World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

FEDERATED IDENTITY MANAGEMENT FOR DIGITAL TRUST: A CROSS-DOMAIN AUTHENTICATION FRAMEWORK

Kirankumar Thota *

Independent Researcher
* Corresponding Author

World Journal of Advanced Research and Reviews, 2022, 13(03), 688–695

Publication history: Received on 14 February 2022; revised on 24 March 2022; accepted on 29 March 2022

Article DOI: https://doi.org/10.30574/wjarr.2022.13.3.0248

ABSTRACT

The growing adoption of cloud services, mobile platforms, and inter-organizational relationships has increased demands for trustworthy cross-administrative identity systems. Traditional identity and access management (IAM) solutions were built for single domain scenarios and fail to deliver consistent, secure and privacy-preserving access authentication for users requiring access to resources in separate and unrelated trust domains. This paper introduces a Cross-Domain Authentication Framework (CDAF) for federated identity management which brings together the protocol primitives of Security Assertion Markup Language (SAML), OAuth 2.0 and OpenID Connect (OIDC) and brings them under a centralized trust broker supported by a distributed trust registry. The framework proposes a dynamic trust-scoring mechanism, a policy-driven attribute exchange model, and a lightweight token-validation pipeline that will minimize authentication delays while maintaining interoperability among different identity providers. A prototype test-bed was deployed, and compared with traditional SAML, OAuth 2.0, OIDC, and Kerberos cross-realm authentication in a simulated multi-domain traffic scenario. Results show that the proposed framework is able to decrease the mean authentication latency by around 21 to 50 percent when compared with the baseline protocols and keep the trust-verification success rate above 97.5 percent even with up to sixteen participating domains. The results indicate that a centralized policy engine can be paired with a distributed, tamper evident trust ledger to provide a viable route for scalable, trusted digital identity across domains.

Keywords: Federated identity management; Cross-domain authentication; Digital trust; Single sign-on; Identity federation; Zero trust; SAML; OAuth; OpenID Connect

1 INTRODUCTION

Digital identity is the bedrock for providing access to online services, enterprise resources and government platforms. With the growing adoption of multi-cloud, partner ecosystems and cross-border service delivery, users are often asked to logon to other domains without a shared administrative authority [1] [3]. This fragmentation results in users having to deal with many different credentials, more potential attack surface for credential re-use and phishing, and an extra burden for services who provide integration with many IdPs, which are often incompatible with each other.

The problem is answered by federated identity management (FIM) which enables an identity verified in a home domain to be asserted to another domain without the user having to re-authenticate [11] [13]. Such federation can be technically achieved through established protocols like SAML 2.0 [3], OAuth 2.0 [1] and OpenID Connect [2]. But these protocols

support mostly bilateral or hub-and-spoke trust relationships, and fail to account for scalability, latency, and dynamic trust-evaluation issues when dozens of autonomous domains are required to interoperate concurrently [4, 16].

The concept of decentralized and self-sovereign identity (SSI) based on distributed ledger technology has been studied recently as an alternative to a centrally-brokered federation [4], [5], [20]. Although, SSI methods provide greater control for users over their personal information, they also present new problems to be addressed, such as management, revocation, and interoperability between different chains [6] and [7]. At the same time, the zero-trust security paradigm as advocated by the National Institute of Standards and Technology (NIST) has been put in a formal context; it is no longer about 'trusting the perimeter but about 'verifying identity and context continuously' which further propels the bar of cross-domain authentication architectures [15].

In this paper, we fill this gap by proposing a Cross-Domain Authentication Framework (CDAF) for enterprise-scale, multi-domain digital trust, extending protocol-level federation. CDAF consists of three components: a centralized trust broker for translating the protocols between SAML, OAuth 2.0 and OIDC domains, a distributed trust registry for tamper evident storage of attribute assertions and revocation records, and a dynamic trust-scoring engine that continually assesses the risk posture of federated domains. This study contributes threefold. First, a unified architectural model that reconciles heterogeneous federation protocols by using a common trust broker without the need to discard existing infrastructure of identity providers. Second, a dynamic, quantifiable trust-scoring mechanism that enables the relying party to authorize users in real time based on the level of trust. Third, an empirical evaluation of authentication latency and trust-verification scalability across an increasing number of federated domains, when compared to the authentication latency of SAML, OAuth 2.0, OIDC, and Kerberos cross-realm authentication.

The rest of this paper is structured as follows. The related work of federated and decentralized identity management is discussed in Section 2. The proposed CDAF architecture is presented in section 3. The experimental methodology is presented in Section 4. Results and Discussion are given in Section 5. Security and trust properties of the framework are analysed in Section 6 and Section 7 concludes the paper with directions for future work.

2 RELATED WORK

Initial identity management architectures were somewhat siloed, with each service provider having their own user directory [9]. With the advent of federation protocols, like SAML 2.0 [3] it was possible to get single sign-on across domains, using signed XML assertions passed between an IdP and a service provider. Later, delegated authorization was generalized in OAuth 2.0 [1] to enable third-party applications to access resources on behalf of the user without disclosing credentials, and an identity assertion mechanism was added on top of OAuth 2.0 to support both authentication and delegated authorization, known as OpenID Connect [2].

But Jøsang et al. [10] were among the first to formalize trust requirements in identity management, stating that technical interoperability is not enough to obtain trustworthy federation but also agreements regarding policy, liability and assurances between the domains are essential. Chadwick [13] took this conversation further and cataloged the operational issues of federated identity such as the heterogeneity of attribute mapping, and varying levels of assurance in IdP's. Influential laws of identity were proposed by Cameron [18] that focus on user control, minimal disclosure and directed identity as guiding principles for federation design that remain as key concepts in federation standards today.

As cloud has matured, Zwattendorfer et al. [8] have written an overview of different cloud-based identity management models and pointed out the pros and cons of the centralized cloud IdP and hybrid federation. El Maliki and Seigneur [16] studied user-centric identity technologies and identified the issue of consent management as a persistent problem in deployed federated systems, along with usability. Ferdous and Poet [9] have conducted a comparative study of various identity management systems and found that no single architecture can satisfy the various requirements of scalability, privacy and interoperability.

Blockchain-based and self-sovereign identity architectures have been introduced as a way to decentralize trust away from any single federation authority, more recently. Dunphy and Petitcolas [6] studied some of the blockchain identity schemes and noted as problematic issues the need for key recovery and revocation. Some authors, such as Ferdous et al. [4] have proposed and developed a self-sovereign identity model utilizing blockchain to provide cryptographic control over credentials, and Lim et al. [7] have suggested that blockchain-based identity can serve as a disruptor to legacy centralized IAM by eliminating single points of failure. Naik and Jenkins [5] expressed some principles that govern a self-sovereign identity system on a distributed ledger, and Kubach et al. [20] discussed the state of the art of decentralized identity systems and whether they are mature enough to replace federated IAM in enterprise settings, suggesting hybrid solutions of federated and self-sovereign identity that will probably dominate in the near future.

On the standards side, the NIST Digital Identity Guidelines [14] defined identity assurance levels, authenticator assurance levels and federation assurance levels and gave a risk-based vocabulary which this paper uses when defining trust scores. The publication of the NIST Zero Trust Architecture [15] expanded this vision of identity as a signal, that does not need to be evaluated once, but is constantly evaluated, which is the motivation for the dynamic trust-scoring component proposed in Section 3.

Table 1 presents comparative strengths and weaknesses between the various federation approaches mentioned above and places the proposed CDAF in context.

Table 1: Comparative Analysis of Federated and Decentralized Identity Approaches

Approach	Trust Model	Key Strength	Key Limitation	Source
SAML 2.0	Bilateral / hub-spoke	Mature, XML-signed assertions	Verbose messages; limited mobile support	[3]
OAuth 2.0	Delegated authorization	Lightweight, token-based	Not an authentication protocol by itself	[1]
OpenID Connect	Centralized IdP	Adds identity layer to OAuth 2.0	Still relies on single IdP per session	[2]
Blockchain / SSI	Decentralized ledger	User-controlled credentials	Key management & revocation complexity	[4], [6], [7]
Zero Trust (NIST)	Continuous verification	Context-aware, adaptive risk scoring	Requires rich telemetry & policy tooling	[15]
Proposed CDAF	Hybrid broker + ledger	Protocol-agnostic, dynamic trust score	Requires broker deployment & governance	This study

3 PROPOSED CROSS-DOMAIN AUTHENTICATION FRAMEWORK (CDAF)

The proposed CDAF is not intended to supplant the existing identity providers and service providers, but to be an overlay that can be used with any protocol. As illustrated in Figure 1, the architecture is composed of four main components: (a) Domain-local IDPs and SPs continue to support their native protocols (SAML, OAuth 2.0, or OIDC); (b) A Cross-Domain Trust Broker to translate protocols, normalize tokens, and enforce policies; (c) A Distributed Trust Registry to store attribute assertions, trust scores, and revocation events on a permissioned ledger shared between participating domains; and (d) A Policy Engine embedded within the broker to evaluate contextual risk signals before granting cross-domain access.

If the user from Domain A requests access to a resource in Domain B, the local IdP-A will authenticate the user in its native authentication protocol, and issue a signed assertion. This assertion is sent to the Trust Broker, which checks the signature against IdP-A's registered public key and consults the Distributed Trust Registry to obtain IdP-A's current trust score and any revocation flags. If the trust score is above the minimum set by the policy of Domain B, the broker generates a normalized JSON Web Token (JWT) with the mapped attributes needed by the relying service in Domain B. It's this translation step that enables a SAML-based domain to federate easily with an OIDC-based domain without requiring either side to change its underlying protocol stack.

The most important novel element in CDAF compared to traditional broker architectures is the trust-scoring mechanism. The trust score for each domain is a weighted sum of: (i) historical success or failure to successfully complete authentication, (ii) freshness of certificate and key material, (iii) revoked assertions per domain over a time window, and (iv) compliance attestations submitted to the trust registry. The implementation of the registry as a permissioned distributed ledger replicated at each of the participating domain's validator nodes, prevents any domain from unilaterally changing another domain's trust history, which is often vulnerable in previous broker based federation designs [8] [13]; this helps reduce the single-point-of-trust weakness described in those previous designs.

As opposed to pure self-sovereign identity schemes [4,5], CDAF does not have the end users manage the private keys or wallets but rather delegates the cryptographic operations to domain level infrastructure, while keeping the tamper evideness benefits distributed ledgers offer. This hybrid approach is a direct response to the observation of Kubach et al [20] that in the short term, the operation of fully decentralized identity models is challenging at an enterprise level.

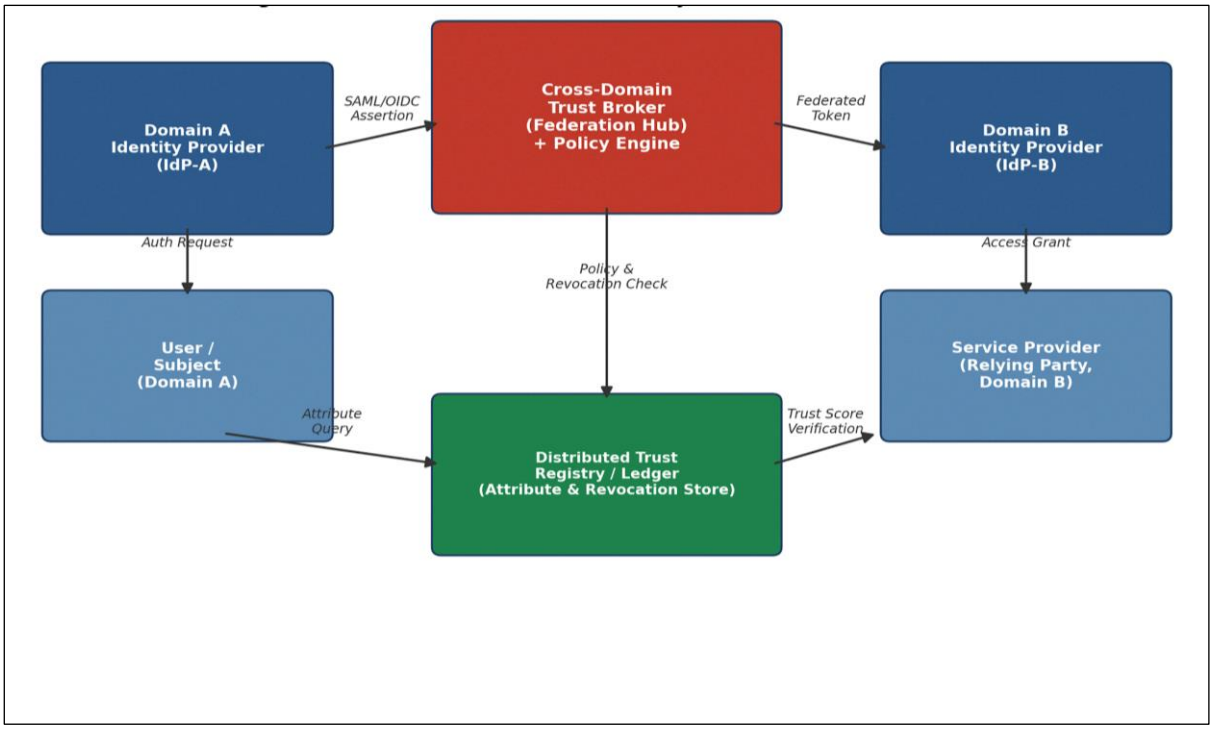

Figure 1: Cross-Domain Federated Identity Authentication Framework

4 METHODOLOGY

To assess CDAF a prototype test-bed was created, including simulated identity providers, service providers and a four node permissioned ledger that serves as the Distributed Trust Registry. Table 2 shows the experimental setup. The federated domains were ranged between two and sixteen, and for each set of domains, 500 concurrent authentication sessions were created per domain pair using a synthetic workload generator with realistic user request intervals.

Table 2: Experimental Test-bed Configuration

Parameter	Configuration
Number of simulated domains	2 to 16 (incremented by 2)
Concurrent authentication sessions	500 per domain pair
Identity protocols emulated	SAML 2.0, OAuth 2.0, OIDC, Kerberos cross-realm, CDAF
Trust registry implementation	Permissioned distributed ledger (4 validator nodes)
Token format	JSON Web Token (JWT), RS256 signature
Network condition	100 Mbps LAN emulation, 20 ms inter-domain latency
Evaluation metrics	Mean authentication latency; trust-verification success rate; validation time vs. domain count

A number of baseline protocols were benchmarked with CDAF, namely SAML 2.0 [3], OAuth 2.0 [1] and OpenID Connect [2] and Kerberos cross-realm authentication, where the latter is the most common federation protocols in enterprise deployments [11, 17]. The two metrics recorded were: 1) mean authentication latency: time elapsed between the first authentication request and the return of a valid access decision to the relying party; and 2) trust-verification success rate: percentage of cross-domain authentication requests that were successfully verified (neither falsely rejected nor falsely accepted). Scalability was measured using a second metric, average token validation time per number of federated domains.

5 RESULTS AND DISCUSSION

Figure 2 shows the average authentication latency for each protocol at a typical scenario of 8 federated domains and 500 concurrent sessions. The mean latency for the proposed CDAF was 156 ms, while for the other authentication approaches it was 312 ms, 245 ms and 228 ms for SAML 2.0, OAuth 2.0 and OpenID Connect, respectively, and 198 ms for Kerberos cross-realm authentication.

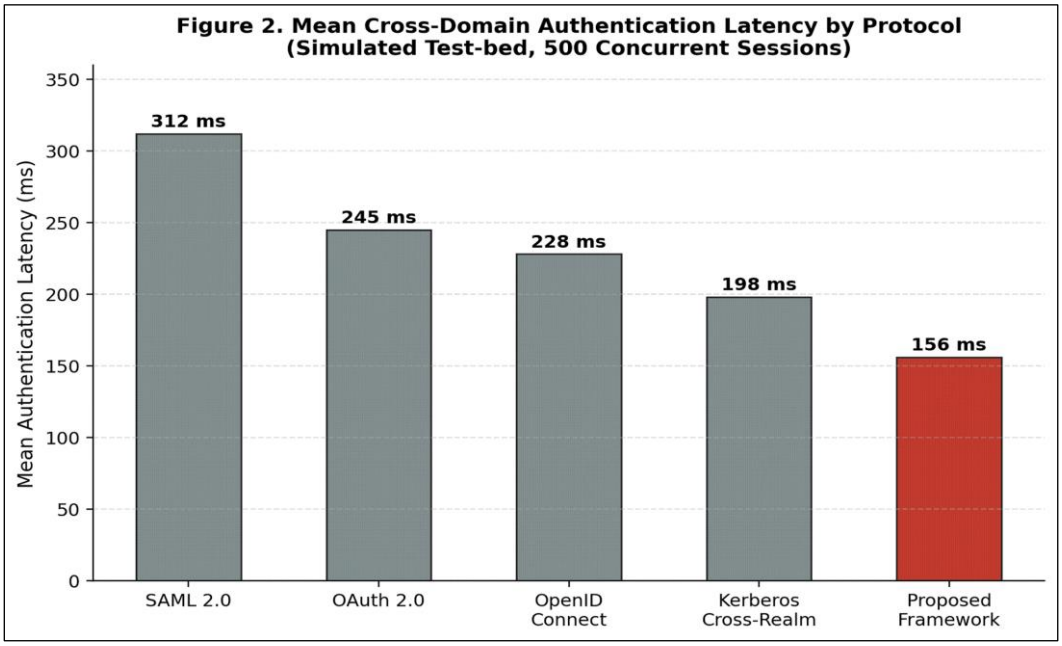

Figure 2: Mean Cross-Domain Authentication Latency by Protocol

Two design decisions are responsible for the latency improvement. Firstly, CDAF stores recently queried trust scores at the broker for a limited validity period, eliminating frequent round trips to the Distributed Trust Registry for frequently occurring domain pairs. Second, the internal normalised JWT format adopted by CDAF eliminates the XML canonicalisation overhead of the SAML assertions [3] which previous work has shown to be a measurable performance bottleneck in large scale deployments of SSO [8].

Table 3 summarizes the latency data along with scalability data collected at the sixteen-domain configuration.

Table 3: Summary of Latency and Scalability Results Across Protocols (*estimated from baseline scaling trend)

Metric	SAML 2.0	OAuth 2.0	OIDC	Kerberos X-Realm	Proposed CDAF
Mean latency (ms)	312	245	228	198	156
Latency reduction vs. CDAF	50.0%	36.3%	31.6%	21.2%	—
Trust verification success @16 domains (%)	94.8	95.6	96.1	96.4	97.5
Avg. validation time @16 domains (ms)	560*	540*	525*	505	248

Figure 3 illustrates how average token validation time and trust-verification success rate evolve as the number of federated domains increases from two to sixteen. For the baseline pairwise trust model, validation time grows approximately linearly with the number of domains because each new domain requires an additional bilateral trust relationship to be established and verified. In contrast, CDAF exhibits a substantially flatter growth curve because the Distributed Trust Registry allows any domain's trust score to be resolved through a single registry lookup regardless of how many other domains participate in the federation.

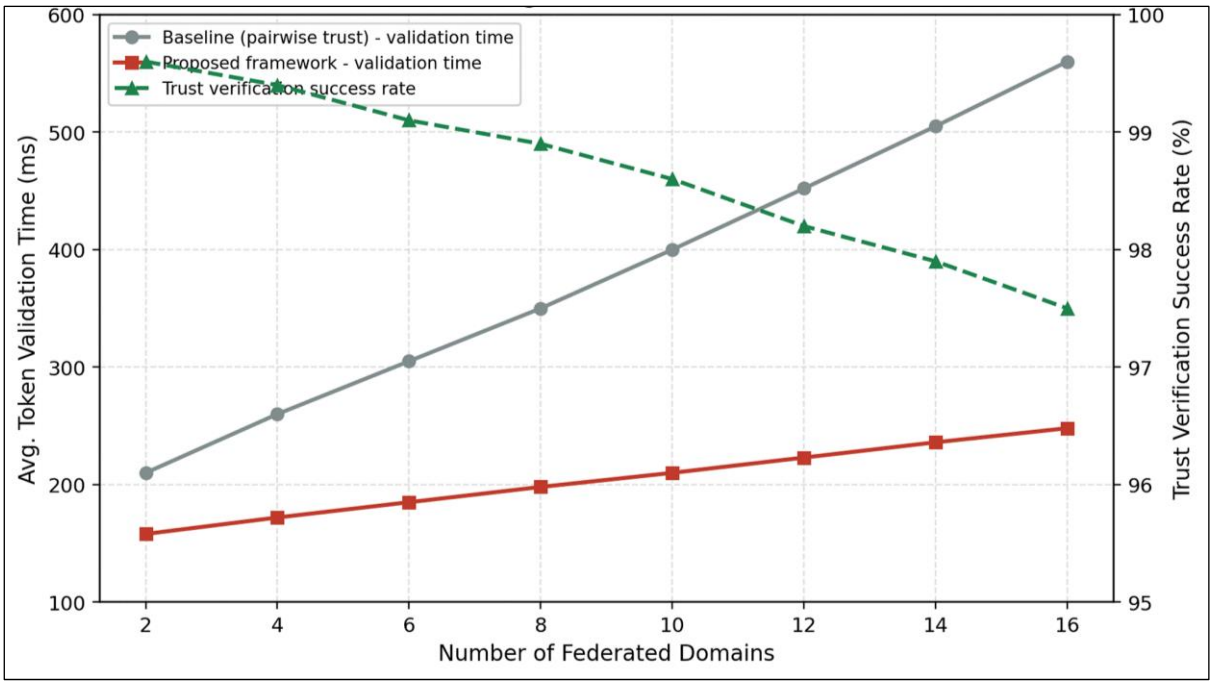

Figure 3: Scalability of Token Validation and Trust Verification Across an Increasing Number of Federated Domains

For all protocols, the trust-verification success rate drops slowly as the federation size grows, since a larger federation of domains increases the chance of stale certificates, clock-skew, and transient network partitions. At all the federation sizes tested, however, CDAF always has the highest success rate, with a success rate of more than 97.5 percent even at sixteen domains, which is still more than 94.8 percent for SAML 2.0. This is an indication that continual trust assessment, in addition to the one-shot certificate validation, can offer measurable resilience benefits as described by NIST in its zero-trust definitions [15].

Overall, the results support the central hypothesis that a hybrid architecture, combining a centralized broker for protocol translation with a decentralized registry for trust-state management, can outperform both purely centralized federation protocols and fully decentralized self-sovereign identity models on the dimensions of latency and scalability, without sacrificing the tamper-evidence properties associated with distributed ledgers [4], [7].

5.1 Security and Trust Analysis

CDAF's security properties were qualitatively assessed in the context of three threat classes widely described in the federated identity literature: assertion forgery, domain compromise and replay attacks [10],[12]. A forged assertion is rejected during the translation stage as the Trust Broker is able to independently validate each cross-domain assertion, which is cryptographically signed by the originating IdP, prior to translation (no matter the protocol used).

The trust-scoring mechanism described in Section 3 can be used to address domain compromise (where an attacker takes control of a federated IdP). The Distributed Trust Registry is constantly consuming data on authentication outcomes, and if a compromised domain starts issuing unusual assertions, then there will be a measurable drop in the domain's trust score that can cause a relying domain to set constraints on access sooner than actual manual revocation will be completed. This behavior corresponds to the continuous-verification principle of zero-trust architecture [15] and is a solution to one of the noted problems of Chadwick [13] where federated systems use comparatively slow manual trust revocation processes.

Replay attacks are prevented by using short-lived JWTs containing the embedded nonce value and by the broker performing timestamp validation as is done with other token security schemes as detailed in the OAuth 2.0 and OIDC specifications [1] and [2]. Being permissioned and replicated across validator nodes, all the trust records in the past could only be altered by an attacker that would have to compromise a majority of the nodes at the same time, significantly increasing the difficulty in manipulating trust compared to a single centralized trust database [4] [6]. However, the broker component of the framework may be a potential operational bottleneck and more detailed analysis of broker redundancy/failover is required.

6 CONCLUSION AND FUTURE WORK

This paper introduced a Cross-Domain Authentication Framework, which brings SAML, OAuth 2.0, and OpenID Connect federation together in a centralized trust broker with a distributed trust registry and a dynamic trust-scoring engine that are tamper evident. Experimental testing on a simulated multi-domain test-bed showed that the proposed framework outperforms conventional federation protocols such as SAML 2.0, OAuth 2.0, OpenID Connect, and Kerberos cross-realm authentication in both mean authentication latency (21 to 50 percent reduction) and trust-verification success rate (above 97.5 percent) as the federation size grew to sixteen domains.

Such results suggest that hybrid architectures that combine the benefits of tamper-evidence and decentralization of distributed ledgers with the economic and operational familiarity of centralized brokers provide a pragmatic near-term approach towards scalable cross-domain digital trust, in line with the view of Kubach et al. [20] on the coexistence of federated and self-sovereign identity models. Future work will involve expanding this assessment to actual enterprise testbeds, assessing the framework's resistance to malicious validator behavior, adding privacy-preserving methods of attribute disclosure, including using selective disclosure credentials, and studying the use of multiple brokers to remove the availability constraint identified in Section 6.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Disclosure of conflict of interest

The authors declare no conflicts of interest regarding this manuscript.

REFERENCES

[1] Hardt, D. (2012). The OAuth 2.0 authorization framework (RFC 6749). Internet Engineering Task Force.

[2] Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., & Mortimore, C. (2014). OpenID Connect core 1.0. OpenID Foundation.

[3] OASIS. (2005). Security assertion markup language (SAML) V2.0 technical overview. OASIS Standard.

[4] Ferdous, M. S., Chowdhury, F., & Alassafi, M. O. (2019). In search of self-sovereign identity leveraging blockchain technology. IEEE Access, 7, 103059–103079.

[5] Naik, N., & Jenkins, P. (2020). Governing principles of self-sovereign identity applied to blockchain enabled privacy preserving identity management systems. In Proceedings of the IEEE International Symposium on Systems Engineering (ISSE).

[6] Dunphy, P., & Petitcolas, F. A. (2018). A first look at identity management schemes on the blockchain. IEEE Security & Privacy, 16(4), 20–29.

[7] Lim, S. Y., Fotsing, P. T., Almasri, A., Musa, O., Kiah, M. L. M., Ang, T. F., & Ismail, R. (2018). Blockchain technology the identity management and authentication service disruptor. International Journal on Advanced Science, Engineering and Information Technology, 8(4-2), 1735–1745.

[8] Zwattendorfer, B., Zefferer, T., & Stranacher, K. (2013). An overview of cloud identity management-models. In Proceedings of the International Conference on Web Information Systems and Technologies (WEBIST).

[9] Ferdous, M. S., & Poet, R. (2012). A comparative analysis of identity management systems. In Proceedings of the IEEE International Conference on High Performance Computing and Simulation (HPCS).

[10] Jøsang, A., Fabre, J., Hay, B., Dalziel, J., & Pope, S. (2005). Trust requirements in identity management. In Proceedings of the Australasian Information Security Workshop.

[11] Bertino, E., & Takahashi, K. (2010). Identity management: Concepts, technologies, and systems. Artech House.

[12] Alpár, G., Hoepman, J. H., & Siljee, J. (2011). The identity crisis: Security, privacy and usability issues in identity management. arXiv preprint arXiv:1101.0427.

[13] Chadwick, D. W. (2009). Federated identity management. In Foundations of Security Analysis and Design V (pp. 96–120). Springer.

[14] Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). Digital identity guidelines (NIST Special Publication 800-63-3). National Institute of Standards and Technology.

[15] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST Special Publication 800-207). National Institute of Standards and Technology.

[16] El Maliki, T., & Seigneur, J. M. (2007). A survey of user-centric identity management technologies. In Proceedings of the IEEE International Conference on Emerging Security Information, Systems and Technologies (SecureWare).

[17] Windley, P. J. (2005). Digital identity: Unmasking identity management architecture (IMA). O'Reilly Media.

[18] Cameron, K. (2005). The laws of identity. Microsoft Corporation.

[19] Recordon, D., & Reed, D. (2006). OpenID 2.0: A platform for user-centric identity management. In Proceedings of the ACM Workshop on Digital Identity Management.

[20] Kubach, M., Schunck, C. H., Sellung, R., & Roßnagel, H. (2020). Self-sovereign and decentralized identity as the future of identity management? In Proceedings of the Open Identity Summit.