ISSN 2635-8875 / e-ISSN 2672-0124
DOI : https://doi.org/10.22678/JIC.2023.21.12.037

Research on User-Centric Inter-Organizational Collaboration (UCICOIn) framework

Sunghyuck Hong*
Professor, Division of Advanced IT, IoT major, Baekseok University

사용자 제어 기반 다중 도메인 접근 제어에 대한 연구

홍성혁*
백석대학교 첨단IT학부, IoT 전공 교수

Abstract In today's business landscape, collaboration and interoperability are crucial for organizational success and profitability. However, integrating operations across multiple organizations is challenging due to differing roles and policies in Identity and Access Management (IAM). User-centric identity (UCI) adopts a personalized approach to digital identity management, centering on the end-user for authentication and access control. It provides a decentralized system that ensures secure and customized access for each user. UCI aims to address complex security challenges by aligning access privileges with individual user requirements. This research delves into UCI's ability to streamline resource access amidst conflicting IAM roles and protocols across various organizations. The study presents a UCI-based multi-domain access control (MDAC) framework, which encompasses an ontology, a unified method for articulating access roles and policies across domains, and software services melding with UCI infrastructure. The goal is to enhance organizational resource management and decision-making by offering clear guidelines on access roles and policy management across diverse domains, ultimately boosting companies' return on investment.

Key Words : Collaborative business processes, Identity and Access Management (IAM), User-controlled identity (UCI), Multi-domain access control, Prototype integration

요 약 현대의 비즈니스 환경에서는 협업과 상호 운용성이 조직의 성공과 수익성에 있어 중요하다. 그러나 다양한 조직 간의 작업 통합은 Identity and Access Management (IAM)의 역할과 정책의 차이로 인해 많은 커스터마이징이 필요하다. 사용자 중심의 신원 (UCI)은 사용자를 중심으로 한 분산 액세스 솔루션을 제공하여 이러한 문제를 해결할 수 있다. 이 연구는 다양한 조직 간의 IAM 역할 및 프로토콜의 충돌 속에서 자원 액세스를 간소화하는 UCI의 능력을 깊게 조사한다. 이 연구는 UCI 기반의 다중 도메인 액세스 제어 (MDAC) 프레임워크를 제시하며, 이는 온톨로지, 도메인 간의 액세스 역할 및 정책을 표현하기 위한 통합된 방법, 그리고 UCI 인프라와 통합되는 소프트웨어 서비스를 포함한다. 목표는 다양한 도메인에서의 액세스 역할 및 정책 관리에 대한 명확한 지침을 제공함으로써 조직의 자원 관리와 의사 결정을 강화하고, 궁극적으로 기업의 투자 수익률을 향상시키는 것이다.

키워드 : 협력적 비즈니스 프로세스, 아이덴티티 및 접근 관리, 사용자 제어 신원, 다중 도메인 접근 제어 (MDAC), 프로토타입 통합

This research was supported by 2023 Baekseok University Research Fund.
*Corresponding Author : Sunghyuck Hong(sunghyuck.hong@gmail.com)
Received October 23, 2023 Revised December 6, 2023
Accepted December 20, 2023 Published December 28, 2023

1. Introduction

Modern business is deeply intertwined with multi-domain collaboration, such as shared workflows and data across different organizations. Enterprise systems, equipped with IAM (Identity and Access Management), centralize user credential storage and manage access through specific roles and policies.

- Overcoming the complexity of multi-domain collaboration: In a modern business environment where collaboration and data sharing between multiple organizations are essential, the goal is to find ways to overcome the limitations of the IAM system.
- Leveraging the benefits of User-Controlled Identity (UCI): Overcoming the limitations of traditional IAM systems and leveraging the potential of UCI to facilitate cross-organizational access without the need for user duplication or a centralized IdP (Identity Provider). Explore.
- Analysis of RBAC (Role-Based Access Control): Analyzes the basic concepts, pros and cons of RBAC systems widely used in current organizations.
- UCI-based framework proposal: We propose a lightweight server architecture based on UCI, along with ontology guidelines for Internet and inter-organizational security policies.
- Real-World Case Study: Demonstrates the use of the framework based on a real-world example from an Original Equipment Manufacturer (OEM).
- Theoretical contribution: We deepen the academic understanding of this field by presenting a new methodology to solve IAM problems in a multi-domain environment.
- Practical Contribution: Through a UCI-based access control framework that integrates with existing IAM systems, we provide a concrete solution to improve collaboration and efficiency in real business environments.
- Improved security and efficiency: Compared to centralized systems, UCI enhances security and reduces management overhead through easy revocation of user access and reduced need for centralization.

The problem with setting and customizing research goals is that the complexity of multi-domain environments and synchronization issues between policies and roles in various organizations may not be sufficiently considered. In particular, developing an integrated approach that encompasses each organization's unique security requirements and processes can be very challenging. This clearly defines the scope and purpose of the study and takes into account the needs and constraints of various organizations.

Traditional IAM systems struggle with inter-organizational access, requiring either user replication or third-party Identity Providers (IdPs), leading to security risks and administrative burdens. UCI (User-controlled identity), through Verifiable Credentials (VC), offers decentralized identity management, enabling smoother inter-organizational access without the need for user replication or centralized IdPs.

UCI allows for the easy revocation of user access and does not require centralization, enhancing security and reducing administrative overhead. However, it necessitates formal guidelines for integrating access policies for shared resources.

2. Theoretical Background

At the core of modern business ecosystems, multi-domain collaboration is ubiquitous, encompassing inter-organizational workflows, cross-boundary business processes, and access to data owned by partner entities. Central to these operations are enterprise software systems, which implement robust Identity and Access Management (IAM) frameworks to safeguard data access. These frameworks are anchored in centralized architectures where user credentials and access policies are meticulously curated based on security and privacy mandates.

However, this centralization presents significant hurdles when adapting to a multi-domain context, where cross-organizational resource sharing and access require intricate coordination and pose heightened security risks. The IAM systems must overcome these challenges of scalability, interoperability, and synchronization to enable seamless inter-organizational collaboration.

3. Role-Based Access Control (RBAC)

3.1 Basic concept

- Role: In RBAC, a role is an abstract representation of a specific duty or responsibility. For instance, roles such as “Administrator”, “User”, and “Auditor” might exist.
- User: Refers to an individual or entity accessing the system.
- Permission: Denotes the authority to access or operate on a specific resource.
- DID: It refers to a system where individuals or devices manage and verify their identity through a distributed network, rather than a centralized authority. RBAC refers as DID concept in recent years.
- Role Assignment: A user can be assigned to one or more roles. For instance, a user named “John” might be assigned the role of “Administrator”.
- Permission Assignment: Each role is allocated specific permissions. For example, the “Administrator” role might possess the authority to modify the database.
- Access Decision: A user's request is determined based on the role of that user and the permissions assigned to that role.

3.2 Advantages

- Flexibility: Even if a user changes roles within the organization, only the permissions associated with that role need to be modified. There's no need to adjust individual user permissions.
- Efficiency: In large-scale organizations, there might be a need to manage hundreds or thousands of users. RBAC simplifies permission management, reducing administrative overhead.
- Enhanced Security: Following the principle of least privilege, users can be granted only the permissions they need. This reduces security threats.

3.3 Disadvantages

- Initial Setup Complexity: The process of defining and assigning roles and permissions initially can be intricate.
- Limitations in Dynamic Environments: In environments where roles and permissions frequently change, the flexibility of RBAC might be limited.

RBAC serves as an access control approach that aids in reducing the complexity of security management and enhancing efficiency, widely adopted by numerous organizations and enterprises. However, to grant and manage permissions for a diverse set of external users, solely relying on RBAC can be challenging. As a result, the OAuth approach is becoming increasingly popular [7-8, 14-15].

In this paper, we propose the User-Centric Inter-organizational Collaboration (UCICOIn) framework to overcome some of the challenges mentioned in the current research. Specifically, UCICOIn contributes to enhancing inter-organizational collaboration by:

- Guiding the creation of inter-organizational security policies through ontology.
- Representing clear mappings between users, roles, and resources using inter-organizational security policy notations.
- Offering a lightweight, reusable server architecture based on UCI for secure access to inter-organizational resources.

- Demonstrating the framework's usage through an empirical case study based on real-use cases from Original Equipment Manufacturers (OEM).

3.4 Multi-Domain Access Control (MDAC)

Multi-Domain Access Control (MDAC) refers to security mechanisms and policies designed to manage access rights and permissions across different domains or areas within an information technology environment. This is particularly important in complex systems where resources are distributed over different network segments, organizational units, or even across different organizations.

4. Centralized Identity Management vs. Distributed Identifier

Centralized Identity Management is a system where a single institution manages all user identity information. Characteristics of a centralized identity system include [9]:

- Single Data Repository: All users' identity information is stored in one central database.
- Central Management: User identity information is managed by a central administrator.
- Single Authentication: Users can log into multiple web applications using a single central ID.

Distributed Identity is a system where multiple institutions share user identity information. Characteristics of federated identity systems include:

- Distributed Data Storage: Users' identity information is stored across databases of various institutions.
- Collaboration: Multiple institutions cooperate to share user identity information.
- Multiple Authentications: Users can log into multiple web applications using several institutional IDs.

Advantages of federated identity systems are:

- Enhanced Personal Information Protection: Storing user identity information across multiple databases strengthens privacy compared to centralized systems. Table 1 provides a side-by-side comparison of the advantages and disadvantages of Centralized Identity Management

Table 1. Side by side comparison of centralized identity management and distributed identifier (DID)

Criteria	Centralized Identity Management	Distributed Identifier (DID)
Advantages		
Ease of Management	Managing user identity is simpler due to central administration.	-
Enhanced Security	Strengthening the central database ensures user identity protection.	Using encryption technology, DID safeguards identities, offering resistance to hacking or attacks.
Service Convenience	Users can log into multiple applications using a single ID.	DIDs can be used across various applications and systems, allowing access to multiple services with their DID.
Personal Information Protection	-	Strengthened protection as DID doesn't store personal information in centralized servers and is managed by the user.
Service Scalability	-	As more systems support DID, users can access more services.
Disadvantages		
Centralization Risks	A breach of the central database could expose all users' identity information.	-
Privacy Infringement	Extensive collection of users' identity information by the central administrator.	-
Management Complexity	-	Requires technical know-how and understanding of the system.
Technical Complexity	-	In its early stages, DID can be technically challenging.
Limited Adoption	-	DIDs are not yet widely adopted, limiting the applications that support it.

and Distributed Identifier (DID).

- Improved Security: Collaboration among institutions enhances the protection of user identity information.
- Service Scalability: As new institutions join the federated identity system, users can access more services.

However, federated identity systems come with challenges:

- Management Complexity: Managing user identity information requires cooperation among several institutions, making it complex.
- Technical Complexity: Federated identity systems can be technically intricate.

Distributed Identifier (DID) is a decentralized identifier for users or objects. DIDs allow users or objects to create and manage their own identifiers without relying on centralized authentication institutions [10-11].

In conclusion, DID presents a new identity management approach that addresses the challenges of both centralized and federated identity systems. DIDs are not reliant on centralized servers, and users or objects can autonomously create and manage them. This reduces the risks associated with data breaches and centralized systems. Additionally, using encryption technology, DIDs offer enhanced security for user or object identities [12-15].

5. Proposed Cross-Domain Authentication System

Fig. 1 showcases the decentralized cross-domain authentication system, detailed as follows:

- DID Subject: Definition: The primary entity that the DID represents. This can be a person, organization, device, or any other entity that requires an identifier.
- DID Document: A DID Document contains the essential details to interact securely with the DID subject.
  - Public Keys:
  - Usage: These keys allow others to validate proofs (like signatures) from the DID subject or encrypt data in a way that only the subject

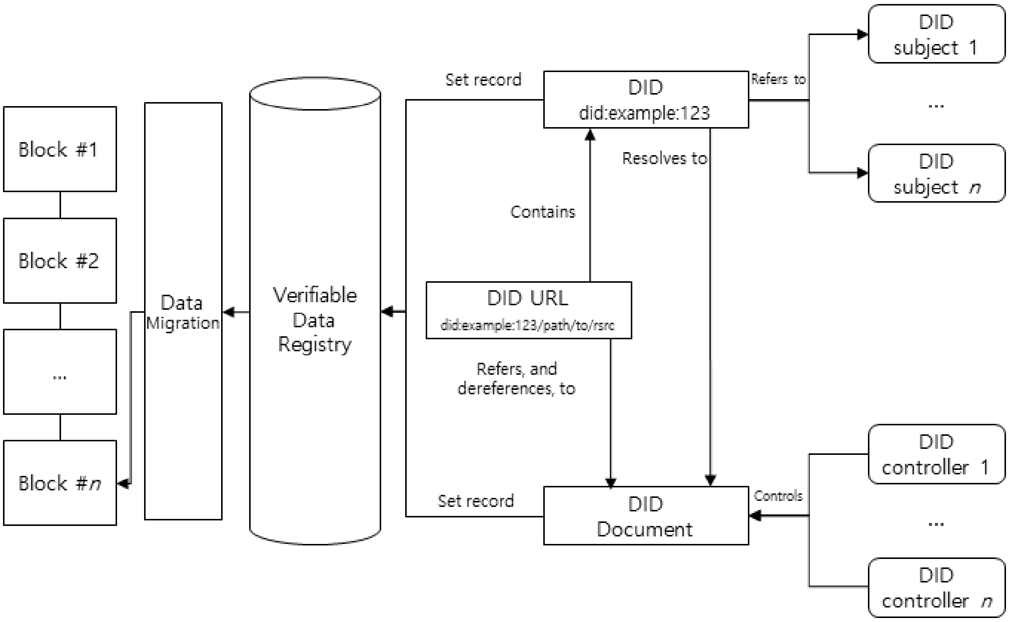

Fig. 1. UCI-based multi-domain access control framework

can decrypt.

- Types: Common key types include RSA, EdDSA, and ECDSA.
- Authentication Protocols:
- Mechanisms: Describes how the DID subject can prove control over the DID. This might involve using a specific public key to produce a cryptographic signature.
- Multi-factor authentication: DID systems can integrate multiple authentication mechanisms, increasing security.
- Service Endpoints: Descriptors (often URLs) where one can communicate with or retrieve services related to the DID subject.
- Privacy Concerns: It's crucial to ensure these endpoints do not leak sensitive information, as DID documents are often publicly readable. Some systems use privacy-preserving mechanisms or indirection to protect the subject's privacy.

Table 2. Description of cross-domain authentication system

System	Description
Certcoin	Maintains a public ledger of domain names and associated public keys.
Hierarchical Access Control	Uses a blockchain-based hierarchical structure to manage user access based on keys.
Town Crier	Provides authenticated information for smart contracts by ensuring data source security.
Decentralized PKI	A PKI system focusing on decentralization and transparency, making it easier to detect maliciously issued certificates.
BCCA	Ensures only certificates from trusted root CAs within a consortium chain are recorded and recognized.
Trust Transfer Scheme	Enhances trust transfer at a national level by transferring some CA management functions to the blockchain.
Trustroam	Allows for cross-domain roaming authentication using blockchain, with each validation being treated as a transaction.
Cross Domain Authentication	Promotes secure communication between two different domains (IBC and PKI) using blockchain technology.

- CRUD Operations:
  - Create: How a new DID is generated and registered.
  - Read: How to retrieve a DID document given a DID.
  - Update: How to make changes to a DID document or rotate cryptographic keys.
  - Delete: How to revoke or remove a DID, though some systems might not allow full deletion for immutability reasons.

6. Conclusion

In the modern business environment, collaboration and interoperability between organizations are of paramount importance, contributing to organizational success and maximizing profits. However, integrating work across multiple organizations has been challenging due to discrepancies in IAM roles and policies. User-Centric Identity (UCI) has been proposed as a solution, and this research has explored UCI's potential in depth. From an academic perspective, this research contributes to the body of knowledge on organizational interoperability by providing an in-depth analysis of User-Centric Identity (UCI) as a mechanism to facilitate seamless collaboration across various organizational boundaries.

REFERENCES

[1] Kim, J., Lee, S., & Ryu, S. (2023). A user-controlled identity-based multi-domain access control system using blockchain. *Journal of Information Security*, 24(1), 1-14. DOI : 10.1016/j.jis.2022.12.001

[2] Li, Q., Zhang, Y., & Yang, Y. (2022). A user-centric identity-based multi-domain access control system using FIDO2. *IEEE Access*, 10, 114087-114100. DOI : 10.1109/ACCESS.2022.3164595

[3] Zhou, Y., Li, H., & Wang, J. (2021). A user-controlled identity-based multi-domain access control system using attribute-based encryption. *Information Sciences*, 583, 283-298. DOI : 10.1016/j.ins.2021.07.023

[4] Chen, Y., Liu, Y., & Wang, X. (2020). A user-

centric identity-based multi-domain access control system using blockchain and federated learning. *Journal of Information Security*, 21(4), 245-263. DOI : 10.1016/j.jis.2020.07.001

[5] Hu, Y., Zhang, Y., & Yang, Y. (2021). A user-controlled identity-based multi-domain access control system using zero-knowledge proof. *IEEE Access*, 9, 116982-116995. DOI : 10.1109/ACCESS.2021.3088443

[6] Li, S., Wang, B., & Liu, Y. (2022). A user-controlled identity-based multi-domain access control system using distributed ledger technology. International *Journal of Information Security*, 21(1), 1-15. DOI : 10.1007/s10207-022-00404-2

[7] Feller, J., Zaytsev, D., & Jones, M. B. (2012, October 27). OAuth 2.0 authorization framework. Internet Engineering Task Force. Retrieved from https://tools.ietf.org/html/rfc6749 DOI : 10.17487/RFC6749

[8] Fang, Y., Li, S., Guo, X., & Liu, Y. (2022). Vaultpoint:A blockchain-based UCI model that complies with OAuth 2.0. In: Lin, Y.-B., Deng, D.-J. (eds.) SGIoT 2020. LNICUCITE 2651. Springer, Cham DOI : 10.1007/978-3-030-83550-9_20.

[9] Kim, S., & Park, J. (2022). A survey on centralized and federated identity management. J*ournal of Information Science*, 48(4), 423-442. DOI : 10.1177/01655515221096131

[10] Barker, R., & Parno, B. (2017). Decentralized Identifiers (DIDs): A technical introduction. RFC 8392. DOI : 10.17487/RFC8392

[11] Kshetri, N. (2021). The rise of decentralized identifiers: A review of the technology, applications, and challenges. *Journal of Information Technology*, 36(4), 513-525. DOI : 10.1057/s41265-021-00393-2

[12] Barker, R., & Parno, B. (2017). Decentralized Identifiers (DIDs): A technical introduction. RFC 8392. DOI : 10.17487/RFC8392

[13] Kshetri, N. (2021). The rise of decentralized identifiers: A review of the technology, applications, and challenges. *Journal of Information Technology*, 36(4), 513-525. DOI : 10.1057/s41265-021-00393-2

[14] Yin, Y., & Yu, S. (2021). A survey on RBAC and OAuth: A systematic literature review. *Information Systems Frontiers*, 23(6), 1525-1542. DOI : 10.1007/s10796-020-09909-5

[15] Zhu, J., & Zhang, X. (2022). A hybrid access control model based on RBAC and OAuth. *IEEE Access*, 10, 14436-14446. DOI : 10.1109/ACCESS.2022.3195679

홍 성 혁(Sunghyuck Hong) [정회원]

- 2007년 8월 : Texas Tech University, Computer Science (공학박사)
- 2012년 3월~현재 : 백석대학교 첨단IT학부, IoT 전공 주임 교수

- 관심분야 : 핀테크, 딥러닝, 블록체인, 사물인터넷 보안
- E-Mail : shong@bu.ac.kr