.

A. CENTRALISED IDENTITY

1) SINGLE POINT OF FAILURE

User data is stored and maintained in batches in centralized user management systems. All user data are stored in a single place. Even if there are multiple locations or copies of the data, it is still a centralized method of managing data. This approach introduces the risk of a *single point of failure*. In the event of a technical failure in IDM, the user data (and thus the connected services) are inaccessible. Another issue observed is a security breach in which many user data can be leaked. Therefore, such centralized systems are also known as *honeypots*.

2) SECURITY

In a cross-cloud context, security can take many forms, including data integrity and confidentiality, conflicting security expectations, user identity protection, etc. While data confidentiality entails keeping what should be kept confidential, data integrity means acquiring entirely accurate data (allowing only the authorized user to alter them).

User-centric information (such as health or location data) is particularly sensitive and necessitates high protection. In the case of a security breach, identity theft, profiling, and other issues can cause privacy breaches in individuals' lives.

Distinct Security Requirements: During the project's life cycle, temporary user groups are used in cross-domain collaborative projects. The schema of this group is frequently different from that of the participants. Diverse parties sharing data and resources require varying levels of protection. While some data are very sensitive and must be appropriately protected, others do not. As a result, finding balance in cloud-based collaborative projects is a complicated issue. Given that single sign-on (SSO) in some organizations allows for social identity authentication (e.g., Facebook, Twitter, Google), the potential of a security compromise has increased. On the other side, the federation's primary objective is to enable collaborative projects, which necessitates the federation's dynamic nature and openness to new members while maintaining security for all.

3) MANAGEMENT OF DYNAMIC USER GROUPS

User groups are an essential part of access management systems. In single-domain legacy systems, creating and maintaining such entities are relatively simple. Role-based access control is a typical form of group administration. Things get

more tricky when it comes to a cloud environment. Cloud computing facilitates and encourages collaborative initiatives with people from various companies and creates a bed for cross-organizational projects. Though data and service sharing across an extensive network appear to be valid, it is inconvenient to administer. Given the dynamic nature of user groups, a static access control technique is vulnerable to security breaches in this situation, particularly in a cloud context where multiple IdPs and SPs are involved. The new circumstances must be considered if a newly joined user in the group or a group member's access is canceled or changed.

Secure data exchange has become increasingly challenging due to membership changes. Several studies focus on group keys where the data owner shares the encrypted data, and group members must obtain the key to access and decrypt these data [9], [36], [39]. As soon as a new user joins the group, problems arise. Initially, the new system requires newly permitted users to discover the contents of data stored before their involvement because recent users cannot contact anonymous data owners and gain the relevant decryption keys. Another issue emerges when a user's access to the group is revoked. Because this person still has access to the group key, it is necessary to update it for all users to preserve security. It is not a particularly efficient method in dynamic groups.

Single privileged groups: In a typical collaborative project, the technical and human resource access structures are organized and managed by a single organization. The rest of the participants depends on this one. This scenario needs to be more flexible and can cause dissatisfaction. Since each participant can share a service or data, having an agreement to lead the process can be complicated. Considering this issue, several studies focus on multi-authority cross-domain access control schema. Fan et al. [40] conducted a study that presents a cross-organizational access control approach for social network data based on multi-authority attribute encryption. Employing trustworthy agents, rather than forcing ciphertext re-encryption in policy retrieval, improves system efficiency. Another study [10] focuses on multi-authority service in healthcare data. When it comes to patient diagnosis and treatment, safe data sharing is crucial. The proposed model has a configurable access control system resistant to attribute collision and protects attribute privacy.

4) INCOMPATIBLE ACCESS CONTROL METHODS

In a federated environment, there are diverse participants. Each participant has different authentication and access control systems and sometimes incompatible ones. The entity might facilitate RBAC, ABAC, or another access schema for its services. Each provider relies on its security architecture. Such a heterogeneous environment is a challenge for security. The identity mapping approach aims to meet this challenge. When users request access to a remote service, their identification information is mapped (converted) to the requested service. To achieve a successful relationship, identity mapping requires authentication information from both the requester and the requested [41]. It results in the participants' policies being revealed - policy disclosure.

The study [42] aims to provide a secure access control schema in a smart health environment. One of the main contributions of this work is the ability to hide the access policy partially. In this schema, the user attributes are shared without their values. Since the value of those attributes reveals more sensitive information, hiding them is a reasonable approach.

The study [56] is dedicated to a flexible federation architecture. The heterogeneity of the services provided has been taken into account. M. Stihler and colleagues developed an integrative federated identity management design to enable cross-clients in a multi-provider context. This work allows the creation of multi-provider setups by replicating account data. On the other hand, it does not address the issue of establishing trust connections.

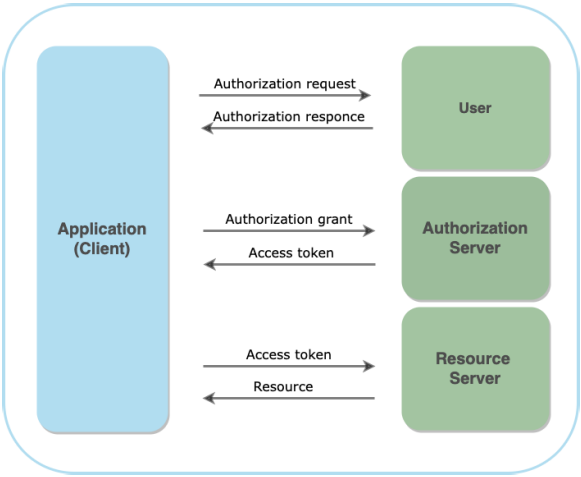

FIGURE 5. OAuth 2.0 schema.

5) INTEROPERABILITY

Interoperability is the capability of 2 parties to communicate and share data while keeping in view each entity's regulations and policies to ensure no barriers to interaction.

Identity management models differ: The identity and access control schema varies depending on the organizational structure or project needs. In *isolated identity* model, all the tasks related to identity management are carried out by the local IDM on the SP side [43]. It can be called an internal identity management schema as well. There is no need for a third party to perform user authentication or authorization. On the other hand, *the central IDM* model supports the centralized identity and access control [44]. In this model, all the tasks related user's identity and access management are maintained by the external IdP. Regarding relatively more extensive collaborations, *federated identity* approach is facilitated [45]. There are multiple IdPs and SPs in this model. No central IdP handles all authentication and access control in this environment. Instead, all of the parties have a trust

relationship. The trust relationship can be direct or indirect. It is called a direct trust relationship if it is established directly between SP and IdP. However, it is indirect if it is done through another IdP (e.g., across different federations) [46].

Interoperability can be an issue inside one federation, between SP and IdP, or between different federations.

Technical interoperability: Interoperability can be grouped into numerous categories: political, legal, organizational, semantic, syntactic, and technical. Since the main objective of this work is access management, the technical level is covered here. SAML [47], OAuth 2.0 [48], OpenID Connect (OIDC) [49], and WS-Federation [50] protocols are a huge part of IAM schemas to handle the authentication and data exchange process.

SAML is an XML-based (EXtensible Markup Language) authentication mechanism that allows IdPs and SPs to exchange assertions. This protocol enables the communication of authorization and authentication data across SOAP, SMTP, HTTP, and FTP. According to the SAML schema, the service provider asks for user information, and the identity provider responds. It is primarily utilized in web-based authentication systems because of its complexity.

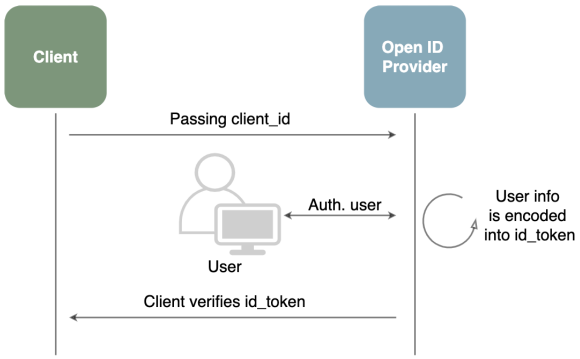

FIGURE 6. OIDC schema.

Another popular authentication protocol is OAuth 2.0 which is JWT based. OAuth 2.0 is lightweight compared to SAML token. Therefore it is widely used for mobile applications. There are several roles in this schema, including client (application), resource owner, authorisation server, and resource server (Figure 5). OAuth 2.0 is used in the deployment of many online and mobile applications. Among these are the social media networks Facebook and Linkedin. Dropbox and GitHub integrate OAuth 2.0 to let users authenticate their services. It allows for the customisation of services while increasing functionality. With OAuth 2.0, the client (application) requests authentication on behalf of the user. There is no need to exchange user information in this scenario. OAuth 2.0 was created primarily for authentication purposes. OIDC (Figure 6) evolved further to address authorization issues in OAuth 2.0, such as requesting user identity information, ensuring the user is authorized. OIDC establishes communication for secure identity data exchange for users by facilitation id_token. id_token holds encoded user information and serves authorization purposes.

When it comes to the data exchange between different federations, such as one based on SAML, and another OAuth 2.0, the heterogeneous protocols and formats lead to a lack of understanding and interruption in the process. A more detailed evaluation of technical interoperability challenges has been covered in [51] and [55].

Metadata: Exchanging a specific type of data that includes information about the participant is required to develop trust between participants. Metadata is the term for this type of information. Aside from metadata, the responsible party's public certificate is also transferred to assure federation confidentiality. The metadata transfer and mapping is usually a manual process that should be checked and renewed whenever a new participant exists. In practically every federation, there are a few almost universal information categories. These are entity id that indicates SP or IdP, certificates of the trusted parties to maintain confidentiality, endpoints (e.g., SSO), and a list of federation members. Since the communication is based on a simple message exchange, the HTTPS protocol is also a part of the federation.

Interoperability schemas: When evaluating the federation structure, it was possible to divide the majority of existing implementation into three groups. The IdP-oriented schema is the initial model. In this case, access to SPs depends on the IdP (Figure 7a). When requesting a service from another federation, the internal IdP acts as a gateway, and success is contingent on its availability. Another model supports the interoperability model that is dependent on SP. In this scenario, the lack of SP restricts service access to only this SP (Figure 7b). There is a third option in which the process is maintained by a trustworthy third party to reduce interoperability difficulties (Figure 7c). In this instance, however, all SPs and IdPs rely on this third party.

6) COMPOSITION OF FEDERATED SERVICES

Higher-level identity management is relatively less complex when there is a one-to-one relationship between service and identity providers. On the other hand, Federated services can be dynamic based on organizational structure. Long-term or short-term commercial connections necessitate coordination across various service providers that creates composed services. Composed services have a relatively complicated authentication and access control system. The metadata (or security) needs of a home SP may differ from those of a composed service [52]. Maintaining security and access control across many levels amongst composed services is an intricate problem that has yet to be solved.

7) DIFFERENT USER TYPES: REGULAR USER, IOT, DIGITAL USER

Regular users are not always the focus of authentication and access control. This scenario could include the Internet of Things (IoT). Most big data is generated by IoT devices

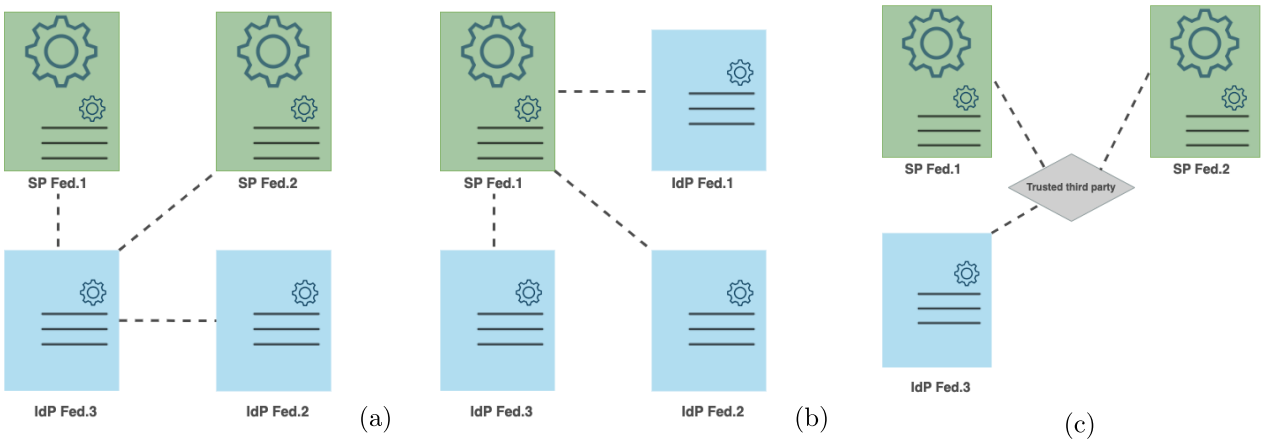

FIGURE 7. Interoperability approaches.

ranging from health care to smart home systems. Since IoT-generated data primarily affects people's privacy, access control becomes a vital issue. Health, financial, and location data are critical data types that might reveal sensitive information about individuals. Flexible and safe access control schemas without demanding human interaction are challenging in a federated context that includes IoT systems. References [53] and [54] focused on secure access management in IoT federations. On the other hand, the growing number of digital employees (remote users) necessitates implementing long-term access management solutions.

B. DECENTRALISED IDENTITY

The constraints in centralized identity models – security, privacy, scalability, portability– lead this field toward a more flexible, user-centered sovereign identity approach. Many of these and more can be addressed through SSI. However, this technology is not yet advanced enough to address all of the current problems. This section discusses some of the significant issues that the industry is now facing.

1) NO STANDARDIZED INTEROPERABILITY SOLUTION

One of the primary goals of SSI is independence from a centralized authority. This feature will necessitate great interoperability, comparable to that of internet protocols (TCP/IP). However, a growing number of SSI solutions need to include it. Various organizations provide diverse ways to obtain and maintain SSI. The W3 consortium has previously offered a standardized methodology for DID and VC that organizations proposing SSI solutions could adopt. The Trust over IP Foundation (ToIP) [16] strongly supports W3 standards. ToIP seeks to provide an internet-wide solution and interoperability in a secure IAM environment.

2) LACK OF INTEGRATION WITH CURRENT IAM SYSTEMS

Even with the standardization of SSI, and interoperable wallets, it is unrealistic to expect SSI to replace all existing IAM systems at once. Companies have spent significant sums of money developing and implementing their IAM models, and it is unlikely they will be keen to throw them out and start from scratch. As a result, legacy IAM systems must be compatible with SSI. Several SSI initializers take this circumstance into account. *Accenture* [18] has a similar strategy, which will be discussed further in the review section.

Reference [19] developed a concept for an assurance level in a cross-border health system based on the eIDAS initiative.

3) TRANSPARENCY VERSUS UNLINKABILITY

Users have control over their data when they have self-sovereign identification. They determine what to disclose, with whom, and to what extent (selective disclosure). This implies that the users determine the transparency of their data. Insufficient transparency leads to challenges with trust, authentication, and access management. High transparency, on the other side, might result in user data linking, which leads to traceability and profiling. As a result, the balance between these two factors must be carefully monitored.

4) USER EXPERIENCE

Almost all centralized (or federated) user administration occurs without user interruption. For the user, the data exchange procedure is obscured. In SSI, users must learn to adapt to digital wallets to ensure security and govern the data exchange process. It might be something that only some would be willing to take on. Another area for improvement is that users should have compatible devices (e.g., smartphones, tablets, laptops). Even though it may appear to be a minor issue, it could be one of the most challenging obstacles in developing countries.

5) LEGAL CHALLENGES

SSI intends to provide a borderless, portable identity solution. However, when it comes to user data that must be adequately secured, legal requirements must be addressed. Apart from being adapted in different countries, data management must comply with General Data Protection Regulation (GDPR)

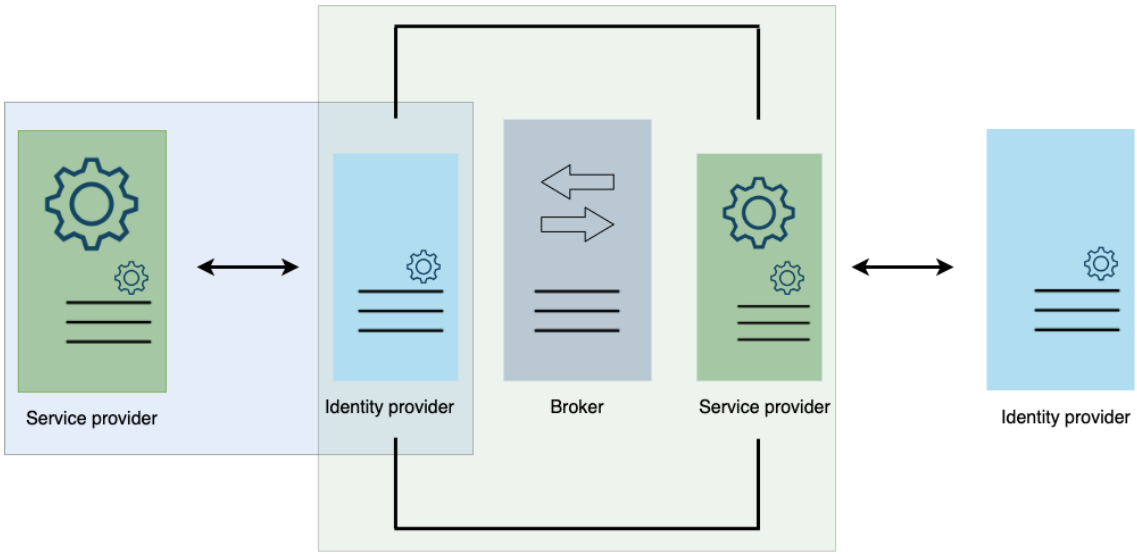

FIGURE 8. Identity federation based on NIST.

[20] standards, particularly in Europe. The acceptability of digital signatures is another legal concern of SSI. The EU project eIDAS [21] attempts to address this issue at the EU level.

6) TECHNICAL CHALLENGES

The distributed ledger locates in the center of SSI. It keeps the majority of the security intact. Although distributed ledger technology is not new, integration with the IAM system is. The first guideline of security is not to keep any user identity-related data on the public ledger. Another issue is with tail files. Tail files contain information for each VC. These files are essential during the revocation procedure as well [22]. However, the size of these files is large, making them unsuitable for the mobile and lightweight apps, and it reduces SSI's scalability.

7) QUALITY OF TRUST ASSURANCE

The trust schema in centralized identity is transparent and is decided by the central authority. Service providers submit their criteria for accessing their services. Some may necessitate PKI, certificates, predefined attributes, or approved profiles (for example, InCommon bronze or silver profile [116]). In this case, the degree of trust (assurance) is reasonably simple to regulate. When it comes to a decentralized sovereign identity, however, establishing a shared sense of trust is a challenging task. Being secure does not necessarily imply having authority or access to all services, which points to the importance of the level of assurance (LoA) for SSI in IAM.

IV. ACCESS CONTROL MODELS IN CLOUD

For a long time, dynamic user management has been a prominent topic. It is an issue that has been the subject of several works. The core objectives in this area are to make collaborations easier, to make user data exchange between services and identities flexible, and to ensure maximum security.

Various ways have been tried to deal with the mentioned issue. The proposed systems can roughly be grouped into two categories: centralized trust management (which could be a trusted third party or a federation's leading participant) and non-centralized trust management. Figure 8 [57] demonstrates two approaches at once - the blue rectangle indicates a direct connection between SP and IdP, green one shows a broker-based identity federation. NIST (National Institute of Standards and Technology) [58] created this solution to provide a high level framework for organizations to share identification information in order to access distant services. The proposed schema uses SAML protocol to exchange the data between SP and IdP. Each approach has its pros and cons. Even though central trust models seem more straightforward and simple to establish, it causes a single point of failure. Another challenge that must be focused on is a non-scalable system in centralized models. Non-centralized models, on the other hand, are complex to create and maintain.

In this chapter, the chronological review of the IAM concept has been evaluated. Several studies and projects have been mentioned with different identity management schemas, including more futuristic concepts such as blockchain-based self-sovereign identity models. The methodology for this review paper involved conducting a systematic search of the literature using a combination of keywords. The investigation included peer-reviewed articles, conference proceedings, and white papers published in the last years to ensure the relevance and currency of the results. The databases used for the search included IEEE Xplore, ACM Digital Library, and Scopus. The inclusion criteria for the articles were that they had to be original research studies written in English and related explicitly to IAM.

The identified studies were then screened and assessed for quality using predetermined criteria such as the methodology used.

A. BROKER-BASED FEDERATIONS

Any federation system relies heavily on data exchange. The main goal here is to collaborate with users from other organizations, share resources and data, and do so among authorized individuals. User administration in the cloud is complex, considering different factors such as security, privacy, and interoperability. Managing participant organizations in bulk is a more adaptable strategy, or, to put it another way, employing brokers [57], [59]. Brokers can be chosen from the federation's members, or they can be an external, trusted third party. Remote user control and administration are managed at the broker level in any circumstance. Although it implies a single point of failure, a broker is a widely adopted method because of its feasibility.

The [60] research project focuses on identity federation via a trusted broker (TB). The broker is responsible for bringing the parties together. When IdPs want to access the SP's service, they'll contact the TB to establish a connection. On the other hand, the brokered federation is immobile, and the parties are entirely reliant on the broker. There will be no broker-side inspection in the future.

Another paper introduced automatic federation based on predefined criteria [61]. The IdP or SP will indirectly trust the other parties, and the federation will be dynamically formed. However, a third party is used to calculate the trustworthiness, which is unknown to the relying parties and constitutes a security risk.

Reference [62] proposes a cloud identity broker-based paradigm for dynamic federation. The broker must be trusted for entities in the cloud to have trusting relationships. It enables the entities to form an active federation. The employment of cryptographic methods, particularly re-encryption proxy, promotes user privacy in this new architecture. However, because this data is stored on a public cloud, several security concerns arise. Furthermore, the centralized brokered identity solution has more drawbacks. The user and the SP should utilize the same identity broker for access control and identification. It drastically restricts flexibility and the ability to choose among several identity broker solutions.

Several studies proposed an approach for a dynamic cloud environment [63], [65], [66]. In the study, [63], the trustworthiness of all the participants is calculated based on predefined trust features before the federation process is carried on. It succeeds if only the party's policy requirements are met. On the other hand, the authors do not mention how trust features and API calls are exchanged with depending parties to complete the transaction and calculate trustworthiness. No API structure is given to make a call for IdP. Calculating or trusting if there are no ranks for an entity's features is not a sound business practice.

TABLE 2. Requirements for cloud access control schemas.

Name	Code	Description
Scalability	C1	Fast adaptability of a dynamic environment
Functionality	C2	Service discovery, interoperability, performance
Security	C3	Secure data exchange and management in broker
Portability	C4	Adaptability to different cloud federations
Privacy	C5	User data privacy, privacy policy adaptation
Trustworthiness	C6	Internal SP, IdP policies, trust relationship requirements
Evaluation	C7	Implementation based on real environment (R) or in simulation (S)

In [64], authors demonstrate an FIM model with central trust management called Trust Service Provider (TSP). Identity and service providers will be untrustworthy at first. After the federation is completed via TSP, they enter the TSP circle of trust. Centralized trust management and indirect authentication exchange help to deploy FIM quickly. It established the trust between parties automatically. This study aims to establish authentication without the need for a federation. This schema, on the other hand, has limited flexibility and is not dynamic in addition to having security vulnerabilities.

Diniz et al. [25] use a relatively different approach for cloud identity management. A hierarchical access control model underpins the suggested method. In this model, access to shared resources is checked by the cloud service provider's administrator. It is another example of a centralized paradigm with scalability constraints.

Another option for broker-based services is called cloud access security brokers (CASB), according to the study [67]. CASBs are the main spots where security is enforced between users and service providers, who often have security restrictions in place to access cloud services. The CASBs may influence the company's internal operations as well. The core security controls include authorization, policy identification, malware detectors, security audits, etc. On the other hand, some security threats, such as customer-data manipulation and hijacking, still exist.

Reference [68] is the next stage in modeling and analyzing trust relationships using fuzzy cognitive maps. It employs a trust computation model. If sufficient data is available, the suggested model can be used to determine the trustworthiness of unfamiliar users (or parties). This strategy makes setting up a secure Infrastructure as a Service (IaaS) accessible, especially in a federated cloud context. Because the proposed approach features a dynamic and quickly adaptive qualification, the scalability issue is significantly mitigated. Despite using anonymization techniques, the system, nevertheless,

TABLE 3. Comparative evaluation of brokering models.

References	C1	C2	C3	C4	C5	C6	C7
Huang,He Yuan,et al. [60]		✓	✓		✓	✓	S
Zwattendorfer, Bernd, et al. [62]			✓	✓			S
Prashant et al. [75]		✓	✓			✓	R
Bah, Abdramane, et al. [52]	✓		✓				R
Fernandez, Eduardo B, et al. [67]		✓			✓	✓	S
Patiniotakis, Ioannis, et al. [69]	✓	✓	✓		✓	✓	R
Jiang, Jian, et al. [64]		✓		✓			
Basney, Jim, et al. [76]	✓	✓	✓	✓	✓	✓	
Liu, Chuanyi, et al. [71]	✓	✓	✓		✓	✓	R
Keltoum, Bendiab, and Boucherkha Samia [66]	✓	✓					

stores personal data in an external database, presenting a privacy concern. The approach focuses on a specific use case.

Prashant et al. [75] proposed another cloud brokering model. It considers several aspects, such as SLA and resource management in virtual machines. This approach is not portable where the internal policy privacy is another issue.

Another stud called PuLSaR [69] aims to maintain the fuzziness in service selection. It uses the multi-criteria decision-making (MCDM) method.

Enabling secure data publishing and retrieval in a reliable environment was addressed in several works [70], [71]. While encrypted data can be easily shared, sensitive data should be maintained privately. In this case, the critical data will still be secure even if a malicious user can access the data. The project SafeBox [70] also allows data exchange between brokers.

With the aid of a reliable intermediary, a multilayered federation can be set up dynamically and for a wide range of services. The cost of establishing multi-lateral trust relationships might be considerably lowered using the brokered trust paradigm. Furthermore, the trustworthy broker could serve as a referee, resolving cross-service access issues. The cloud is a reliable partner for all in-cloud services and businesses. External services should also have trust in the cloud if they want to connect to it. TABLE 2 presents several criteria used in TABLE 3 while comparing several proposed works. The studies [72], [73], [74] evaluate the brokering in the federation cloud in detail and can be referred to for more information.

B. MULTI-AUTHORITY ACCESS MANAGEMENT

In a cloud context, centralized access management is a commonly adopted model for user control. It establishes a consistent access model and conceals incompatibilities. On the other hand, having a central unit to manage all the access control tasks leads to several issues, such as a single point of failure, performance limitation, overwhelming service, etc. A distributed (multi-authority) access management system has emerged to address the mentioned complications. This section covers two effective methods of distributed access management: attribute-based encryption and blockchain access management.

1) ATTRIBUTE-BASED ENCRYPTION

The ABE schema is a relatively new method frequently used to protect remote data and service access. ABE-based schemas can be grouped into several categories (Figure 9). CP-ABE, KP-ABE, and hierarchical models have been discussed in this paper.

One of the initial studies that focused on attribute-based encryption for multi-authority access management was proposed by Allison Lewko and Brent Waters [77]. This work is backed by ciphertext policy-based ABE. Hence it is called MA-CP-APE. In this approach, multiple attribute authorities (AA) participate. Each assigns a specific attribute to a user while providing the related private key. The provided private key should also be created and managed by AAs. The proposed model eliminates the need for central supervision nodes. On the other hand, the proposed work is open to user collusion issues. Since there is no central controlling unit, distinct user accounts from different organizations might get the same attribute (though they may have different values), which can lead to unauthorized user access.

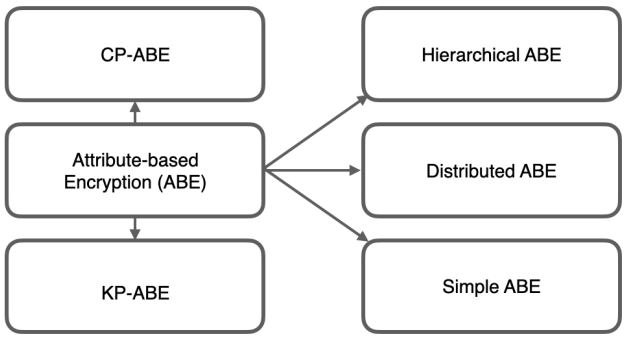

FIGURE 9. ABE approaches.

Reference [78] proposes a reliable multi-authority data access control in a distributed cloud. This work takes advantage of the previously mentioned study [77]. One of the most significant advantages of this study over many others is the

presence of an appropriate revocation method. On the other hand, the proposed design is static and does not address policy updates.

MC!tC) HorvC!th published another study to facilitate the CP-ABE schema for data access management in the cloud [79]. The designed model includes an appropriate revocation technique and a non-centralized multi-authority data access schema. The attribute authorities create a list of active and revoked uses in this study. This list comprises the revoked users' personal information. To control who can decrypt the data, the data owners insert this user list inside the ciphertext.

Yang et al. [80] proposed another access control schema for distributed data in a cloud environment. The fundamental idea is to eliminate the need for a central broker. Access control is maintained by AA inside the organization. The AA requests on their behalf when a user asks for a remote service. The user's privacy is therefore protected. In a distributed system, one of the main challenges is user collusion. Users from different organizations might have the same user attributes, which can lead to unauthorized access. The user attribute is merged with AA's identity information in this work. As a result, the risk of a user collision is minimized. Even though the suggested work has the potential to cure many security issues, several problems still need to be solved. All AAs must establish a trusting relationship when a new member joins the network. Because AAs perform the access request on behalf of the user when there are many requests, the workload for AAs increases, and performance degrades. Another topic that should be included in this study is revocation.

Regarding securing data access on a cloud, several studies focus on securing the content of the data rather than having a secure communication channel. This technique is named data networking - NDN [81]. The studies [82], [83] apply an attribute-based encryption approach to secure data while facilitating the NDN approach.

The EU's Horizon 2020 R&D project PRISMACLOUD [84] focuses on secure data access on the cloud. The proposed approach targets two directions - encrypting outsourced data and preserving users' privacy. The model works based on a shared secret. Data security is maintained by encryption and tokenization techniques. On the other hand, access management is backed by ABAC. However, more than a pure ABAC model is needed to preserve user privacy. Therefore the proposed model adapts attribute anonymization technique and data minimization strategy.

Belguith, Sana, et al. [85] proposed an approach different from existing ones for access control in a cloud by merging ABE and attribute-based signature. To use a privacy-preserving method, the objective is to provide multi-authority access control in the cloud. When a user attempts to authenticate, the cloud service provider (CSP) sends a message to the user, instructing them to sign. After a successful singing process, the CSP determines whether this user has the required attributes. One of the significant advantages of this work is that it offers multiple attributes rather than a single-attribute approach. Furthermore, the CSP manages network traffic to prevent flooding attacks. On the other hand, there is a *honest but curious* thread. The CSP may return the required output and data, but it can still monitor actions, thereby compromising privacy and security.

Okamoto T. and Takashima K. conducted one of the initial studies, which focus on decentralized access control by using attribute-based encryption [86]. The architecture is based on multiple attribute authority and does not require a centralized management system. Interoperability concerns arise since the model requires static parameters to establish secure access. Finding consensus when various endpoints utilize different authentication parameters is a difficult task. The proposed model, on the other hand, is safe and easy to apply. The proposed approach can be improved and adapted to different environments. Furthermore, multi-authority attribute-based encryption (ABE) and signature (ABS) are relatively new concepts and helpful in this domain.

Another work for decentralized access management has been done by Ruj et al. [87] for data storage in a cloud. Similarly, in the study [86], the model also takes advantage of ABE and ABS. The authors propose an anonymous authentication schema to keep user identity private. The cloud service provider should be able to authenticate the provenance of the data under the defined access architecture, where the data is generated by the legitimate user under the condition of obscuring the owner's identity.

Roa and Dutta took advantage of the key-policy-based ABE schema in their work [88] and created a model key-policy-based ABS. An access tree is used to extract the user's key. As a result, a user whose access structure matches this set creates the signature based on a set of attributes.

ABC4Trust [90] - Attribute-based Credentials for Trust is an IAM initiative financed by the EU and ran from 2015 to 2018. The project was supported by big companies such as IBM and Microsoft and multiple institutions (e.g., Goethe University Frankfurt, TU Darmstadt). The project's purpose was to prevent data tracking and correlating from many providers while providing requested access rights securely. The goal was to protect the end user's privacy while accessing services. Data shared via the internet can (and in many circumstances is) be shared with third parties. In an oversimplified scenario, an insurance firm may learn about the customer's lifestyle and raise the health insurance rate. ABC4T uses smart cards, and in the event of card corruption, the rights of the card are removed. On the other hand, this strategy requires using compatible technical devices.

Given that, even inside a single organization, not all user accounts have the same security requirements, making a distinction among them would be reasonable. A limited amount of studies based on ABE schema support this hierarchical approach, such as [89]. This work aims to solve access management issues in a collaborative environment where different types of users exist. CP-ABE backs the proposed model. This approach provides an incomplete decryption structure

TABLE 4. Comparison of ABE based models.

Work	Type	Access Policy	Multi-authority	Revocation
Lewko Allison and Brent Waters [77]	CP-APE	Static	✓	
Yang, Kan, and Xiaohua Jia. [78]	CP-ABE	Static	✓	✓
Horváth, Máté. [79]	CP-APE	Static	✓	✓
Yang, Yan, et al. [80]	CP-APE	Static	✓	
Lee, Craig A., et al. [82]	CP-ABE	Static	✓	
Belguith, Sana, et al. [85]	CP-ABE	Threshold	✓	
Okamoto, Tatsuaki [86]	Simple ABE	Static	✓	
Ruj, Sushmita et al. [87]	Simple ABE	Static	✓	
Rao, Y. Sreenivasa, and Ratna Dutta. [88]	KP-ABE	Static	✓	
Huang, Qinlong et al. [89]	Simple ABE	Threshold	Hierarchical	
ABC4Trust(EU) [90]	ABE	Static	✓	✓
PRISMACLOUD Horizon 2020 [84]	ABE	Static		

and produces partial signatures by delegating signature computation when users decrypt the ciphertext.

In this section, several ABE-based multi-authority access control systems have been covered. A comparative evaluation of these works can be found in TABLE 4.

C. FEDERATED IDENTITY IN ACADEMY AND INDUSTRY

In both academia and industry, current identity federation solutions are critical. Those implementations are particularly beneficial to research associations. On collaborative research projects, data and resource sharing has a tremendous impact. GÉANT [115] is one of the leading solutions in the academy. It offers the eduGAIN service, which allows many identity federations to partner up. As a result, not only do SPs and IdPs interact with one another in this situation, but different federations can build a bridge. Hence, eduGAIN has a federation-to-federation model where the trust is based on predefined protocols. Another option is InCommon [116], which is from the United States. InCommon has two distinct profiles: bronze and silver. The security audit for the bronze profile is performed automatically and is not very thorough, whereas the security audit for the silver profile is performed manually and is highly comprehensive. These two profiles indicate the security level of the participant, IdP or SP. The goal of this service is also to allow connectivity between various IdPs and SPs. A comparable example of identity federation in the academy is Elixir [117]. The program's primary purpose is to supply life science researchers with a wide range of data and service resources. All the described platforms have a consistent set of criteria for all participants. In certain circumstances, these requirements do not align with corporate (provider) policies, resulting in such services being excluded from the federation.

D. DECENTRALISED IDENTITY-BASED ACCESS MANAGEMENT

As mentioned, self-sovereign decentralized identity is the new hype and hot topic for the IDM. This model requires a new way of access management as well. For the time being, two approaches to decentralized identity affect the access management process. One method proposes a central point to verify the VC whenever a user accesses a service (e.g., a university to verify the diploma whenever the holder applies for a job). While this approach is relatively easy to implement, it does not comply with the core concept of SSI - which is privacy. In this model, the issuer has the potential to track user activity. Another model is an entirely decentralized approach where there is no need for communication with the issuer to verify the document. The verification process is done via a verifiable data registry. In this section, both approaches will be covered. Decentralized identity is a very curial area, particularly EU, to preserve the privacy and sovereignty of individuals. Therefore, there are different projects in progress and completed, some being EU-funded or governmental initiatives. This section covers those core projects as well.

Blockchain technology is an advanced tool used in the IT industry for several decades. This design is built on complicated computations and non-centralized trust management. Recently identity management field has also taken advantage of blockchain. In a simplified way, the incorruptible blockchain network validates and ensures the legitimacy of users, operations, and communications. Hence this approach can be assumed quite reasonable in identity and access management. Mainly, decentralized identity management takes advantage of this technology. The study proposed by Ghosh, Bishakh Chandra, et al. [91] focuses on democratic access management in a cloud environment by eliminating the need for central trust authority. The designed model is backed by blockchain technology. This effort intended to address several difficulties, including insufficient transparency, a single point of failure, the risk of identity manipulation, etc. In addition, the study includes maintaining a balance between underutilized and overutilized cloud resources.

Reference [92] combines the ABE schema with blockchain technology to ensure privacy and security in a dynamic cloud environment. One advantage of using blockchain technology

is maintaining an unaltered track for diverse critical events like key generation, access policy assignment, permission request, and revocation. The encrypted data is stored based on the CP-ABE schema, and access is done via the blockchain. However, this model is limited in the case of scalability since the central concept is designed for a single cloud environment.

Bendiab et al. proposed a new architecture WiP [93] for decentralized access management for Infrastructure as a Service cloud model in an untrusted environment, similar to prior works. As the model is based on the blockchain, it does not require any trust relationship between entities.

In collaborative projects, the data or service can be provided by different parties. They can be public or private. The majority of the studies focus on access management in either a public cloud or a private cloud. However, there are not always sharp edges regarding a real-world use case. Several models need to consider the possibility that there can be a combination of public and private clouds that is called a hybrid. There are relatively fewer studies that take this case into account. The model designed by Banerjee et al. [94] is among them. The proposed approach focuses on having high security and privacy while providing users with flexibility in diverse domains such as supply chains, finance, and medical records. Even though blockchain technology is recently applied in authentication and identity management schema, several studies cover different aspects of it [95], [104], [105]. Tables 5 and 7 are comparative evaluations of blockchain-based and decentralized access management schemas. The absence of a threshold for different user types shows a static access policy, whereas democratic access management indicates non-authoritative governance.

E. EXPLORING DECENTRALIZED IDENTITY INITIATIVES

One of the most important efforts in the EU is *eIDAS* [21]. The project's primary goal is to be independent of centralized identity management platforms, most of which are located outside of the EU. This initiative aims to offer people control over their own data. Users may therefore choose who and to what extent they disclose their data. eIDAS is backed by long PKI, which is one of the most trusted authentication methods in the digital world. eIDAS-enabled PKI can increase the flexibility of secure certificate-based authentication, such as *digital guardianship*. The digital guardianship feature of eIDAS helps delegate the user key generation and management, which can be very useful in a situation where the legal person cannot access the digital identity.

The initiative spans several industries. The part on academic identities promotes student mobility across the EU. While students are participating in short-term programs at different institutions, they need to receive a new account at each location. They may, however, bring their home university identification and access to services with them according to the eIDAS program.

In 2014, the first version of eIDAS was suggested. But, it had a number of concerns, ranging from legal to technological. eIDAS2, the most recent version, was finished in 2021 with major changes. The European Digital Identity Wallet's adaptability is one of the new version's primary features. Every country is urged to prepare its digital wallet in accordance with the new model. Yet, developing a global wallet is not limited to a single corporation. Alternatively, several groups can collaborate to establish a wallet. Yet, the government must authorize such a wallet. Another distinctive feature of eIDAS2 is that each individual (wallet) is assigned a unique identification. Overall, eIDAS2 offers various benefits for improving SSI in Europe. It provides a flexible and adaptable model that is not dependent on any specific technology - eIDAS2 is a general concept that does not require any particular technology, such as DLT, for implementation.

It does, however, have certain downsides. One of the significant difficulties is providing users with a single, permanent identification. Even though it is beneficial and harmless in a single domain, it substantially threatens privacy. By tracing individuals through regular activities, a single identity might result in profiling threats. It is one of the open issues of eIDAS2 and is still under discussion.

GAIA-X [96] is a proposal project for the next-generation cloud infrastructure. It is not aiming for a single cloud but rather a collaboration of cloud service providers, with European data protection law as the guiding principle. The project supports more interconnected clouds and includes an SSI design [97]. Although the project is primarily concerned with the future development of data management, compatibility with federated services is also considered. The main focus of this section is on enabling SSI in traditional services so that sovereign users can benefit from them as well. The project's goal is to integrate many areas, from academia to industry, in order to provide a cross-border solution. Yet, bringing a cross-border solution is quite tough. Among the challenges are legal obstacles and data localisation. Also, there are existing solutions from large commercial organizations such as Amazon, and convincing them to utilize the new solution would be difficult.

ESSIF [98] is another EU-funded project that targets the implementation and adaptation of trust in a digital world with the help of SSI. The ESSIF-lab project began in 2019 and will conclude in 2022. This project collects self-sovereign identity business solutions such as eConsent [102], which aims to have a centralized consent system for patients to manage their health data. On the other hand, since there are several projects in this ESSIF lab, compatibility difficulties arise, limiting SSI's capability. Each project may have unique technological needs. As a result, one solution may be incompatible with another, resulting in SSI fragmentation.

ID Union [99] The goal of the project is to build an ecosystem of trusted digital identities for individuals, businesses, and things. The project collaborates with several organizations, primarily in Germany. However, the target is not just Europe but the entire world. IDunion complies with the EU legal frameworks GDPR and eIDAS. To improve technical interoperability, the projects adhere to international

TABLE 5. Comparison of blockchain based models.

Work	Type	Access Policy	Multi-authority	Revocation
Ghosh, Bishakh Chandra, et al. [91]	Blockchain	Static	Democratic	
Sukhodolskiy, Ilya, and Sergey Zapechnikov [92]	Blockchain/ CP-ABE	Static	✓	✓
Bendiab, Keltoum, et al. [93]	Blockchain	Static	✓	
Banerjee, Soumya et al. [94]	Blockchain	Threshold	✓	
Ismail, Reza. [104]	Blockchain	Static	✓	
Tobin, Andrew, and Drummond Reed. [95]	Blockchain	Static	✓	✓
Ali, Muneeb, et al. [105]	Blockchain	Static	Democratic	
Wang, Shangping, Ru Pei, and Yaling Zhang [106]	Blockchain	Static	Democratic	

TABLE 6. Comparison of DID projects.

Factor	eIDAS	GAIA-X	ESSIF	ID Union	SWITCH	Findy	MS Verified ID	Accenture	ToIP
Initiation	Concept	Concept	Concept	App.	App.	App.	App.	App.	Concept
Issuer's authorization	✓			✓	✓	✓			
Blockchain		Static	✓		✓	✓	✓	✓	✓
Portability	✓	✓	✓				✓	✓	✓
Open source			✓			✓			✓

standards such as W3C, DIF, and ToIP. The goal is to provide DID (SSI) structures to users and entities worldwide. Although the project appears to be highly encouraging for SSI implementation, the large number of initiatives for various sectors raises significant problems, such as communication among them.

SWITCH is a Swiss service provider that helps organizations to take advantage of digitization processes. On the other hand, the platform provides IAM schemas while strongly considering security measures. Recently, SWITCH started to offer SSI solutions as well [100]. In its documentation, it provides a general structure for the integration of SSI. The SWITCH SSI model is primarily intended for use by research and academic institutions while leaving the industry outside of the scope. The project's usage is exclusive to Switzerland, limiting its scalability.

Findy (Finland) [101] is a Hyperledger Indy-based decentralized identity database (ledger). The project offers a wide variety of services that support self-sovereign identity. The goal is to provide individuals with user-centric approaches to data management. Findy project is based on ToIP structure. The pilot project based on Findy has begun its testing phase for the journey from Finland to Croatia to ensure its functionality. Findy, on the other hand, is built on blockchain technology, which may limit its compatibility because some governments disagree with this technology as a source of trust.

Microsoft Entra Verified ID is a recent project from Microsoft that aims to incorporate SSI into their Azure system by following W3C guidelines (since August 2022). Microsoft Entra Verified ID [103] is the new architecture integrated into the MS Authenticator app. Companies that use Azure can thus provide VC to their employees. The user authenticates the app using their regular employee username and password. The user can then request VC from the employer in the following step. This work is relatively new and has some limitations, such as a lack of defined quality assurance and compatibility with other systems.

Accenture [18], a consulting company, provides a schema for its customers who want to use the SSI model. The suggested framework focuses on SSI integration into legacy centralized IAM. The core principle is to leave the authentication to the existing IAM and focus on adapting the authentication of new identities. Given the widespread adoption of centralized (or federated) identity management models, this approach is ideal for the transition period. On the other hand, leaving the authorization step to the service providers adds to the system's load. Even if the VC's origin can be verified, the quality of the assurance level is still unidentified. As a result, design modifications to the SP are required to maintain security.

Trust over IP [16] is a Linux Foundation initiative that strives to foster borderless internet-wide trust. ToIP's documentation discusses identity verification with verifiable credentials in a layer paradigm. The ToIP project aims to provide a collection of technological standards and protocols for digital identity that organizations can use worldwide. This would give consumers a unified and trustworthy digital identity that they could use across many platforms and services. The project's wide adaption is slowed by technical and

TABLE 7. Comparative evaluation of decentralized access models.

References	C1	C2	C3	C4	C5	C6	C7
Lewko Allison and Brent Waters [77]	✓			✓	✓	✓	S
Yang, Kan, and Xiaohua Jia. [78]	✓	✓			✓	✓	
Horváth, Máté. [79]		✓	✓		✓	✓	S
Yang, Yan, et al. [80]				✓	✓	✓	S
Lee, Craig A., et al. [82]	✓	✓				✓	P
Belguith, Sana, et al. [85]		✓	✓			✓	S
Okamoto, Tatsuaki, and Katsuyuki Takashima. [86]		✓	✓		✓	✓	S
Ruj, Sushmita, Milos Stojmenovic, and Amiya Nayak. [87]		✓	✓		✓	✓	S
Rao, Y. Sreenivasa, and Ratna Dutta. [88]		✓	✓		✓		
Huang, Qinlong, Yixian Yang, and Mansuo Shen. [89]		✓	✓		✓		
Ghosh, Bishakh Chandra, et al. [91]		✓	✓		✓		S
Sukhodolskiy, Ilya, and Sergey Zapechnikov [92]		✓	✓		✓	✓	
Bendiab, Keltoum, et al. [93]	✓	✓	✓		✓		S
Banerjee, Soumya et al. [94]	✓	✓	✓	✓	✓		S

governance issues. Yet, several projects, such as Findy, are already utilizing ToIP model. [17].

Even though each initiative has its distinct viewpoint, they all serve the same aim. Table 6 compares decentralized initiatives based on general factors.

F. AI, ML APPLICATION IN ACCESS CONTROL

In identity management, artificial intelligence and machine learning techniques have lately become more accessible. Even though there is far less research on the subject, a well-implemented AI-based method can significantly improve the security of identity and access management systems.

Reference [107] suggests using artificial intelligence (AI) in identity management to solve multi-factor authentication problems. The work proposes analyzing and making access decisions based on previous user behavior. There are several types of users in a real-world environment, including digital users and IoT devices. The offered concepts appear plausible in terms of maintaining security and flexibility. However, because no firm model has been implemented, this effort does not qualify as a strong study.

The issues in legacy identity management systems have broadly been covered in [108] and [109]. Legacy systems have static and rigid architectures, whereas harmful users' activities are altered and adapted rapidly. The ability to dynamically identify aberrant actions is a difficult task for which AI can be helpful. Using dynamic access management can improve accuracy and speed in real time.

Khilar et al. [110] proposed another trust-based access control model for a collaborative environment. The design is based on user behavior. Implemented machine learning approach calculates the degree of trust for the user by using the user's past behavior. Several user behaviors have been considered, such as unauthorized user requests, bogus requests, etc.

The authentication and authorization processes are the first steps in access control. The authorized user is not tracked after the access permission is granted in a typical (or traditional) access control design. As a result, malicious user activity may be missed in this situation. Several studies, including [94], consider this possibility and restrict user behavior even after they have been granted permissions. The study considers three attribute types to analyze authenticated user behavior: subject, object, and environmental attributes. One challenge is that tracking user behavior without violating their privacy is difficult. On the other hand, the computational complexity of the system can be excessive.

The study [111] aims to solve the identity theft issue by applying a machine learning algorithm. The facilitated method is the Bayesian probabilistic. The concept is collecting and using a user's digital fingerprint, which contains different data types. The suggested model divides the obtained data into three categories based on their different levels of expressiveness and reliability. Here the bank details and governmental documents give strong evidence about a user's identity, while social media activities are the least reliable ones. Since the study proposes a concept rather than a solid implementation, several issues become very obvious. One of the main problems is privacy breaches, which likely lead to the profiling thread. On the other hand, very sensitive data, such as bank activities, cannot be reached under legal conditions. Therefore, the success of the proposed approach is questionable.

G. DYNAMIC GROUP MANAGEMENT

Dynamic user groups are widely adapted architectures to manage the permission of a group of users. Cross-organizational user groups are dynamic and relatively complex to manage. Several issues arise, such as the design of the group, the leading participants, etc. Several studies focus on solving access management in a dynamic environment,

particularly in the data-sharing domain. Achieving a flexible and secure data-sharing model in a cross-organizational dynamic user group is daunting. Reference [112] facilitates an attribute-based encryption method for its proposed model. The study focuses on two different attribute types: the user's set of attributes and the user's group attribute. Using the broadcast encryption approach increases flexibility while preserving the user's privacy. Only the users that obtain attributes for dynamic groups can access and encrypt the data in that group.

Hierarchy can be considered two ways for user groups: designing hierarchical groups (parent-child groups) or managing hierarchy inside a group. The first approach requires more work and is affordable to implement and manage since it brings an extra workload. On the other hand, the second model is hard to design but relatively easy to manage after a successful implementation. One work that focuses on the hierarchy inside of a user group is [113]. The authors of this paper proposed hierarchical group key management techniques for a cloud environment. Here all keys are generated by group members' secret values and decrypted with group members' secret values as determined by the key distribution server.

To make a distinction between users while sharing data or selectively sharing access to resources is proposed by Baojiang et al. [114]. The data owner supplies all users with an aggregate searchable encryption key in their configuration. By using this key, each user can construct a single trapdoor. The server must also convert the trapdoor into several trapdoors for various files. In this case, a user must build many trapdoors for every question. It requires a lot of computation and communication. On the other hand, a data leak can be the case.

V. DISCUSSION

Identity and access management (IAM) systems have become increasingly important in today's digital landscape as they provide a secure way to manage access to sensitive information. However, the current state of IAM systems has its limitations. One area of concern is the centralized nature of these systems, which can make them vulnerable to breaches and data leaks. The future of IAM lies in the direction of self-sovereign identity, which emphasizes the importance of giving individuals control over their data. By implementing decentralized systems, individuals will have more control over their personal information and be able to share it on a need-to-know basis. This shift towards self-sovereign identity will improve security and give individuals more autonomy and agency in managing their online identities. Organizations must consider the change toward self-sovereign identity in their IAM strategies moving forward.

VI. CONCLUSION

Secure and dynamic access management is crucial for identity and access management systems. In this paper, the most popular IAM architectures are covered chronologically. Considering that the majority of the current systems are based on a centralized (or federated) model, different identity federation approaches have been evaluated. On the other hand, maintaining user control over their data self-sovereign (decentralized) identity appears promising. This architecture enables individuals to collect and store data and supports security and privacy requirements. While it seems most beneficial for users, it reduces the burden of identity management on organizations. The importance of compliance with GDPR in Europe makes the data management process difficult for IdPs.

It allows us to conclude that the future of the IdM lies in decentralized identity. Nevertheless, DID appears to be a viable alternative to a centralized model, but several issues still need to be solved. Some of the issues raised in this survey - non-standardized approach, lack of integration of current IAM, identity recovery - show that DID requires more effort to mature.

This study focused on identity and access management concerns and presented solutions in a cloud setting. Despite a large number of efforts in this domain, various challenges concerning security, privacy, efficiency, and scalability require more attention.

REFERENCES

[1] *Google App Engine*. Accessed: May 22, 2023. [Online]. Available: https://cloud.google.com/appengine
[2] *Amazon Elastic Compute Cloud (Amazon EC2)*. Accessed: May 22, 2023. [Online]. Available: https://aws.amazon.com/
[3] *Microsoft Azure*. Accessed: May 22, 2023. [Online]. Available: https://azure.microsoft.com/en-us/
[4] A. Marinos and G. Briscoe, "Community cloud computing," in *Proc. IEEE Int. Conf. Cloud Comput.*, Dec. 2009, pp. 472–484.
[5] *Christopher Allen: The Path to Self-Sovereign Identity*. Accessed: May 22, 2023. [Online]. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html
[6] D. Ferraiolo, D. Kuhn, and R. Chandramouli, *Role-Based Access Control*. Norwood, MA, USA: Artech House, 2003.
[7] V. Hu et al., *Guide to Attribute Based Access Control (ABAC) Definition and Considerations (Draft)*, NIST SP 800-162, 2013, pp. 1–54.
[8] 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.
[9] P. Gutte, J. V. Wankhade, and S. Mote, "Key generation & access control policy in cloud data sharing," *EasyChair*, vol. 2562, pp. 1–6, Feb. 2020.
[10] A. S. Shahraki, C. Rudolph, and M. Grobler, "A dynamic access control policy model for sharing of healthcare data in multiple domains," in *Proc. 18th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./13th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2019, pp. 618–625.
[11] A. S. Salehi, C. Rudolph, and M. Grobler, "A dynamic cross-domain access control model for collaborative healthcare application," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manage. (IM)*, Apr. 2019, pp. 643–648.
[12] W3C. (2020). *Decentralized Identifiers (DIDs) V1.0*. [Online]. Available: https://www.w3.org/TR/did-core/
[13] *Sovrin Foundation*. Accessed: May 22, 2023. [Online]. Available: https://sovrin.org/
[14] *Decentralized Identity Foundation*. Accessed: May 22, 2023. [Online]. Available: https://identity.foundation/
[15] Hyperledger Indy. *Hyperledger Indy Revocation Registry*. Accessed: May 22, 2023. [Online]. Available: https://hyperledger-indy.readthedocs.io/projects/sdk/en/latest/docs/concepts/revocation/cred-revocation.html?highlight=revocation#how-credential-revocation-works
[16] *Trust Over IP Foundation*. Accessed: May 22, 2023. [Online]. Available: https://trustoverip.org/

[17] *Trust Over IP Foundation: White Papers*. Accessed: May 22, 2023. [Online]. Available: https://trustoverip.org/wp-content/uploads/Introduction-to-ToIP-V2.0-2021-11-17.pdf

[18] Accenture. *A New Approach for Identity in a Digital World*. Accessed: May 22, 2023. [Online]. Available: https://www.accenture.com/_acnmedia/PDF-173/Accenture-Decentralize-Digital-Identity.pdf

[19] V. M. Jurado, X. Vila, M. Kubach, I. H. J. Jeyakumar, A. Solana, and M. Marangoni, "Applying assurance levels when issuing and verifying credentials using trust frameworks," in *Proc. Open Identity Summit*, 2021, pp. 1–12.

[20] European Commission. *General Data Protection Regulation*. Accessed: May 22, 2023. [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection_en

[21] European Parliament and Council. (2014). *Regulation (EU) on Electronic Identification and Trust Services*. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2014/910

[22] Hyperledger Indy. *Hyperledger Indy HIPE*. Accessed: May 22, 2023. [Online]. Available: https://hyperledger-indy.readthedocs.io/projects/hipe/en/latest/text/0011-cred-revocation/README.html

[23] Y. Zhang, H. Zhang, R. Hao, and J. Yu, "Authorized identity-based public cloud storage auditing scheme with hierarchical structure for large-scale user groups," *China Commun.*, vol. 15, no. 11, pp. 111–121, Nov. 2018.

[24] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, and W. Xie, "An efficient file hierarchy attribute-based encryption scheme in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1265–1277, Jun. 2016.

[25] T. Diniz, A. C. D. Felippe, T. Medeiros, C. E. da Silva, and R. Araujo, "Managing access to service providers in federated identity environments: A case study in a cloud storage service," in *Proc. XXXIII Brazilian Symp. Comput. Netw. Distrib. Syst.*, May 2015, pp. 199–207.

[26] M. Li, R. Zhang, X. Du, M. Zhou, L. Yan, and J. Song, "A survey on group key agreement protocols in cloud environment," in *Proc. 1st Int. Cogn. Cities Conf. (IC3)*, Aug. 2018, pp. 160–165.

[27] F. Cai, N. Zhu, J. He, P. Mu, W. Li, and Y. Yu, "Survey of access control models and technologies for cloud computing," *Cluster Comput.*, vol. 22, no. S3, pp. 6111–6122, May 2019.

[28] R. El Sibai, N. Gemayel, J. B. Abdo, and J. Demerjian, "A survey on access control mechanisms for cloud computing," *Trans. Emerg. Telecommun. Technol.*, vol. 31, no. 2, Feb. 2020, Art. no. e3720.

[29] S. Kotha, M. Rani, B. Subedi, A. Chunduru, A. Karrothu, B. Neupane, and V. E. Sathishkumar, "A comprehensive review on secure data sharing in cloud environment," *Wireless Pers. Commun.*, vol. 127, pp. 2161–2188, Dec. 2022.

[30] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Secur.*, Oct. 2006, pp. 89–98.

[31] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *Advances in Cryptology—CRYPTO 2001: 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19–23, 2001 Proceedings*. Berlin, Germany: Springer, 2001.

[32] J. Bethencourt, A. Sahai, and B. Waterss, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2007, pp. 321–334.

[33] J. Lee, S. Oh, and J. W. Jang, "A work in progress: Context based encryption scheme for Internet of Things," *Proc. Comput. Sci.*, vol. 56, pp. 271–275, Jan. 2015.

[34] C. Wang and J. Luo, "An efficient key-policy attribute-based encryption scheme with constant ciphertext length," *Math. Problems Eng.*, vol. 2013, pp. 1–7, Jan. 2013.

[35] S. Yu, K. Ren, and W. Lou, "FDAC: Toward fine-grained distributed data access control in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 4, pp. 673–686, Apr. 2011.

[36] W. Song, H. Zou, H. Liu, and J. Chen, "A practical group key management algorithm for cloud data sharing with dynamic group," *China Commun.*, vol. 13, no. 6, pp. 205–216, Jun. 2016.

[37] G. Lin, H. Hong, and Z. Sun, "A collaborative key management protocol in ciphertext policy attribute-based encryption for cloud data sharing," *IEEE Access*, vol. 5, pp. 9464–9475, 2017.

[38] J. Hur and D. J. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 7, pp. 1214–1221, Jul. 2011.

[39] K. Marimuthu, D. G. Gopal, K. S. Kanth, S. Setty, and K. Tainwala, "Scalable and secure data sharing for dynamic groups in cloud," in *Proc. IEEE Int. Conf. Adv. Commun., Control Comput. Technol.*, May 2014, pp. 1697–1701.

[40] K. Fan, Y. Bai, H. Xu, Q. Pan, H. Li, and Y. Yang, "A secure cross-domain access control scheme in social networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.

[41] OASIS. (May 22, 2009). *Web Services Federation Language (WS-Federation) Version 1.2. OASIS Standard*. [Online]. Available: http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.pdf

[42] Y. Zhang, D. Zheng, and R. H. Deng, "Security and privacy in smart health: Efficient policy-hiding attribute-based access control," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 2130–2145, Jun. 2018.

[43] A. Jøsang and S. Pope, "User centric identity management," in *Proc. AusCERT Asia Pacific Inf. Technol. Secur. Conf.*, vol. 77, 2005, pp. 1–13.

[44] Y. Cao and L. Yang, "A survey of identity management technology," in *Proc. IEEE Int. Conf. Inf. Theory Inf. Secur.*, Dec. 2010, pp. 287–293.

[45] S. S. Y. Shim, G. Bhalla, and V. Pendyala, "Federated identity management," *Computer*, vol. 38, no. 12, pp. 120–122, Dec. 2005.

[46] H. L'Amrani, B. E. Berroukech, Y. E. B. E. Idrissi, and R. Ajhoun, "Toward interoperability approach between federated systems," in *Proc. 2nd Int. Conf. Big Data, Cloud Appl.*, Mar. 2017, pp. 1–6.

[47] A. Armando, R. Carbone, L. Compagna, J. Cuellar, and L. Tobarra, "Formal analysis of SAML 2.0 web browser single sign-on: Breaking the SAML-based single sign-on for Google apps," in *Proc. 6th ACM Workshop Formal Methods Secur. Eng.*, Oct. 2008, pp. 1–10.

[48] D. Hardt. (2012). *The OAuth 2.0 Authorization Framework*. [Online]. Available: https://www.rfc-editor.org/rfc/rfc6749

[49] N. Sakimura, J. Bradley, M. Jones, B. De Medeiros, and C. Mortimore, "OpenID connect core 1.0," OpenID Foundation, San Ramon, CA, USA, Tech. Rep., 2014, p. S3. Accessed: May 22, 2023. [Online]. Available: https://openid.net/specs/openid-connect-core-1_0.html

[50] M. Goodner, M. Hondo, A. Nadalin, M. McIntosh, and D. Schmidt, "Understanding WS-federation," Microsoft, IBM, Redmond, WA, USA, Tech. Rep., 2007.

[51] M. Ates, C. Gravier, J. Lardon, J. Fayolle, and B. Sauviac, "Interoperability between heterogeneous federation architectures: Illustration with SAML and WS-federation," in *Proc. 3rd Int. IEEE Conf. Signal-Image Technol. Internet-Based Syst.*, Dec. 2007, pp. 1063–1070.

[52] A. Bah, P. André, C. Attiogbé, and J. Konaté, "Federated access control in service oriented architecture," LS2N, Université de Nantes, Nantes, France, 2019.

[53] P. Fremantle, B. Aziz, J. Kopecký, and P. Scott, "Federated identity and access management for the Internet of Things," in *Proc. Int. Workshop Secure Internet Things*, Sep. 2014, pp. 10–17.

[54] A. Niruntasukrat, C. Issariyapat, P. Pongpaibool, K. Meesublak, P. Aiumsupucgul, and A. Panya, "Authorization mechanism for MQTT-based Internet of Things," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, May 2016, pp. 290–295.

[55] U. Fragoso-Rodriguez, M. Laurent-Maknavicius, and J. Incera-Dieguez, "Federated identity architectures," *Proc. 1st Mex. Conf. Informat. Secur. (MCIS)*, 2006, pp. 1–8.

[56] M. Stihler, A. O. Santin, A. L. Marcon Jr., and J. D. S. Fraga, "Integral federated identity management for cloud computing," in *Proc. 5th Int. Conf. New Technol., Mobility Secur. (NTMS)*, May 2012, pp. 1–5.

[57] P. Grassi, N. Lefkovitz, and K. Mangold, "Privacy-enhanced identity brokers," NIST-NCCoE, Gaithersburg, MD, USA, Tech. Rep., Oct. 2015.

[58] *National Institute of Standards and Technology*. Accessed: May 22, 2023. [Online]. Available: https://www.nist.gov/

[59] Gartner. (2017). *Magic Quadrant for Cloud Access Security Brokers*. [Online]. Available: https://www.gartner.com/en/documents/3834266

[60] H. Y. Huang, B. Wang, X. X. Liu, and J. M. Xu, "Identity federation broker for service cloud," in *Proc. Int. Conf. Service Sci.* IEEE, May 2010, pp. 115–120, doi: 10.1109/ICSS.2010.46.

[61] D. W. Chadwick, "Federated identity management," in *Foundations of Security Analysis and Design V*. 2009, pp. 96–120.

[62] B. Zwattendorfer, D. Slamanig, K. Stranacher, and F. Hörandner, "A federated cloud identity broker-model for enhanced privacy via proxy re-encryption," in *Proc. IFIP Int. Conf. Commun. Multimedia Secur.*, 2014, pp. 92–103.

[63] K. Bendiab, S. Shiaeles, and S. Boucherkha, "A new dynamic trust model for 'on cloud' federated identity management," in *Proc. 9th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Feb. 2018, pp. 1–5.

[64] J. Jiang, H. Duan, T. Lin, F. Qin, and H. Zhang, "A federated identity management system with centralized trust and unified single sign-on," in *Proc. 6th Int. ICST Conf. Commun. Netw. China (CHINACOM)*, Aug. 2011, pp. 785–789.

[65] P. Khanna and B. Babu, "Cloud computing brokering service: A trust framework," in *Proc. 3rd Int. Conf. Cloud Comput., GRIDs, Virtualization*, Jul. 2012, pp. 206–212. [Online]. Available: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=410261773b45ed6980510655e422f52faf707d7f#page=219
[66] B. Keltoum and B. Samia, "A dynamic federated identity management approach for cloud-based environments," in *Proc. 2nd Int. Conf. Internet things, Data Cloud Comput.*, Mar. 2017, pp. 1–5.
[67] E. Fernandez, N. Yoshioka, and H. Washizaki, "Cloud access security broker (CASB): A pattern for secure access to cloud services," in *Proc. 4th Asian Conf. Pattern Lang. Programs (Asian PLoP)*, vol. 15, 2015, pp. 1–8. [Online]. Available: https://hillside.net/asianplop/proceedings/AsianPLoP2015/AsianPLoP2015ConferenceProceedings.html
[68] G. Bendiab, S. Shiaeles, S. Boucherkha, and B. Ghita, "FCMDT: A novel fuzzy cognitive maps dynamic trust model for cloud federated identity management," *Comput. Secur.*, vol. 86, pp. 270–290, Sep. 2019.
[69] I. Patiniotakis, Y. Verginadis, and G. Mentzas, "PuLSaR: Preference-based cloud service selection for cloud service brokers," *J. Internet Services Appl.*, vol. 6, no. 1, pp. 1–14, Aug. 2015.
[70] G. Wang, C. Liu, Y. Dong, H. Pan, P. Han, and B. Fang, "SafeBox: A scheme for searching and sharing encrypted data in cloud applications," in *Proc. Int. Conf. Secur., Pattern Anal., Cybern. (SPAC)*, Dec. 2017, pp. 648–653.
[71] C. Liu, G. Wang, P. Han, H. Pan, and B. Fang, "A cloud access security broker based approach for encrypted data search and sharing," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Jan. 2017, pp. 422–426.
[72] M. Brouwer and A. Groenewegen, "Cloud Access Security Brokers (CASBs)," Univ. Amsterdam, Amsterdam, The Netherlands, Tech. Rep., 2021. Accessed: May 22, 2023. [Online]. Available: https://rp.os3.nl/2020-2021/p33/report.pdf
[73] S. S. Chauhan, E. S. Pilli, R. C. Joshi, G. Singh, and M. C. Govil, "Brokering in interconnected cloud computing environments: A survey," *J. Parallel Distrib. Comput.*, vol. 133, pp. 193–209, Nov. 2019.
[74] A. Elhabbash, F. Samreen, J. Hadley, and Y. Elkhatib, "Cloud brokerage: A systematic survey," *ACM Comput. Surv.*, vol. 51, no. 6, pp. 1–28, Nov. 2019.
[75] P. Khanna, S. Jain, and B. V. Babu, "BroCUR: Distributed cloud broker in a cloud federation: Brokerage peculiarities in a hybrid cloud," in *Proc. Int. Conf. Comput., Commun. Autom.*, May 2015, pp. 729–734.
[76] J. Basney, H. Flanagan, T. Fleury, J. Gaynor, S. Koranda, and B. Oshrin, "CILogon: Enabling federated identity and access management for scientific collaborations," *Proc. Sci.*, vol. 351, p. 31, Mar. 2019.
[77] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2011, pp. 568–588.
[78] K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 7, pp. 1735–1744, Jul. 2014.
[79] M. Horváth, "Attribute-based encryption optimized for cloud computing," in *Proc. Int. Conf. Current Trends Theory Pract. Informat.*, 2015, pp. 566–577.
[80] Y. Yang, X. Chen, H. Chen, and X. Du, "Improving privacy and security in decentralizing multi-authority attribute-based encryption in cloud computing," *IEEE Access*, vol. 6, pp. 18009–18021, 2018.
[81] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, K. Claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named data networking," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, pp. 66–73, 2014.
[82] C. A. Lee, Z. Zhang, Y. Tu, A. Afanasyev, and L. Zhang, "Supporting virtual organizations using attribute-based encryption in named data networking," in *Proc. IEEE 4th Int. Conf. Collaboration Internet Comput. (CIC)*, Oct. 2018, pp. 188–196.
[83] A. Benmoussa, A. E. K. Tahari, C. A. Kerrache, N. Lagraa, A. Lakas, R. Hussain, and F. Ahmad, "MSIDN: Mitigation of sophisticated interest flooding-based DDoS attacks in named data networking," *Future Gener. Comput. Syst.*, vol. 107, pp. 293–306, Jun. 2020.
[84] *Prisma Cloud IAM Security*. [Online]. Available: https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-iam-security
[85] S. Belguith, N. Kaaniche, A. Jemai, M. Laurent, and R. Attia, "PAbAC: A privacy preserving attribute based framework for fine grained access control in clouds," in *Proc. 13th Int. Conf. Secur. Cryptogr. (SECRYPT)*, vol. 4, 2016, pp. 133–146.
[86] T. Okamoto and K. Takashima, "Decentralized attribute-based signatures," in *Proc. Int. Workshop Public Key Cryptogr.*, 2013, pp. 125–142.
[87] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 384–394, Feb. 2014.
[88] Y. S. Rao and R. Dutta, "Efficient attribute-based signature and signcryption realizing expressive access structures," *Int. J. Inf. Secur.*, vol. 15, no. 1, pp. 81–109, Feb. 2016.
[89] Q. Huang, Y. Yang, and M. Shen, "Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing," *Future Gener. Comput. Syst.*, vol. 72, pp. 239–249, Jul. 2017.
[90] ABC4Trust. (2018). *ABC4Trust*. [Online]. Available: https://abc4trust.eu/
[91] B. C. Ghosh, S. K. Addya, A. Satpathy, S. K. Ghosh, and S. Chakraborty, "Towards a democratic federation for infrastructure service provisioning," in *Proc. IEEE Int. Conf. Services Comput. (SCC)*, Jul. 2019, pp. 162–166.
[92] I. Sukhodolskiy and S. Zapechnikov, "A blockchain-based access control system for cloud storage," in *Proc. IEEE Conf. Russian Young Res. Electr. Electron. Eng. (EIConRus)*, Jan. 2018, pp. 1575–1578.
[93] K. Bendiab, N. Kolokotronis, S. Shiaeles, and S. Boucherkha, "WiP: A novel blockchain-based trust model for cloud identity management," in *Proc. IEEE 16th Int. Conf. Dependable, Autonomic Secure Comput., 16th Int. Conf. Pervasive Intell. Comput., 4th Int. Conf Big Data Intell. Comput. Cyber Sci. Technol. Cong. (DASC/PiCom/DataCom/CyberSciTech)*, Aug. 2018, pp. 724–729.
[94] S. Banerjee, S. Bouzefrane, and A. Abane, "Identity management with hybrid blockchain approach: A deliberate extension with federated-inverse-reinforcement learning," in *Proc. IEEE 22nd Int. Conf. High Perform. Switching Routing (HPSR)*, Jun. 2021, pp. 1–6.
[95] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," *Sovrin Found.*, vol. 29, p. 18, Sep. 2016.
[96] *GAIA-X*. Accessed: Mar. 22, 2023. [Online]. Available: https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html
[97] GAIA-X. (2022). *GAIA-X Secure and Trustworthy Ecosystems With Self Sovereign Identity*. [Online]. Available: https://gaia-x.eu/wp-content/uploads/2022/06/SSI_White_Paper_Design_Final_EN.pdf
[98] *European Self Sovereign Identity Framework Laboratory*. Accessed: May 22, 2023. [Online]. Available: https://cordis.europa.eu/project/id/871932/results
[99] IDunion. *Self Sovereign Identity*. Accessed: May 22, 2023. [Online]. Available: https://idunion.org/projekt/?lang=en
[100] SWITCH. *Self-Sovereign Identity*. Accessed: May 22, 2023. [Online]. Available: https://www.switch.ch/export/sites/default/about/innovation/.galleries/files/SWITCHInnovationLab_IDAS.pdf
[101] Findy. *Decentralised Identity Ledger*. Accessed: May 22, 2023. [Online]. Available: https://findy.fi/
[102] TransCelerate BioPharma. *eConsent*. Accessed: May 22, 2023. [Online]. Available: https://www.transceleratebiopharmainc.com/assets/econsent-solutions/what-is-econsent/
[103] Microsoft. *Microsoft Entra Verified ID*. Accessed: May 22, 2023. [Online]. Available: https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-verified-id
[104] R. Ismail, "Enhancement of online identity authentication though blockchain technology," Malaysia, Tech. Rep., 2017. Accessed: May 22, 2023. [Online]. Available: https://www.dappleworks.com/assets/files/oia-blockchain.pdf
[105] M. Ali, R. Shea, J. Nelson, and M. J. Freedman, "Blockstack: A new internet for decentralized applications," Tech. White Paper, Version 1, 2017. Accessed: May 15, 2023. [Online]. Available: https://pdos.csail.mit.edu/6.824/papers/blockstack-2017.pdf
[106] S. Wang, R. Pei, and Y. Zhang, "EIDM: A Ethereum-based cloud user identity management protocol," *IEEE Access*, vol. 7, pp. 115281–115291, 2019.
[107] L. R. Maciel and V. Dhakal, "Applying AI concepts for identity and access management in cloud environments," NYU Tandon School Eng., New York Univ., Tech. Rep., 2020. [Online]. Available: https://agyacorp.com/Applying%20Artificial%20Intelligence%20Concepts%20for%20Identity%20and%20Access%20Management%20in%20Cloud%20Environments.pdf
[108] I. Azhar, "A significance of identity management as a prerequisite for enterprise AI on the cloud," *Int. J. Creative Res. Thoughts*, vol. 9, no. 8, pp. b16–b19, 2021.
[109] I. Mohammed, "The interaction between artificial intelligence and identity and access management: An empirical study," *Int. J. Creative Res. Thoughts*, vol. 3, no. 1, pp. 668–671, 2015.

[110] P. M. Khilar, V. Chaudhari, and R. R. Swain, "Trust-based access control in cloud computing using machine learning," in *Cloud Computing for Geospatial Big Data Analytics: Intelligent Edge, Fog and Mist Computing*. 2019, pp. 55–79.
[111] J. Blue, J. Condell, T. Lunney, and E. Furey, "Bayesi-chain: Intelligent identity authentication," in *Proc. 29th Irish Signals Syst. Conf. (ISSC)*, Jun. 2018, pp. 1–6.
[112] H. Xiong, H. Zhang, and J. Sun, "Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2739–2750, Sep. 2019.
[113] R. V. Rao, K. Selvamani, S. Kanimozhi, and A. Kannan, "Hierarchical group key management for secure data sharing in a cloud-based environment," *Concurrency Comput., Pract. Exp.*, vol. 31, no. 12, Jun. 2019, Art. no. e4866.
[114] B. Cui, Z. Liu, and L. Wang, "Key-aggregate searchable encryption (KASE) for group data sharing via cloud storage," *IEEE Trans. Comput.*, vol. 65, no. 8, pp. 2374–2385, Aug. 2016.
[115] *GÉANT*. Accessed: May 22, 2023. [Online]. Available: https://geant.org/
[116] *InCommon*. Accessed: May 22, 2023. [Online]. Available: https://www.incommon.org/
[117] Elixir. *Federated Identity*. Accessed: May 22, 2023. [Online]. Available: https://www.elixir-finland.org/en/tag/federated-identity/

AYTAJ BADIROVA received the bachelor's degree in information technology and systems engineering from Baku Engineering University, and the master's degree in applied computer science from the University of Göttingen, where she is currently pursuing the Ph.D. degree in computer science, researching new ways of identity and access management, specifically decentralized identity management. She is an Employee of the IT service provider company Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG) and has an experience on different projects, including international collaborative research projects.

SHIRIN DABBAGHI received the master's degree in distributed systems from the University of Putra Malaysia, in 2014. She is currently pursuing the Ph.D. degree with the University of Göttingen, where she is conducting research aimed at enhancing trust and security in federated identity management. She is an Identity and Access Management (IAM) Developer with GWDG, where she develops and maintains a variety of extensions to meet specific IAM needs of various national and international IAM projects while also addressing day-to-day issues.

FARAZ FATEMI MOGHADDAM received the B.Sc. degree in computer science from the Azad University of Tehran, the M.Sc. degree from Staffordshire University, and the Ph.D. degree in security and policy management in clouds from the University of Göttingen. He is currently a Senior Cyber Security Manager with Hartmann Group, as well as a Guest IT Security Researcher with Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG) and a Lecturer with HAWK (University of Applied Sciences and Arts), Göttingen. He has been involved in several German and European projects. His research interests include potential security and privacy challenges in cloud computing and modern distributed networks, such as data protection, access management, user authentication, and cryptography.

PHILIPP WIEDER received the Ph.D. degree from TU Dortmund, Germany. He is currently the Deputy Leader of datacenter with Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen, University of Göttingen, Germany. He has been actively involved in the FP7 IP PaaSage, SLA@SOI, and SLA4D-Grid projects. He is active in the research areas on clouds, grids, and service-oriented infrastructures for several years. His research interests include distributed systems, service-level agreements, and resource scheduling.

RAMIN YAHYAPOUR received the Ph.D. degree in electrical engineering. He was a Professor with Technische Universität Dortmund. He is currently the Managing Director of GWDG, a joint compute and IT competence center of the university and the Max Planck Society. GWDG is a national supercomputing and AI service center. He is also a Full Professor of practical computer science with the Georg August University of Göttingen. He was and is active in several national and international research projects. His research interests include high-performance computing, scheduling, cloud computing, resource management, data-intensive computing, data analytics, and parallel computing. He is an organizer and a program committee member of several conferences and workshops, as well as a reviewer of multiple journals. He regularly serves as a reviewer for funding agencies and a consultant for IT organizations.