International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.4 (2025) pp. 4440-4447
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Scalable Identity and Access Management Frameworks for Hybrid and Multi-Cloud Platforms

Dinesh Kollu*

Sikkim Manipal University, Gangtok, Sikkim, India.
* **Corresponding Author Email:** dkollu50@gmail.com - **ORCID:** 0000-0002-5247-9950

Article Info:

DOI: 10.22399/ijcesen.5144
Received : 01 March 2025
Revised : 25 March 2025
Accepted : 30 March 2025

Keywords

Identity and Access Management;
Hybrid Cloud;
Multi-Cloud Security;
Zero Trust Architecture;
Access Control Models

Abstract:

The development of hybrid and multi-cloud computing has a high rate of adoption and has had a paradigm shift on the IT infrastructure of the enterprise, making it scaled, flexible, and resilient. Nonetheless, this change has come with critical issues of controlling identities and access in the heterogeneous and distributed settings. Identity and Access Management (IAM) is a very vital element in the process of securing the cloud resources because the systems are only accessed by authorized parties with certain condition. Most of the traditional IAM models that were created with centralized backgrounds are not sufficient in cutting across the complexities of the multi domain cloud ecosystems. This paper will give an overview of scalable IAM frameworks on hybrid and multi-cloud systems. It discusses the development of the IAM architectures, such as centralized, federated, and decentralized models, and the suitability of those in the distributed cloud environment. The paper also examines access control models like Role-Based Access Control (RBAC),Attribute-Based Access Control (ABAC) and policy-based models with emphasis on their advantages and shortcomings in the provision of fine-grained and scalable authorization. Also, the paper addresses how Zero Trust Architecture (ZTA) and cloud-native IAM practices can be integrated, focusing on the continuity of authentication, least privilege access, and workload identity policy. The main issues like the interoperability, identity sprawl, policy inconsistency, and performance overhead are deeply examined. There are also investigations of emerging trends, such as identity decentralization and IAM based on AI. The results show that there is no one IAM model which can meet the needs of hybrid and multi-cloud environment. Rather, it is a mix of federated approaches, policy-oriented approaches, and approaches based on Zero Trust, which is needed to ensure scalability and security. The review gives us an idea of the current studies, and future expectations of coming up with an unified and adaptive IAM frameworks.

1. Introduction

Application of cloud computing has significantly changed how organizations manage the digital resources whereby it can access infrastructure, platforms and services on a scale and on demand basis. In the recent years, businesses are migrating to hybrid or multi-cloud applications rather than single-cloud applications in a bid to achieve a higher degree of flexibility, vendor lock-in, and resiliency. However, this transition poses serious issues of identity control and access control on the heterogeneous platforms and, in turn, Identity and Access Management (IAM) is a crucial component of the modern cloud security design [1].In some circumstances, IAM secures the entry of particular resources to the approved users, applications, and services. The IAM systems which were old were designed to become central and relatively stable yet the hybrid and multi-clouds ecosystems are distributed, dynamic, and multi-domain in nature. This therefore means that the conventional IAM models face interoperability, identity federation, and policy inconsistency and scalability across cloud providers [2]. They are also exacerbated by the increasing number of identities not only of human users, but also machine identities, such as API, containers, and microservices. To overcome such limitations, the current IAM frameworks have developed and integrated federated identity management, attribute-based access control (ABAC), and decentralized identity to facilitate

convenient authentication and authorization of identities across domains [3]. SAML, Oauth and OpenID connect are federated identity standards that enable single identity to be used by a user to access many cloud services enhancing user friendly applications without compromising the security. Simultaneously, the decision of access in ABAC is fine-grained and context sensitive which is more appropriate in dynamic cloud settings than traditional role-based models. Further recently, IAM design principles were once again remodeled by the rise of Zero Trust Architecture (ZTA). The concept of zero trust works according to the belief that one should not trust anything, and it is time to verify that active authentication is applied, the least-needed access is used and risk is evaluated constantly no matter where it is placed within the network [4]. This paradigm is applicable to hybrid and multi-cloud contexts and perimeter-based security frameworks are not applicable.In spite of these developments, scalable and multi-cloud environments have become an open research problem. Companies have to strike the right balance between security and controlling the lifecycles of identities to different cloud ecosystems [5]. Therefore, the general study of the scalable IAM frameworks is required to study about the current approaches, identify limitations, and identify novel approaches to research. The scalable hybrid and multi-cloud platform and scalable IAM frameworks are presented and reviewed based on the architectural model, access control, and the new paradigm of Zero Trust and decentralized identity.

2. Background: Identity and Access Management in Cloud Environments

IAM of access control to resources by users, applications, and services is one of the most important cloud security pillars. In cloud, IAM involves all identity lifecycle, such as creating identity, dealing with credentials, authentication, authorization and auditing. Due to the rising use of cloud systems, IAM systems must be operated on distributed systems of infrastructure and in this situation, effective access control and mechanisms are required to ensure that the systems offer secure and effective access controls to the systems [6]. Public, private, hybrid multi-cloud models are a common typology and each implies varying IAM need. Hybrid cloud combines on-premise infrastructure and the use of the public cloud services whereas multi-cloud implies the simultaneous use of different cloud service providers. These models make them more difficult since identities and access policies need to be consistently supported at heterogeneous platforms that have varying security models and APIs [7]. Consequently, IAM solutions have to facilitate interoperability and standardization to facilitate easy identity propagation across domains. IAM authentication schemes identify either the identity of users or systems that access resources. Nevertheless, the emergence of cloud-native application demands the increased need of more powerful and responsive authentication methods that should reflect contextual aspects like the device trust, location, and behavior. This has seen the use of federated standards of identity including Security assertion markup language (SAML), OAuth and OpenID connect that allow single sign-on (SSO) across a variety of platforms [8].IAM is based on permission whereby the authenticated entities gain permission to access. Role-Based Access Control is the traditional models, which distribute permissions depending on the built-in roles and are therefore easy and broadly used. RBAC, however, is not flexible in dynamic environments where there are varying access decisions based on the situation attributes. In this regard, a novel approach of making access decisions has been proposed, namely, the Attribute-Based Access Control (ABAC), which makes access decisions depending on user attributes, the environmental conditions, and the characteristics of resources. ABAC offers detailed control to a cost, but it is affected by complex and scalable policy challenges [9].Identity federation is also another facet of IAM in the cloud since identities can be shared between different security spaces. Federation minimizes the requirement of multiple credentials and makes the access management of multi-cloud systems easier. Nonetheless, it poses problematic issues of building trust, identity mappings and coordination of policies among providers. Also, the growing usage of the microservices and containerized apps has created a problem of machine identities that demand scalable and automated IAM solutions in order to secure the service-to-service authentication [10]. On the whole, IAM of hybrid and multi-clouds should strike the right balance between security, scalability, and usability. The types of identities and changing threats demand the creation of new IAM solutions that can be effectively worked with the process.

3. Scalable IAM Architectures for Hybrid and Multi-Cloud Platforms

The growing use of hybrid and multi-clouds has led to a need to design scalable IAM systems that can be used across multiple administrative domains. The conventional centralized IAM systems cannot be used in this type of environment because there is

a lack of interoperability, performance bottlenecks, and single points of failures. Consequently, contemporary IAM designs have been developed to be federated, decentralized and cloud-native IAM designs enabling scalability and cross-domain trust [11].

3.1 The centralized IAM Architectures

Centralized IAM architectures involve having a single identity provider (IDP) which takes care of authentication and authorization of all resources. Although this strategy will ease the management of identities and implementation of policies, it also presents issues of scalability in multi-cloud-based systems where numerous providers and services need to be combined. The use of centralized models is also not as flexible and fast as dealing with workloads that are geographically dispersed [12]. Irrespective of these shortcomings, centralized IAM can be applied to the context of both private and hybrid clouds where strict control and adherence is needed.

3.2 Federated Identity Management

The federated IAM architecture works around the issues experienced by centralized architectures as they are capable of sharing of identities across different domains. This model uses authentication by trusted identity providers and therefore, a user is able to access various services with one identity. The famous technologies to use to perform federation are SAML, OAuth 2.0, and OpenID Connect. Federated identity systems streamline authentication and reduce redundancy in identity storage. They, however, come with their own issues regarding the management of trust, identity mapping, and the synchronization of policies amongst different cloud platforms [13]. Multi-cloud and hybrid environments imply that there is a compulsory need of federation in such a way that providers may be presented without waste of security borders.

3.3 Dispersed and Distributed IAM Models

Decentralized IAM models have been proposed to increase resilience and eliminate central points of failure. These models take advantage of distributed technologies such as blockchain and DIDs to provide identities and trust. Decentralized IAM enhances resilience and privacy because it provides users with more control over their identity information. Nonetheless, there are still obstacles of standardization, overhead of performance and integration with the current enterprise systems [14]. Nevertheless, in spite of these restrictions, decentralized identity is gaining popularity as a possible solution to next-generation multi-cloud IAM systems.

3.4 Workload and Cloud-Native Identity Frameworks

Along with the emergence of microservices, containers, and serverless computing, IAM is also required to work with non-human identities, including applications, services, and workloads. Cloud-native IAM systems are dedicated to automated and scalable techniques of management of such identities. A workload identity federation is one of the emerging techniques where long-term credentials are removed and instead of having long-term credentials, short-term tokens are issued, along with making secure identity exchanges among cloud providers. The approach dramatically helps to decrease the attack surface and increases the scalability within the distributed environment. Also, it can be connected to container orchestration platforms like Kubernetes and provision identity dynamically at scale and implement policies [15] (Table 1, Figure 1).

4. Access Control Models and Enforcement Mechanisms

Identity and Access Management (IAM) inherently include access control as one of its elements, which ensures the way authenticated entities access cloud resources. Access control mechanisms in a hybrid or multi-cloud environment need to aid in scaling, flexibility and fine-grained policy enforcement of distributed systems. The conventional models are good in a fixed environment but must be adjusted to suit the dynamism of the cloud platform [16]. RBAC refers to the concept of assigning role access permissions to groups of people.

4.1 Role-Based Access Control (RBAC)

The most adapted access control model is the Role-Based Access Control (RBAC) because it is the simplest and easy to manage. With RBAC, a role is given permissions and a user is assigned to that role, this ensures that there is less work in administration. The model is especially applicable in organisations that have clear job roles. But in the hybrid and multi-cloud environments, RBAC is limited to dynamic and context-aware access controls. RBAC is challenging to scale and support due to the explosion of roles in large-scale systems, which is also commonly termed as role explosion. Moreover, the concept of RBAC does not allow

flexibility to include contextual properties like time, location, or device trust [16].

4.2. Attribute-Based Access Control (ABAC)

ABAC builds on the existing access control framework with the distinction that access-requests are considered as per various attributes such as attributes related to the user, environmental factors, and properties of the resource. This facilitates sharp and contextual decision making that is indispensable to distributed cloud-environment. ABAC also fits quite well into hybrid systems and multi-cloud systems due to the fact that it can dynamically enforce the policies on the various platforms. Nevertheless, greater flexibility of ABAC comes with problems that pertain to policy complexity, performance overhead, and governance particularly dealing with large sets of attributes [17].

4.3 Policy-Based and Hybrid AAM Model

The shortcomings of RBAC and ABAC have led to a situation where today IAM systems are adopting hybrid models of access control, which intersect role-based and attribute-based models. Access control frameworks involving policy-based access control, including tools based on the eXtensible Access Control Markup Language (XACML) offer a uniform methodology to grant and deny access policy to the distributed systems. Centralized policy definition but decentralized implementation is possible, thus, the models can be applied in multi-clouds. Nonetheless, there are still some issues associated with the maintenance of policy consistency, interoperability, and effective evaluation of heterogeneous platforms [17].

4.4 Access Control using Encryption

Cryptographic solutions, including the Attribute-Based Encryption (ABE) tool, have also been developed as useful ways to implement access control when using cloud-based solutions. ABE gives access control and encryption by enabling encrypted data on access policies which given access is only by authorized users. This will increase the level of data security especially in outsourced and multi-tenant settings. Nevertheless, ABE adds computational overhead and complexity on key management, which can affect the performance of large systems [18] (Figure 2).

5. Zero Trust and Modern IAM for Cloud-Native Platforms

The growing cost of hybrid and multi-cloud environments has accelerated the application of the Zero Trust Architecture (ZTA) as the new paradigm of the modern Identity and Access Management (IAM). In contrast to the traditional security models which are based on the use of the perimeter-based security, the zero trust approach presupposes that none of the entities must be trusted, either, inside or outside of the network. Rather, any access request should be constantly checked in terms of its identity, situation, and risk factors. This paradigm shift comes in especially with distributed cloud environments whereby resources are accessed at a variety of sites and in various administrative domains [19].The main thing about Zero trust is that the concept of IAM evolves to emphasize more on continuous authentication and authorization rather than authentication that occurs once. This is a model where identity is the center of security management and the decision of access is dynamically evaluated by considering contextual (user behavior, device posture and the environment) information. This solution will make it more secure as least-privilege access is a requirement and the risk of unauthorized access is reduced in case of credentials breach. Since cloud-native applications are becoming increasingly dependent on microservices and API-based applications, Zero Trust provides each interaction to be authenticated and authorized separately, thus limiting lateral movement within systems [20].Another applicable trend in the history of the modern IAM is the process of the appearance of the augmented role of machine and workload identities. A massive portion of interactions in the clouds native environments occur between the services and not between the human beings. Some of these machine identities that require secure and scalable authentication solutions include containers, serverless functions and microservices. The traditional credential-based systems such as the static API keys cannot be trusted since they can be leaked and misused. In order to cope with such challenges, recent IAM systems provide temporary credentials, automatic identity generation, and secured service to service authentication links [19]. Integration of Zero Trust principles with IAM has also led to introduction of the policy-based and contextual access control. Policies are increasingly being written in a more declarative fashion, also called policy-as-code, and giving companies a uniform application of access control to a diverse range of cloud environments. Such policies will be evaluated in real-time basis thereby making adaptive access decisions based on the risk evaluation. These are imperative methods of maintaining security and compliance of the dynamic environment where the users and

resources are ever varying [20]. In addition, the contemporary IAM solutions are adopting intelligent and adaptive functionalities with the application of artificial intelligence and machine learning. These technologies enable the capability of detecting an irregularity, analysis of behavior and automatic reaction that will enhance the detection and prevention of security threats in real time. With a combination of the principles of the Zero Trust and insights provided by AI, IAM frameworks will become more scalable, efficient, and resilient to mixed and multi-cloud systems [21].Although this has been achieved, there are various challenges to implementation in practice of Zero Trust IAM. The challenge that organizations have to concern is related to integrating it with legacy systems, performance overhead due to the endless verification, and the challenge of having to work with various environments and policies. However, Zero Trust is a severe trajectory of the development of IAM, a potent groundwork of securing the current cloud environments (Figure 3).

6. Challenges and Limitations

It have been considerable progress in the Identity and Access Management (IAM) models of hybrid and multi-cloud environments, there are some serious challenges and constraints. Interoperability between heterogeneous cloud platforms is one of the most significant problems. All cloud service providers have their own IAMs, APIs, and identity models, so it is hard to make them interoperable with each other and have a standard way of enforcing policies. Such non-standardization makes the federation of identities harder and the chances of misconfigurations more likely, a major source of security breaches in the cloud systems [22]. The identity sprawl is another issue which is mainly fuelled by the increase of both human and machine identities that are fast proliferating. With the increased use of microservices, containers, and serverless, identities in the organizations are increasing exponentially, which increases the complexity of identity lifecycle management. Such growth causes the inability to sustain visibility, least-privileged access, and timely revocation of credentials, which escalates the attack surface [23]. Other issues are policy control and uniformity. There is an intrinsic tendency to enforce similar access control policies on various platforms in a multi-cloud environment, as there is a variation between policy languages and even enforcement mechanisms. Policy-as-code methods in any form still need rich orchestration mechanisms to provide real-time syncing between policies and prevent conflicting policies [24]. The performance overhead of the continuous authentication and authorization is also limiting with regards to scalability, especially in Zero Trust architectures. Although the benefits of continuous verification is that it increases security, it also creates latency and computational overhead, which might impact system performance, particularly in large-scale distributed systems with high traffic rates [25].

The other drawback is the management of trust in certain areas. It cloud providers and identity domains and so in federated IAM systems. The functions of trust anchors, certificate management and identity mapping should be well handled to prevent vulnerabilities and provide secure communication [26]. The sensitivity of identity data frequently contains personal and organizational information that is hard to obtain and, therefore, is susceptible to cyberattacks. To facilitate the meeting of regulatory requirements, including GDPR, the foundation of data protection mechanism and maintaining identity storage, is necessary [27]. Also, there is practical challenge in integrating IAM and legacy systems. Hybrid organizations have environments that will contain old infrastructure that is not made with the current IAM systems, and which will result in compatibility problems and raised implementation expenses [28]. New devices like decentralized identity and AI-driven IAM seem to open new opportunities but also have their uncertainties, which are issues of standardization, governance, and ethics. The absence of developed standards and broad usage reduce their usability in the enterprise space in the short term [29], [30] (Table 2).

Table 1. *Comparison of IAM Frameworks in Hybrid and Multi-Cloud*

Framework Type	Core Concept	Strengths	Limitations	Scalability Suitability	Typical Technologies / Standards
Centralized IAM	Single identity provider manages all identities and policies	Simple management, strong control, easier auditing	Single point of failure, poor cross-cloud scalability	Low–Medium	LDAP, Active Directory
Federated IAM	Identity shared	Enables SSO,	Complex trust	High	SAML, OAuth

	across domains using trust relationships	reduces credential duplication	management, identity mapping issues		2.0, OpenID Connect
Decentralized IAM	User-controlled identity without central authority	Improved privacy, eliminates central dependency	Lack of standards, integration complexity	Medium (emerging)	Blockchain, DIDs
RBAC-based IAM	Access based on predefined roles	Simple, widely adopted, easy to implement	Role explosion, lacks flexibility	Medium	RBAC models
ABAC-based IAM	Access based on attributes and context	Fine-grained, dynamic decision-making	Complex policies, high computation cost	High	ABAC, XACML
Policy-Based IAM	Central policy definition with distributed enforcement	Flexible, scalable across clouds	Policy conflicts, synchronization challenges	High	XACML, Policy-as-Code
Zero Trust IAM	Continuous verification with no implicit trust	Strong security, least privilege enforcement	Performance overhead, implementation complexity	High	ZTA, MFA, SIEM
Workload Identity IAM	Identity for services, APIs, containers	Scalable for cloud-native systems	Complex automation, lifecycle management	Very High	Kubernetes, OIDC, JWT

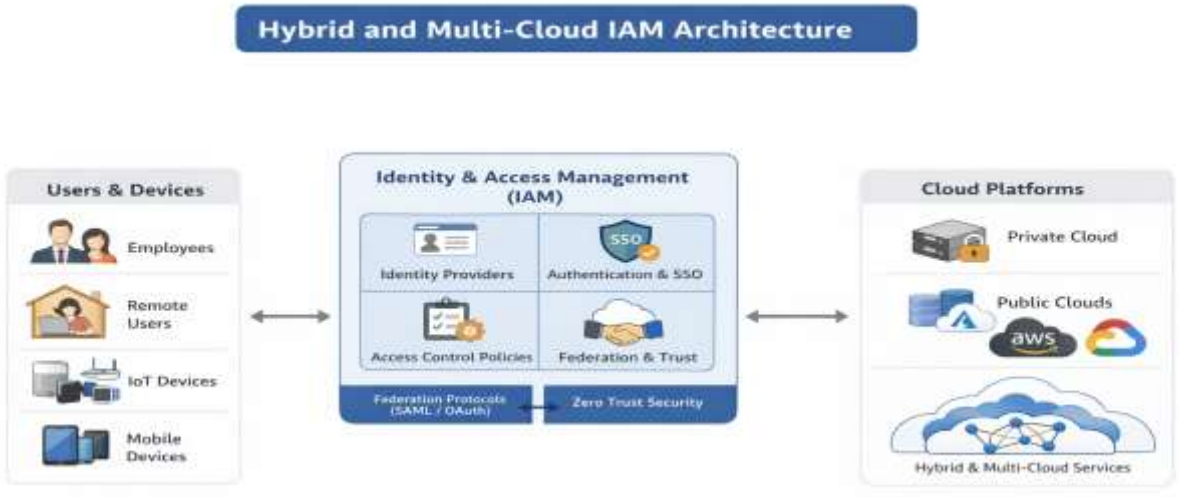

Figure 1. *Hybrid and Multi-Cloud IAM Architecture.*

Table 2: *Summary of Selected Studies*

Focus Area	Environment	Key Contribution	Limitation
Federated IAM	Multi-domain systems	Introduced federated identity concepts	Limited scalability discussion
Token-based authentication	Multi-cloud	JWT enables lightweight identity exchange	Token security risks
Decentralized identity	Distributed systems	Proposed self-sovereign identity model	Lack of enterprise adoption
Cloud-native IAM	Kubernetes	Workload identity management	Operational complexity
RBAC	Enterprise systems	Standard RBAC model	Poor flexibility
Policy-based IAM	Distributed cloud	Standardized XACML policies	Complexity in deployment
ABE encryption	Cloud storage	Fine-grained encrypted access	High computational cost
Zero Trust	Enterprise networks	Introduced Zero Trust concept	Initial lack of tools
Zero Trust IAM	Cloud-native	Practical ZTA implementation	Integration challenges
Cloud IAM risks	Multi-cloud	Highlighted misconfiguration	Not technical framework

		risks	

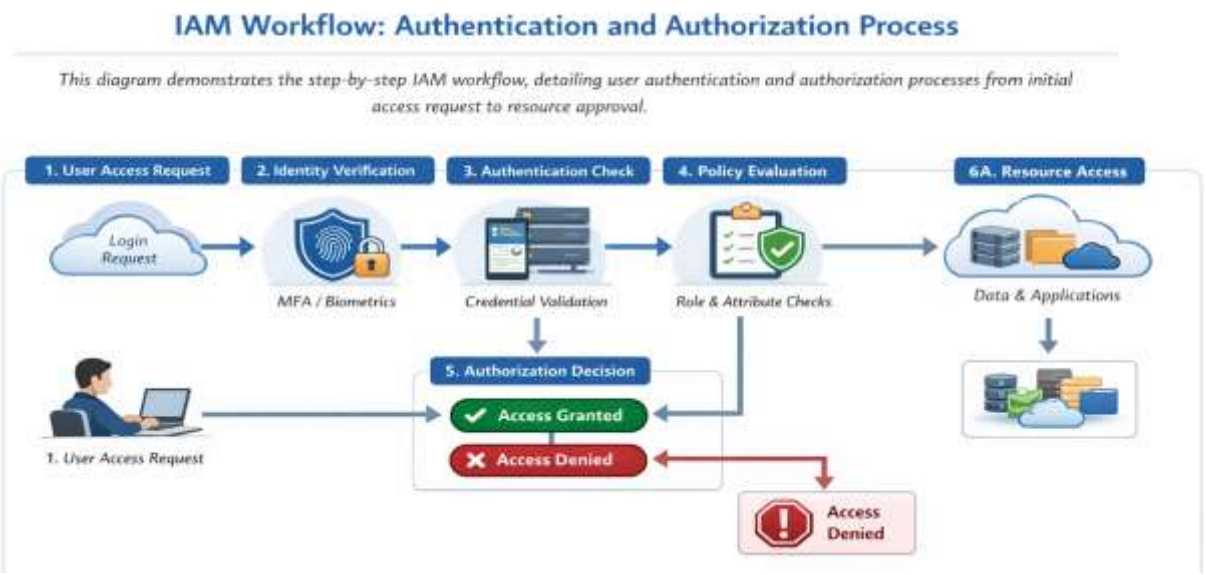

Figure 2. *IAM Workflow for Authentication and Authorization in Hybrid and Multi-Cloud Environments.*

Figure 3. *Evolution of IAM Architectures from Traditional to Zero Trust and Cloud-Native Models.*

7. Conclusions

The current paper has examined scalable IAM for hybrid and multi-cloud systems, noting how the century-old centralized models have been transformed into decentralized and federated models along with the Zero Trust-based models. It was shown that the analysis level of modern cloud environment needs IAM solutions, which can serve dynamic, distributed, and multi-domain infrastructure. Although federated identity and attribute-based access control has a strong advantage of flexibility and interoperability, it also has policy management and trust establishment issues. ZTA increases security validation and minimum access privilege. Other limitations that were also noted in the study are the problem of interoperability, identity proliferation, and the lack of scalability problems in large scale systems. New technologies are also promising, including decentralized identity and AI-assisted IAM which need to be further standardized and tested. All in all, the implementation of scalable and security IAM in hybrid and multi-cloud settings requires cohesive and responsive and policy-based frameworks that ease security, usability, and effectiveness.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

- **Use of AI Tools:** The author(s) declare that no generative AI or AI-assisted technologies were used in the writing process of this manuscript.

References

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," *NIST Special Publication 800-145*, National Institute of Standards and Technology, 2011.

[2] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "How to enhance cloud architectures to enable cross-federation," *IEEE International Conference on Cloud Computing*, 2010, pp. 337–345.

[3] D. Hardt, "The OAuth 2.0 Authorization Framework," *IETF RFC 6749*, 2012.

[4] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," *NIST Special Publication 800-207*, 2020.

[5] E. Bertino and N. Islam, "Botnets and internet of things security," *Computer*, vol. 50, no. 2, pp. 76–79, 2017.

[6] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, "Role-based access control models," *IEEE Computer*, vol. 29, no. 2, pp. 38–47, 1996.

[7] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Computer Systems*, vol. 25, no. 6, pp. 599–616, 2009.

[8] S. Cantor et al., "Assertions and protocols for the OASIS Security Assertion Markup Language (SAML) V2.0," *OASIS Standard*, 2005.

[9] V. C. Hu, D. Ferraiolo, and D. Kuhn, "Assessment of access control systems," *NIST Interagency Report 7316*, 2006.

[10] J. M. Bishop, "Computer Security: Art and Science," Addison-Wesley, 2003.

[11] D. Chadwick, G. Inman, K. W. Chappell, and S. M. Otenko, "Federated identity management," *Computer*, vol. 42, no. 5, pp. 120–122, 2009.

[12] S. Pearson and A. Benameur, "Privacy, security and trust issues arising from cloud computing," *2010 IEEE Second International Conference on Cloud Computing Technology and Science*, pp. 693–702, 2010.

[13] M. Jones, J. Bradley, and N. Sakimura, "JSON Web Token (JWT)," *IETF RFC 7519*, 2015.

[14] C. Allen, "The path to self-sovereign identity," *Life With Alacrity Blog*, 2016.

[15] K. Hightower, B. Burns, and J. Beda, *Kubernetes: Up and Running*, O'Reilly Media, 2017.

[16] D. F. Ferraiolo, D. R. Kuhn, and R. Chandramouli, *Role-Based Access Control*, Artech House, 2003.

[17] OASIS, "eXtensible Access Control Markup Language (XACML) Version 3.0," *OASIS Standard*, 2013.

[18] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," *Proceedings of the 13th ACM Conference on Computer and Communications Security*, 2006, pp. 89–98.

[19] J. Kindervag, "Build security into your network's DNA: The Zero Trust Network Architecture," *Forrester Research*, 2010.

[20] R. Gilman and J. Barth, "Zero Trust Networks," *O'Reilly Media*, 2017.

[21] E. Bertino, "Data security and privacy in the IoT," *Proceedings of the 19th International Conference on Extending Database Technology (EDBT)*, 2016, pp. 1–2.

[22] Gartner, "Is the cloud secure? Misconfigurations are the biggest risk," Gartner Research, 2019.

[23] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[24] T. Moses, "eXtensible Access Control Markup Language (XACML) Version 2.0," *OASIS Standard*, 2005.

[25] S. Z. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661–2674, 2013.

[26] N. Li, B. N. Grosof, and J. Feigenbaum, "Delegation logic: A logic-based approach to distributed authorization," *ACM Transactions on Information and System Security*, vol. 6, no. 1, pp. 128–171, 2003.

[27] A. Cavoukian, "Privacy by design: The 7 foundational principles," Information and Privacy Commissioner of Ontario, 2009.

[28] P. R. P. J. Bonatti and D. Olmedilla, "Rule-based policy representation and reasoning for the semantic web," *Lecture Notes in Computer Science*, vol. 3761, pp. 240–268, 2005.

[29] D. Reed, J. Sporny, D. Longley, C. Allen, R. Grant, and M. Sabadello, "Decentralized identifiers (DIDs) v1.0," *W3C Working Draft*, 2020.

[30] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, 2016.