International Journal of The Nigerian Institute of Architects (IJNIA)

The International Journal of the Nigerian Institutes of Architects (IJNIA) serves as a dynamic platform for advancing architectural scholarship, professional innovation, and interdisciplinary built environment research. The journal seeks to foster meaningful dialogue and knowledge exchange among researchers, architects, industry professionals, policymakers, and global stakeholders in addressing contemporary challenges facing buildings, cities, infrastructure, and communities. Through its focus on sustainable design, resilient urban development, digital transformation, emerging technologies, and socially responsive architectural practice, IJNIA aims to promote transformative research and professional knowledge that contribute to adaptive, inclusive, intelligent, and sustainable built environments.

Received: 04/07/2026
Revised: 19/07/2026
Accepted: 22/07/2026
Published: 27/07/2026

Volume: 2026
Issue: 01
Pages: 24-48

Review Article

Digital Interoperability and Research Dissemination in Architecture and the Built Environment

Ebere Donatus Okonta[1], Oluyemi Kehinde[1], Excel Michael[2*], Uchechi Grace Okonta[3], Ogochukwu Francis Okeke[4], Enobong Bennett Equere[5], Chidinma Emma-Ochu[6], Akinyemi Oke[7]

[1]Teesside University, Middlesbrough, United Kingdom
[2] National Open University of Nigeria, Abuja, Nigeria
[3] Newcastle City Council, Civic Centre, Newcastle upon Tyne, United Kingdom
[4] Canterbury Christ Church University, Canterbury, Kent, United Kingdom
[5] University of Uyo, Uyo, Nigeria
[6] Federal Polytechnic Nekede, Owerri, Imo State, Nigeria
[7] Federal University of Technology and Environmental Sciences, Iyin Ekiti, Nigeria

*Correspondence: nou254240533@noun.edu.ng

Abstract

Digital interoperability plays a critical role in enhancing the dissemination, accessibility, and usability of scholarly research across architecture and the built environment. However, fragmented digital access systems across academic publishing platforms continue to create barriers for researchers, limiting seamless interaction with scholarly resources. This study investigates how digital interoperability influences research dissemination by examining the structure and functionality of log-in systems within academic publishing ecosystems, using Elsevier journal platforms as a case study. The study employed a systematic literature review to identify the key factors influencing log-in system design, alongside the challenges and benefits associated with Single Sign-On (SSO) implementation. In addition, a case study of 176 Elsevier journals was conducted to evaluate the extent of interoperability across journal platforms and their capacity to support unified access mechanisms. Findings reveal a significant lack of SSO integration across the examined journals, resulting in fragmented access pathways that may hinder efficient knowledge dissemination and user engagement. Key factors shaping log-in system design include identity management frameworks, protocol standards, security requirements, and application design structures. The study further identifies major implementation challenges related to security, policy frameworks, integration complexity, and user experience, while highlighting the benefits of interoperable systems in improving accessibility, operational efficiency, and user satisfaction. The study concludes that strengthening digital interoperability within academic publishing infrastructures is essential for advancing research dissemination, fostering interdisciplinary knowledge exchange, and improving accessibility to built environment scholarship.

Keywords: Interoperability; Log-in Systems; Elsevier Journals; Single Sign-On (SSO); Academic Publishing; User Experience; Unified Log-in.

Highlights

- Fragmented log-in systems across journals create barriers to efficient research dissemination.
- A significant lack of SSO integration in journal platforms hinders seamless user access.
- Strengthening digital interoperability is essential for advancing scholarly exchange.

1 Introduction

Log-ins provide a security layer between unsecured and secure activity (Pal et al., 2020). In other words, all data transfers are typically encrypted once a user logs in to a safe website. Log-in systems are thus defined as security measures to prevent unauthorised access to confidential data (Omotunde & Ahmed, 2023). Most log-in systems are unique to the websites they were created for, with most being used as long as there are internet access and connectivity (Bhana & Flowerday, 2021). On the other hand, with numerous user log-in systems, recalling passwords and usernames sometimes gets quite complicated. Hence, " interoperability " is a more seamless way to address these challenges. Interoperability refers to the degree to which a software system, devices, applications or other entity can connect and communicate with other entities in a coordinated manner without effort from the end user (Vernadat, 2007; Albouq et al., 2022).

In the digital age, the accessibility of scholarly literature is paramount for advancing academic research and knowledge dissemination (Edwards, 2018; D'Cruz et al., 2021). Academic publishing platforms Such as Elsevier facilitate access to many journals and articles (Gonzalez et al., 2022). However, the user experience on these platforms can be hindered by issues related to log-in interoperability (Giraldi et al., 2023). Researchers, academics, and students often encounter the inconvenience of creating and managing multiple accounts to access different journals, leading to inefficiencies and user frustration (Brembs et al., 2023). As a result, the quick transition to digital use of technology publication over the last two decades has brought more online resources closer to users than ever before, but at the expense of accessibility (Okonta et al., 2025). Within the field of architecture and urban planning, the paradox of accessibility is particularly critical. There exists a continuous requirement for unhindered access to a multidisciplinary spectrum of journals, for researchers developing data-driven methodologies for urban morphology or exploring biophilic design principles. The fragmentation of the access system disrupts the synthesis of spatial data and environmental science research. Thus, by focusing on Elsevier's expansive repository as a case study, this research highlights systemic barriers that limit the efficient dissemination of built environment scholarship.

Interoperability, in the context of digital systems, refers to the ability of different systems and organisations to work together seamlessly (Hodapp & Hanelt, 2022). For academic publishing platforms, this means enabling users to navigate between various journals and access their content using a single set of credentials (Moore, 2020). A well-designed log-in system that supports interoperability can significantly enhance the user experience by simplifying access and improving the efficiency of academic workflows (Daniel et al., 2023; Wang et al., 2021). This study seeks to tackle the issue of disjointed log-in experiences for accessing built environment and engineering research, by examining the log-in interfaces of 355 journals within the Elsevier ecosystem, in order to evaluate their interoperability. The study aimed to systematically review literature to assess factors affecting log-in systems, as well as the challenges and advantages of implementing single log-in systems. The fundamental research questions of this investigation is: to what extent do academic publishing login interfaces, with Elsevier as a principal case study, facilitate interoperability, and what enhancements may be implemented to improve user experience and accessibility for researchers? The study will also seek to identify the factors influencing log-in system design and the challenges and benefits of implementing a single log-in system. By exploring these questions, the study aims to identify the factors that affect the design of log-in systems, and propose recommendations for creating a more unified and user-friendly access mechanism for academic platforms hosting architectural and built environment research, drawing insights from the Elsevier model. The significance of this study lies in the

fact that improving the interoperability of log-in systems for Elsevier journals is crucial for enhancing the user experience of researchers, academics, and students who rely on these publications for their work. Addressing this issue has the potential to streamline access to scholarly literature, increase user satisfaction, and ultimately improve the efficiency of academic workflows.

2 Literature Review

Users' experience on any platform is a determining factor for continuous usage. Academic platforms serve as digital knowledge repositories, emerging as an indispensable reservoir, seamlessly intertwining with the fabric of contemporary education and learning (Khan, 2021; Panda et al., 2023). Peker et al. (2023) highlighted that a well-designed and user-friendly online journal interface possesses two traits: researcher satisfaction and bolstering the reputation of academic publishers within the scholarly community. Furthermore, a characteristic trait for enhanced user experience is accessible design on platforms. Accessibility is based on ensuring all content and digital functionality are available to everyone regardless of physical or cognitive impairment or device used (Clifford, 2021). However, the findings reveal that accessibility is not a one-off activity but one that is strategic and enhances the operational capability of any platform. Giannakoulopoulos et al. (2024) say that this unified approach, which improves both digital and human resource management, can handle differences in the area and keep the institution's web presence growing steadily over time.

Academic papers in the built environment rely heavily on vast datasets, particularly spatial models and climate forecasts. According to Horký and Caha (2024), the rising prevalence of digital media and the anticipated expansion of virtual reality necessitate effective solutions for managing large 3D models. When researchers are unable to access related data repositories and additional architectural files across various publishing platforms, the dissemination of essential urban infrastructure research is significantly hindered. Scherer (2020) states that by investing in interoperable metadata standards and practices and creating a networked landscape of systems and communities, technology ecosystems can be created that encourage researchers to make even more of their research open while streamlining research information management activities.

Log-in systems restrict access to scholarly information, guaranteeing that only authorised users can see or download full-text publications (Mollakuqe & Dimitrova,2024). These systems serve a variety of objectives, including authentication, which verifies user identity and ensures lawful access privileges (Capes-Davis & Neve, 2016). Authorisation grants certain permissions based on the user's role or subscription level (Esposito et al., 2021), whereas personalisation customises user experiences based on preferences and previous interactions (Chiu et al., 2021). Predominantly, the IP-based authentication log-in system is utilised by institutions to grant user access to sites based on the user's Internet Protocol (IP) address, typically allowing seamless access from within the institution's network (Wiefling et al., 2022). The standard log-in procedure is often applied to retrieve user credentials (usernames/passwords) associated with their subscription or institutional access as utilised by Elsevier (Alruwaili, 2020). Furthermore, access could also be gained via Single Sign-On (SSO), which allows users to log in using existing credentials from their institution or a trusted third-party provider like Google or Web of Science, reducing the number of passwords users need to manage (Pandey & Nisha, 2021).

Access to scholarly literature has long been an issue due to various circumstances, including expensive subscription fees for journals and databases, which prevent individuals and organisations with limited budgets from accessing it (Budzinski et al., 2020). Licensing

agreements that limit content access and sharing, stifling free distribution and information reuse; and technological barriers to open access (Ashikuzzaman, 2018), privacy, and unauthorised access, undermining publisher revenue and exposing user data to exploitation (Christen et al., 2020). There appears to be a scarcity of work that tackles log-in systems and access difficulties concerning scholarly publication, compounding an already significant deficit. However, similar research in this area, such as Manzoor et al. (2019) on "Multi-tier authentication schemes for fog computing: Architecture, security perspective, and challenges," indicated that log-in systems face major data security and privacy issues.

This finding was supported by Rehnbäck (2023), which found over 120,000 log-in attempts from remote desktops in just 24 hours using Remote service software to establish a connection to an asset on another network. Interoperability has been widely studied in various domains, including healthcare, information technology, and library science. The concept of interoperability, as defined by (Shehzad et al., 2021; Rita et al., 2024), involves the ability of systems to exchange and use information seamlessly. In academic publishing, interoperability enables users to access diverse resources without navigating multiple, disjointed systems. Research by (Shahzad & Khan, 2022; Abdul Rahman & Mohezar, 2020) has demonstrated that interoperability can significantly enhance the usability of digital libraries by providing a unified access mechanism. Despite its benefits, achieving interoperability in digital systems presents several challenges. According to de Mello et al., (2022), technical limitations, legacy systems, and differing standards across platforms can hinder the implementation of interoperable systems. In academic publishing, (Rita et al., 2024) notes that business models and publisher policies also play a significant role in shaping access protocols, which can impact interoperability.

Several initiatives have sought to address interoperability in digital libraries and academic publishing. For instance, the Open Researcher and Contributor ID (ORCID) system, as discussed by (Thibault et al., 2023; Makwana, 2022), provides a unique identifier for researchers, facilitating seamless access across different platforms. Additionally, the Single Sign-On (SSO) technology, examined by (Yusuf et al., 2024), has been proposed to streamline log-in processes by allowing users to access multiple resources with a single set of credentials. Contemporary research suggests that whereas educational platforms aim for inclusivity, their foundational gatekeeping mechanisms create structural impediments that hinder user fluidity. Digital publishing platforms predominantly depend on conventional Internet Protocol (IP) authentication systems (Wiefling et al., 2022) or typical credential retrieval mechanisms (Alruwaili, 2020) to oversee user identity, role-based access control, and content customisation (Capes-Davis & Neve, 2016; Chiu et al., 2021; Esposito et al., 2021; Mollakuqe & Dimitrova, 2024). Nevertheless, this significant dependence on isolated authentication systems establishes pronounced practical limitations. Although universal solutions like Single Sign-On (SSO) and centralised identifiers such as ORCID provide avenues to alleviate multi-credential password fatigue, their adoption is persistently hindered by a confluence of expensive subscription models, inflexible institutional licensing agreements, and significant backend data security vulnerabilities. Concurrent technical fields validate that outdated access configurations encounter significant vulnerabilities, often experiencing intense unauthorised remote access attempts (Manzoor et al., 2019; Rehnbäck, 2023). As a result, realising the conventional definition of seamless cross-platform interoperability (Shehzad et al., 2021; Rita et al., 2024) demonstrated to enhance digital library usability (Abdul Rahman & Mohezar, 2020; Shahzad & Khan, 2022) is hindered by outdated infrastructure limitations, incompatible technical standards, and restrictive commercial practices of publishers (de Mello et al., 2022; Rita et al., 2024).

Much research has been done on the user experience and interoperability, however, scant research addresses the interoperability of log-in systems within prominent academic publishing platforms that disseminate essential built environment research, such as Elsevier. This research will contribute to the current literature by thoroughly evaluating the log-in interfaces of architectural and built environment in the Elsevier database for interoperability, and will propose enhancements based on these findings. The research starts from the existent base of study and, in doing so, contributes to the present debate on academic publishing platforms, user experience, and interoperability. The findings will have implications for enhancing the accessibility and usability of scholarly resources, ultimately benefiting researchers, academics, and students.

3 Methodology

Concerning the study's aim and objectives, a two-pronged methodological approach was adopted: a Systematic Literature Review (SLR) of published research articles and a Case Study of academic journals. The SLR was applied to analyse the determinants impacting log-in systems, in addition to the difficulties and merits of establishing single log-in systems. At the same time, the case study methodology explored how well major publishing platforms endorse interoperability, with Elsevier's journal ecosystem serving as a case in point. Elsevier's engineering and technology collection was chosen as it exemplifies a premier segment of the globe's largest academic publisher, serving as an essential benchmark for assessing if top-tier digital infrastructure facilitates the collaborative, data-driven processes of technical researchers. Although the empirical focus was limited to one publisher, the results possess extensive applicability as they assess universal open standards like SAML and OpenID Connect uncovering systemic legacy integration deficiencies that are easily applicable to other prominent publishing platforms. Ultimately, this recorded authentication friction conceptually extends to the wider scholarship of the built environment, demonstrating how disjointed digital portals fundamentally hinder interdisciplinary workflows for researchers who must consistently traverse distinct repositories to cross-reference spatial, architectural, and environmental information.

3.1 Systematic Review

The study utilised the systematic literature review to evaluate factors influencing log-in systems and the challenges and benefits of implementing single log-in systems. Conducting systematic reviews of user experience with log-in systems allowed for a thorough examination of existing literature (Aromataris & Pearson, 2014; Kim et al., 2020), leading to the identification of challenges and trends with interoperable log-in systems. Furthermore, systematic reviews generate evidence-based insights (Lewis et al., 2021), which could be further harnessed to develop improved log-in systems.

The study relied on the Scopus database because that ensures only high-quality data are indexed and has a wide global and regional coverage of scientific journals, conference proceedings, and books (Bass et al., 2020) and it is owned by Elsevier. The search query was created by combining relevant terms and synonyms linked to the user log-in interface using the Boolean operators "OR" and "AND". The search query used was ("log-in system design" OR "authentication system design" OR "single sign-on" OR "SSO" OR "interoperable log-in" OR "federated log-in" OR "unified authentication" OR "cross-platform authentication") AND ("digital platforms" OR "academic platforms" OR "publishing platforms" OR "web applications" OR "research databases" OR "scholarly communication"). As illustrated in the PRISMA flow chart (Figure 1), the initial database search yielded a total of 281 documents (comprising 191 conference proceedings, 82 journal articles, 5 book chapters, 2 reviews, and 1 book).

The enhancement procedure was carried out in four successive phases to reduce this selection to the ultimate synthesis. Initially, a preliminary format evaluation eliminated novels, book chapters, and reviews to concentrate solely on primary research articles and conference proceedings, narrowing the selection to 223 documents. Secondly, a linguistic and duplication filter was implemented, resulting in the exclusion of 10 papers in Chinese and 1 in Portuguese, so retaining 147 publications. Thirdly, a screening of titles and abstracts eliminated articles that did not concentrate on digital interoperability or user login interfaces in architecture and the built environment, refining the selection to 116 pieces. Ultimately, a thorough full-text eligibility evaluation was performed to assess the empirical depth concerning the challenges and advantages of single sign-on (SSO), resulting in the exclusion of irrelevant papers and a final sample of 87 documents (including 61 conference papers and 26 journal articles) for the systematic review.

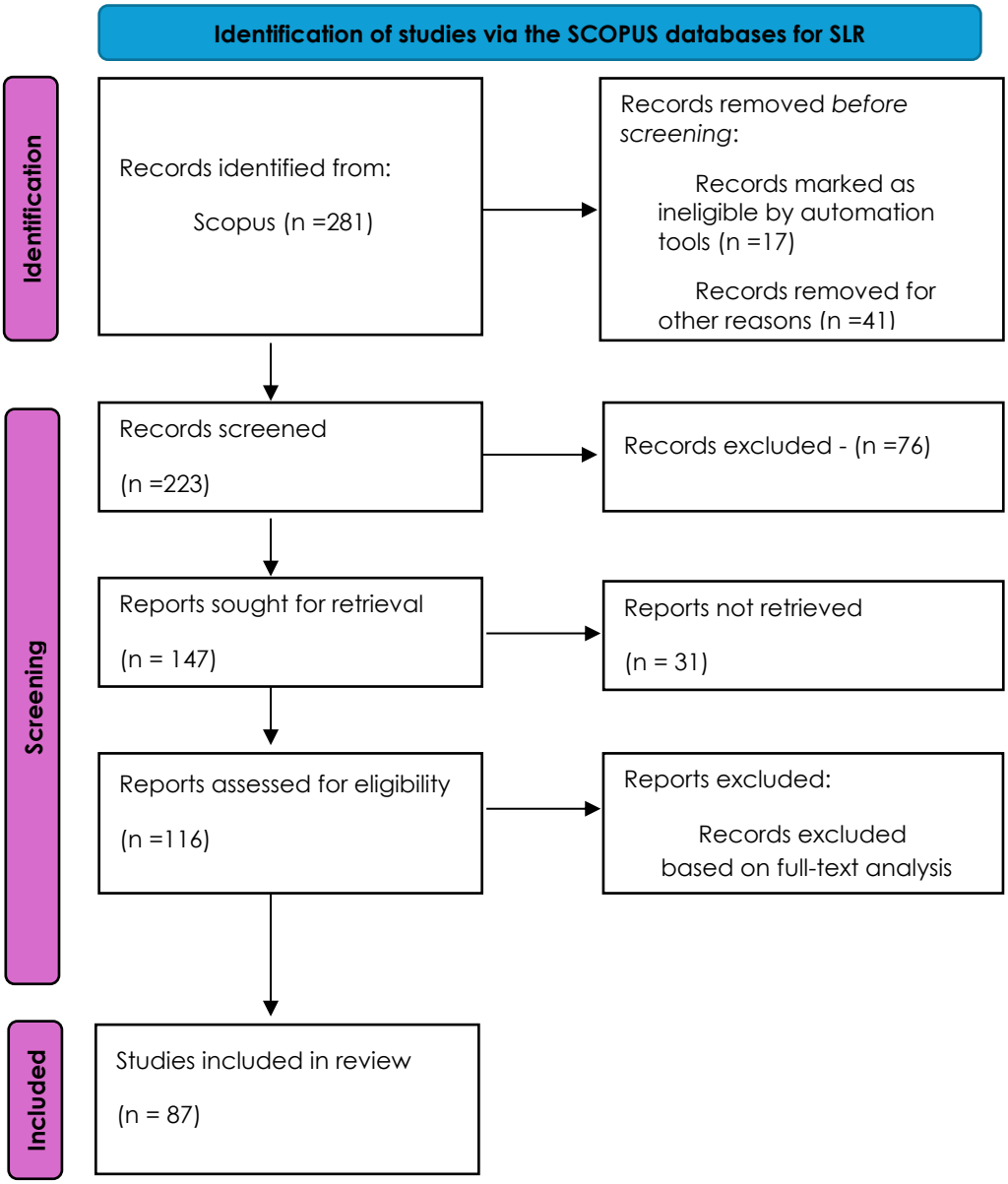

Figure 1. Identification of Studies via Databases on PRISMA for SLR

The inclusion criteria encircled papers published between 1999 and 31st December 2025, which were searched based on the search criteria used. This was selected to focus on the most recent literature (and experience of users) on digital interoperability as a catalyst for

research dissemination in architecture and the built environment, Peer-reviewed articles, and conference papers cutting across the major categories of the Elsevier journals, such as Physical sciences and engineering, Life Sciences, Health Sciences, and social sciences and humanities; qualitative, quantitative or mixed methods research; research investigating factors influencing log-in system design, and research aimed at investigating the challenges and benefits of the single log-in system. The final screening retained only 87 documents, including 61 conference papers and 23 journal articles.

3.2 Case Study

Secondly, the study utilised a case study to contextualise the real-world application of interoperable log-in systems (Kilroy, 2021), which gave context to theoretical findings from systematic reviews. It also highlighted real-world practical challenges, benefits, and key factors influencing the need for interoperable log-in systems, especially within academia (Liu & Panagiotakos, 2022)

3.2.1 Case Study Data Collection

This particular portfolio was chosen as a sample case study due to its inclusion of the fundamental scholarly literature pertaining to architecture, urban planning, and the constructed environment. Analysing this database provides a flexible structure for evaluating the digital interoperability challenges faced by the international built environment research community. The log-in interface of each journal was evaluated during the data collection phase. From the original cohort of 183 journals, 5 were inaccessible owing to server malfunctions, and 2 were omitted as duplicates. As a result, the ultimate sample size employed for the data analysis comprised 176 publications. This database analysis offers a strong and scalable framework for assessing the extensive digital interoperability issues encountered by the global built environment research community. Regarding the data collection, the authors visited the log-in interface of each journal in the Engineering and Technology category; the authors documented their observations and collected data on each interface, such as whether single sign-on is supported. Whether the same credentials can be used across multiple journals, any variations in the log-in process across journals, navigation options available post-login, and any additional features or limitations related to interoperability.

3.2.2 Case Study Data Analysis

To analyse the case study of the Journal of Engineering and Technology, the study through literature review established and defined the key criteria of interoperability for the case study data analysis such as;

- Single Sign-On (SSO) Support: The authors investigated whether any of the journals offered a Single Sign-On feature, allowing users to access multiple journals with a single set of credentials. This feature can greatly enhance user experience by streamlining the log-in process.
- Credential Consistency across Journals: The study analysed whether users could utilise the same credentials across different journals. This is essential for creating a seamless experience for researchers who frequently access multiple publications.
- Variations in the Log-in Process: The authors analysed the log-in procedures for each journal, noting any differences that could affect user accessibility. This included evaluating password requirements, user interface design, and security measures.
- Post-Login Navigation Options: Once logged in, the authors assessed the available navigation options within each journal. They focused on easy access to important

sections such as the main menu, submission portals, and help resources. Understanding how users navigate post-login is critical for evaluating the overall usability of the journal platforms.

Additional Features and Limitations: Finally, the authors documented any notable features or limitations regarding interoperability among the journals. This included assessing whether journals could effectively share user data or provide cross-platform functionality.

4. Results and Discussion

In exploring the results and discussion section, the study examined the key issues related to log-in to the interface and discussed the challenges, benefits, and factors influencing log-in system designs.

4.1 An overview of Elsevier's journal platform and its log-in system.

The Elsevier journal platform has a unique user interface with 3 key components. The first landing page briefly provides visitors with a summary of what the journal offers. Using the Accident Analysis and Prevention Journal, which is one of the journals in the Engineering and Technology category, this page briefly reveals the "Title", "Volume", "Issue", "ISSN", "Editor-In-Chief", "Impact Factor", and a summarised "Description", which can further open "Read more" redirects the reader to the description journal component which provides information on topical issues of concern to be hosted within the journal as well as affiliations if any. The page also reveals the subscription option, allowing annual personal or institutional subscriptions to the journal. The page also has product details that provide a bullet point detail of the International Standard Serial Number (ISSN), volume, issue, 5-year impact factor and the current impact factor. The final part of this page is titled "View journal on "ScienceDirect", which provides the guide for authors, policy and access to the latest articles on ScienceDirect. This particular journal exemplifies the larger issue effectively. For urban planners and architects, empirical data derived from accident analysis is essential for the design of safer, more inclusive transport infrastructures and public spaces. When this essential knowledge is confined to fragmented access portals, these digital barriers impede the conversion of engineering research into practical urban solutions.

A click on the final part redirects users to the journal page on ScienceDirect, which starts the next component. This provides information on how to submit articles and an author's guide. It also has an About section, a search function, and various drop-down menus that might meet users' needs. Clicking submit an article finally redirects users to the Log-in page, which possesses 5 different log-in options: "Author Log-in", "Reviewer Log-in", "Editor Log-in", "Publisher Log-in", and "ORCID Log-in". This page also allows for registering new users and log-in help in case one forgets the password. Furthermore, the post-login interface enables the user to perform various functions such as submitting manuscripts, revising manuscripts, tracking submission progress, and accessing help through tutorial videos.

The assessment of journal platforms brings to light several significant challenges related to interoperability and user experience across various Elsevier Engineering and Technology interfaces. As illustrated in Table 1, a primary observation is the lack of support for SSO across all platforms evaluated. This absence indicates that users must follow traditional, individual sign-in processes for each journal without the convenience of a unified access point. This result directly impacts the user experience, increasing the time and effort required to access different journals. Although users can utilise the same credentials for multiple journals, they must go through re-registration for each, further complicating access and deterring seamless interaction across platforms. The absence of SSO support across all journal

platforms is a critical issue. SSO systems allow users to authenticate once and gain access to multiple systems without needing to log in repeatedly. By not offering this feature, Elsevier journals require users to go through repeated log-in procedures, creating a fragmented and cumbersome experience.

This increases friction and reduces accessibility, particularly for researchers who frequently navigate between different journals within the platform. Despite the use of identical credentials, the need for re-registration for each journal adds further complexity and may lead to potential frustration among users. This setup is especially problematic for institutions with access to multiple journals, where a unified log-in system would greatly improve workflow efficiency. The absence of SSO integration presents a significant impediment for multi-disciplinary professionals who regularly shift across publications in environmental research, public policy, and architectural design. The lack of seamless literature cross-referencing hinders the formulation of comprehensive urban flood resilience strategies and health infrastructure policy frameworks. An interoperable environment is essential for the progression of intricate, multi-layered urban research, rather than merely a convenience.

Table I. Summary of Journals Interoperability

S/N	Checklist	Observation	Deductions
	Document observations and collect data on each interface, including		
1	SSO Supported	No	All Journal platforms are not interoperable. A standard sign-in procedure is utilised.
2	the same credentials can be used across all the journals	No	The same details can be utilised; however, re-registration is required for each journal.
3	Any variations in the log-in process across journals	No	The log-in process/procedure is uniform across all journals.
4	Navigation options available post-login	Yes	Main menu, Submit a Manuscript, About, Help, New submissions, Revisions and Completed status bars.
		Excluded Journals	
	Journal	ISSN	Remarks
5	Automatica	0005-1098	Invalid Attempt to Log in
6	Fluid Abstracts: Civil Engineering	0962-7170	The page you were looking for has not been found
7	Fluid Abstracts: Process Engineering	0962-7162	The page you were looking for has not been found
8	Geological Abstracts	0954-0512	The page you were looking for has not been found
9	Oceanographic Literature Review	0967-0653	The page you were looking for has not been found
		Duplicated Journals	
	Journal	ISSN 1	ISSN 2
10	Microelectronics Journal	0026-2692	1879-2391
11	Micro & Nanostructures	0749-6036	2773-0123

Despite the lack of SSO, the case study analysis shows that the log-in process is consistent across all journals in the portfolio. The study encounters a uniform procedure when accessing any of the journals. While uniformity can be beneficial in providing a predictable experience, the absence of any adaptive log-in methods (such as biometric authentication or multi-factor authentication) limits users' flexibility and security options. While standardising access, this uniformity does not compensate for the limitations created by the lack of interoperability.

Concerning post-login navigation and user experience, once logged in, the study discovered that users are presented with a comprehensive set of navigation options, enhancing the post-login experience. These options typically include access to the main menu, manuscript submission tools, help resources, and status bars for new submissions, revisions, and completed tasks. This structured navigation system aids users in efficiently managing their submissions and accessing essential resources. Although the initial log-in phase presents challenges, the post-login interface offers intuitive and well-organised pathways, making it easier for researchers to complete tasks. This demonstrates that while

the log-in phase is problematic, the user experience improves significantly after successful log-in.
Several journals were excluded from the study due to technical issues encountered during log-in attempts. Journals such as Automatica and Fluid Abstracts (in both Civil and Process Engineering) were found to be inaccessible, with error messages indicating that the pages could not be found. This unreliability in accessing certain journals raises concerns about platform stability and accessibility. These issues hinder user access to important research resources and suggest a potential lack of platform maintenance or technical oversight. Such errors create significant disruptions for researchers who rely on consistent access to academic resources.

Additionally, the analysis revealed the presence of duplicated journals within the database. For example, Microelectronics Journal is listed under two distinct ISSNs (0026-2692 and 1879-2391), which may confuse cataloguing, referencing, and accessing journal content. Such duplications complicate bibliographic records and indexing, leading to potential misrepresentation in citations or academic databases. Accurate cataloguing is critical for ensuring that journal articles are easily discoverable and referenced correctly, and any inconsistencies could negatively impact both authors and readers. The findings from this assessment suggest broader implications for the interoperability of Elsevier's journal platforms. The lack of SSO support, re-registration requirements, and platform reliability issues point to areas where significant improvements are needed. In an increasingly digital and interconnected research environment, providing seamless and interoperable access to journal resources is essential for maintaining a positive user experience. Currently, the platform requires users to expend additional time and effort to access each journal, limiting the efficiency and ease of use expected in a modern academic platform. Addressing these challenges could lead to substantial improvements in user satisfaction and engagement.

4.2 Factors Influencing Log-in System Design

Multiple factors are seen to influence the log-in system SSO. These include the SSO Concepts, authentication and authorisation, identity management, protocols, standards and security considerations, integration and API management, and web and application design, as seen in Figure 2.

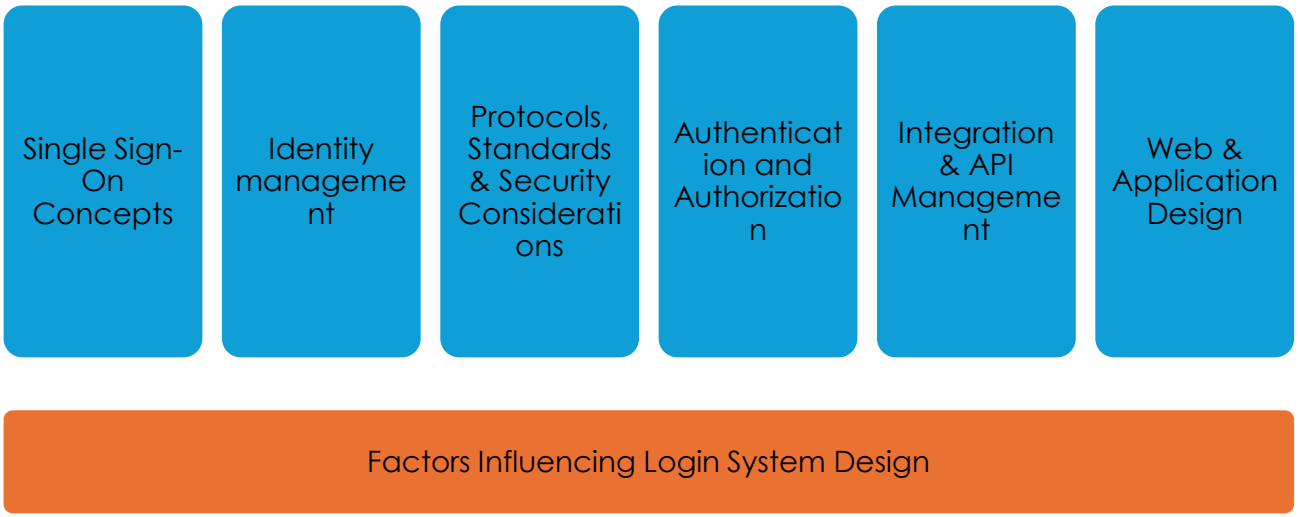

Figure 2. Factors Influencing Log-in System Design

4.2.1 Single Sign-On (SSO) Concepts

Several SSO concepts exist, such as systems, solutions, services, mechanisms, and federated patterns. The lack of cross-platform solutions has always limited the Single sign-on requirement: a single sign-on that only works on one platform or technology is nearly useless (Ormancey, 2008). For example, OAuth 2.0 is a protocol that grants authorisation online. Thus, it influences large social networks such as Facebook, Google, and Twitter to create APIs based on the OAuth protocol to improve the user experience of SSO and social sharing (Hossain et al., 2018). However, Wei et al. (2021) emphasised that securely integrating these services remains difficult, as security vulnerabilities have been repeatedly documented in recent years.

Furthermore, the increased desire for organisations to connect many web application systems into a new application to create an SSO portal (Chalandar et al., 2007) is critical. Furthermore, the fact that SSO systems allow users to utilise a single password for numerous websites rather than managing several username/password combinations contributes to their requirement (Yamaji et al., 2010). According to Zhu and Diao et al. (2010), using a global identification and password across several platforms is inappropriate for security reasons. Another contributing issue is that minimal research has been undertaken on SSO deployment on mobile platforms (Ye et al., 2016). Bilal et al. (2023) ultimately revealed weak communication service and hijacking as factors that significantly influence log-in systems design.

4.2.2 Authentication and Authorisation

An SSO solution is intended to address this issue. However, developing an SSO covering historical software products takes time and money because each legacy item typically has an authentication engine that must be redesigned. When the authentication server fails or is offline, users cannot access Web services, even if they are operational. (Patil et al. 2014). Furthermore, Goncalves et al. (2022) discovered that a person's level of trust when accessing services with their devices in various circumstances (for example, untrusted networks such as public hotspots) can influence protected data access. Another problem influencing log-in system design is a lack of awareness of integration needs and the complexity of implementing programs inside black-box web servers (Zhou & Evans, 2014). Another element to consider is the need for a single sign-on solution that is open-standard, product-neutral, and developer-independent to be widely used (Boonmee et al., 2011). Furthermore, Chavan (2018) discovered that in certain contexts, the need for protecting so-called "server-side" tools (i.e., apps that handle business logic) as well as creating HTML code for the User Interface (UI) is another important aspect that influences log-in system design.

4.2.3 Identity Management

In terms of identity management, trust information with regards to service access Goncalves et al., 2022) irrespective of wide usage in several domains (enterprise, web applications), dynamically distributed identity information and delegate identity tasks across security domains (Maler & Reed, 2008) as well as simplified authentication processes keeping the underlying software unmodified (Short et al., 2017) are identity management factor that influences log-in system design. The limited level of authorised access in some circumstances when the trusted Identity Provider (IdP) cannot provide enough user information to the service provider (SP), according to Yamaji et al. (2010), is a factor for consideration. Sciarretta et al. (2016) revealed that the lack of a proper reference model for Single Sign-On (SSO) for mobile native applications is another factor that drives many social network vendors (acting as Identity Providers) to develop their mobile solutions.

4.2.4 Protocols, Standards and Security Considerations

Basney et al. (2020) discovered that while authentication seldom fails, the consequences are severe, and the underlying causes remain unknown. Basney et al. identified CILogon faults (0.4%), SAML IdP mistakes (18.8%), OIDC RP problems (36.6%), and other errors (44.2%) as factors influencing log-in system design. Furthermore, Goncalves et al. (2022) acknowledged that mistakes are why solutions like SAML and OpenID Connect, which rely on OAuth 2.0, are widely used to offer Single-Sign-On capabilities. According to Alessandro et al. (2017), there is a demand in the public administration arena to simplify and streamline how to provide services to residents and businesses through cloud computing. This, however, presents significant issues for security and trust. However, Ferry et al. (2015) hypothesised that when properly implemented, the OAuth 2.0 standard can be a secure authorisation system. This was due to the discovery of high-impact exploits resulting in account hijacking by some large websites. Furthermore, the lack of cross-platform solutions has always limited the demand for Single Sign On (Ormancey, 2008). However, it is exposed to security issues when moved to the mobile environment. (Kah & Katuk, 2018)

4.2.5 Integration and API Management

According to PT.XYZ, an educational consulting company, one major factor influencing the design of log-in systems is the prevalence of human errors, such as employees forgetting passwords on an application due to the number of applications and credentials (Syarif et al., 2022). In addition, there are issues with session sharing across cross-platform web apps and the difficulty of SSO implementation (Yang & Yang, 2014). Furthermore, because of the risk of unauthorised access, reliable identification of users is required. The loss of critical information makes clients knowledgeable enough to know who they are dealing with, necessitating a Centralised Authentication System (CAS) (Sharma & Sihag, 2016). Chayan (2018) discovered that the fragmented structures between a "single page" UI in a browser and one or more back-end servers influence log-in system design.

4.2.6 Web and Application Design

When it comes to web and application design, Loomba et al. (2022) believe that the primary factor that could influence the design of log-in systems is the goal of developing an information architecture to support data workflows throughout the research lifecycle for cross-state teams of translational researchers. However, the major problem of such flows is the token transfer from the IDP's popup/iframe to the primary window of the Single Page (SP) (Jannett et al., 2022). Jannett et al. (2022) state that an account takeover is feasible if the token is leaked to an attacker. Fett et al. (2014) believe that the web is a complex infrastructure, and as seen by various attacks, careful study of standards and online applications is required. However, in Akhawe et al.'s (2010) case study of five security mechanisms, including HTML5 forms, Referer validation, and a single sign-on solution, three distinct threat models were discovered that can be used to analyse web applications, ranging from a web attacker who controls malicious web sites and clients to stronger attackers who can control the network and leverage sites designed to display user-supplied content. The design of contemporary login systems is progressively shaped by the transition to passwordless and decentralised models. Akman and Dalkılıç (2025) emphasise that real-time communication protocols, such as WebSockets, and dynamic QR-code techniques are essential components in the design of multi-domain SSO systems to eradicate human credential input. The demand for data sovereignty concurrently impacts system design; Horký and Caha (2024) observe that self-hosted architectures and interchangeable storage layers, when combined with SSO providers, allow organisations total control over their data ecosystems. Moreover, Balatska et al. (2024) underscore the significance of blockchain

technology, wherein decentralised identity frameworks, smart contracts, and non-fungible tokens (NFTs) are emerging as novel elements for administering access control independent of centralised databases.

4.3 Challenges of implementing SSO

From the SLR, the challenges associated with log-in systems are categorised into six major groups: security, authentication and access management, technical implementation challenge, web application and integration, policies and guidelines, and user experience and satisfaction, as seen in Figure 3.

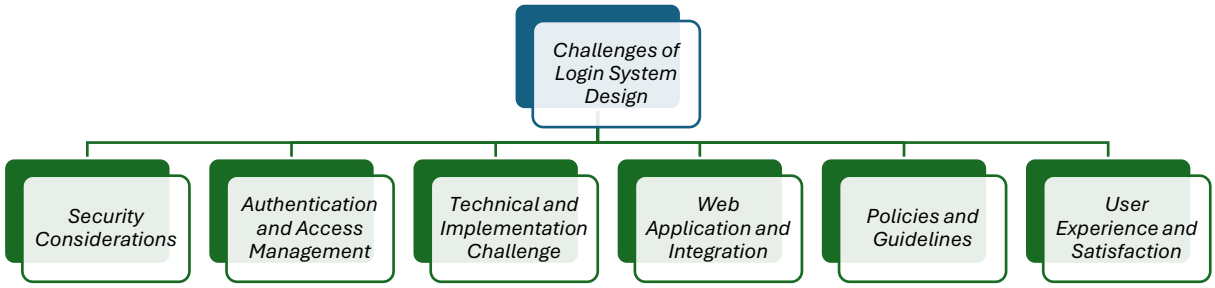

Figure 3. Challenges of implementing a log-in system design

4.3.1 Security Considerations

Security is a critical challenge for Log-in Systems. For example, according to Naito et al. (2007), many authentication processes generate a large amount of authentication data for each person, which raises administrative expenses while decreasing information system security. According to Bilal et al. (2023), hijacking is yet another issue that substantially impacts web communication. Deeptha and Mukesh (2015) classify log-in system security as assaults that allow a malicious service provider multiple access to a lawful user username/password and a third party with no security credentials. Bangalore and Sood (2009) backed this by claiming that increasing numbers of web servers are compromised yearly due to malware attacks. According to Zhang et al. (2023), the initial level in the security system is log-in and ID authentication, which serves as the foundation for establishing access control. According to Bilal et al. (2023), the fundamental criterion for the efficient performance of any Web system is perceived latency, which is the time it takes to open a Web page. As a result, wireless networks require user privacy and authentication. Setiawan et al. (2016) thus revealed that using SSO with the OAuth method on web portals could enhance the security of user data.

Notwithstanding its benefits, the implementation of complex SSO systems presents novel technical and security challenges. Akman and Dalkılıç (2025) assert that although passwordless and QR-based single sign-ons mitigate conventional phishing threats, they add new dangers, including QR hijacking, replay attacks, and session binding flaws, necessitating rigorous token validation and ephemeral credentials. Furthermore, Horký and Caha (2024) indicate that dependence on cloud-based SSO and storage solutions may provide significant privacy and security compliance challenges for certain organisations, exacerbated by the absence of safe open-source alternatives and the persistent risk of email injection attacks. Transitioning to decentralised SSO models presents challenges; Balatska et al. (2024) warn that incorporating blockchain into access management may lead to performance degradation as blockchain size increases, as well as complications in integrating with legacy systems and achieving complete data anonymisation.

4.3.2 Authentication and Access Management

User authentication and access control will be another difficulty. According to Yang and Yang (2013), session sharing among cross-platform web apps and the deployment of SSO are problematic due to their complexity. However, Nishimura and Sato (2008) propose the LESSO protocols and certificate authentication, which allow authentication information to be shared between servers. When the authentication server fails or is offline, users cannot access Web services, even if they are operational. Patil et al. (2014). According to Goncalves et al. (2022), authentication and access settings are necessary on all available applications since existing and future networks must address identity management to authenticate and authorise users to access services.

Singh (2012) demonstrates that with greater sharing, there is a pressing need for access control regulations and systems to preserve users' privacy. However, according to Komorowski et al. (2016), several log-ins and passwords are required when surfing the web, making it difficult for users to manage them. Still, many entities require various web-based applications for operational activities, making centralised access management for web-based applications very much needed (Hermawan et al., 2023). For the sake of security, it is improper to use a global identifier and password among several systems; hence, the SSO is the most popular schema proposed to solve the problem (Zhu & Diao, 2010).

4.3.3 Technical and Implementation Challenges

Implementation and technological challenges have also been identified as issues with log-in systems. For example, Maler and Reed (2008) said that security and privacy concerns provide a hurdle for implementing human digital identities. As a result, successfully integrating third-party services into web applications is difficult, and errors can have serious consequences when using third-party services for security-critical tasks like authentication and authorisation (Zhou & Evans, 2014). Another problem has been the increasing amount of information stored and shared on various online platforms, which is often impossible without sharing the account (Gupta et al., 2023). Furthermore, due to the fundamental difference between the isolation mechanisms in mobile operating systems and applications and the origin-based isolation in browsers, SSO encounters a fresh attack surface and adversarial models. (Ye et al. 2016).

4.3.4 Web Application and Integration

Most web application log-in systems' success depends on integrating with other enterprise systems rather than exclusively on the tool's merits, such as ORCiD ID (Powell et al., 2019). Thus, Langenberg and Dryndos (2016) state that collaborations between SMEs differ from those between traditional OEM-supplier chains. However, unless the activities have been designed to facilitate web applications, integrating their analytics into a single dashboard can require significant development effort. (Martínez-Ortiz et al., 2019)

4.3.5 Policies and Guidelines

Policies also pose a barrier because regulatory measures require specific systems to adhere to established procedures/protocols within a geographical, business, or academic setting. For example, in scenarios with numerous secure authentication and authorisation solutions for web apps, their adaptation to the mobile context represents a new and open challenge that necessitates important recommendations and policy orientations (Sciarretta et al., 2016; 2017). On the other hand, if rules exist, such as the most recent version of the environmental management system standards, ISO 14001:2015, revisions may impact the

data and information required for decision-making and accomplishing organisational objectives (Susanto & Mulyono, 2018).

4.3.6 User Experience and Satisfaction

It is vital to emphasise that a single log-in server approach is motivated by resource efficiency, increased security, security management flexibility, increased IT productivity, and improved overall user happiness (Encheva and Tumin, 2008). According to Bacher's (2012) research, identifying and implementing various methods, such as touch gestures for improved user experience in desktop log-in systems, is difficult. According to Yamaji et al. (2010), in a federation, SSO for web apps can be performed by authenticating at the user's home organisation, known as the identity provider (IdP), and authorising at the service provider (SP). For the built environment scholar, this federated approach is not simply a technical convenience; it serves as the conduit that unites fragmented domains of knowledge. A unified identity provider enables researchers to seamlessly navigate the digital academic landscape, whether extracting spatial data from an engineering repository, cross-referencing public policy literature, or retrieving environmental impact assessments, akin to the fluidity necessary for designing sustainable physical environments.

4.4 The Benefits of SSO

From the SLR, there were several benefits of designing an effective single log-in system. However, all identified benefits were grouped into five major themes: enhanced user experience, security enhancement, simplified identity management, operational efficiency, trust and privacy.

4.4.1 Enhanced User Experience

Users' experience with a particular web user interface could determine if they visit such web spaces again. Susanto and Mulyono (2018) thus state that adopting SSO improves user experience within their web spaces. Similarly, a unified user log-in interface would make it easier for users to access the web, enhancing user experience while providing seamless and secure access and removing the fear of having multiple passwords by heart (Nishimura & Sato, 2008; Gupta et al., 2023; Murri et al., 2011). Furthermore, the degree of ease of operation and service use, according to (Komura et al., 2009), as well as the supporting statement that a single log-in system empowers users by enabling direct interactions between IDps (Identity Providers) and SP (Service Providers) provides another key benefit (Maler & Reed, 2008). Maler and Reed (2008) also suggested that human digital IDs could simplify network usage and enable new types of applications. Furthermore, the simplicity and standardised development of web applications, especially single log-in systems, allow for an easy-to-use platform with a trustworthy exchange of identity-related information (Short et al., 2017), reduced authentication time of users to access (Chalandar et al., 2007), and creates a formal foundation for web security (Akhawe et al., 2010).

4.4.2 Security Enhancements

It can be implied that the whole idea of a unified user log-in interface is to ensure that users' information is secure while removing the complexity of holding multiple passwords to heart. In other words, Nishimura & Sato (2008) state that enhanced security benefits SSOs. This degree of security enhancement is achieved as SSO provides stronger authentication (Höhnlein et al., 2014). Höhnlein et al. (2014) state that this is achieved via security for dispersed authentication infrastructures and privacy-friendly identity management technologies in the future. Furthermore, with a higher level of security, better performance

through a secure architecture, distributed APIs, and harmonised metadata is achieved (Loomba et al., 2022). This eliminates the need for registration by adding support to third-party authentication systems (Gougousis & Bailly, 2016), preventing unauthorised access, which is more secure, minimising phishing attacks, allowing the system to run stably and achieving the expected effect (Zhang et al., 2023; Qbea'h et al., 2023; Bilal et al., 2019).

The advancement of SSO technologies offers significant advantages for user experience and organisational security. Transitioning to passwordless, QR-based Single Sign-On architectures facilitates seamless authentication, markedly diminishing the dangers of phishing and credential exposure by entirely eliminating human password input from the user process (Akman & Dalkılıç, 2025). Moreover, incorporating SSO into self-hosted apps streamlines account administration and enhances data security, as local systems are not required to retain important passwords (Horký & Caha, 2024). Structurally, the implementation of decentralised SSO with blockchain technologies distributes authentication data, hence removing centralised failure points and offering enhanced transparency and immutable access records for secure audits (Balatska et al., 2024).

4.4.3 Simplified Identity Management

A user's identity is locked within the web app (Elsevier). These key details could potentially give away little information from user preferences to vital information such as credit card details. However, SSO has allowed for a common secure authentication and authorisation framework (Patil et al., 2014), creating a system which not only secures user data but is flexible and orderly enough to allow log-in to third-party web applications without the need to create a new identity (Zhou & Evans, 2014). In other words, this ability of the SSO reveals an evolution in identity management (IdM) beneficial as it allows for uniform identity authentication among heterogeneous systems with the capability to detect, display, and modify multiple different SSO protocols at the same time (Zhu & Diao, 2010; Murri et al., 2011; Pérez Méndez et al., 2016). According to Zhao et al. (2016), the SSO's benefits are that it supports hybrid authentication protocols, eliminating a single point of failure and single-point bottleneck. According to Zhang et al. (2023), another advantage is that the SSO can determine whether a user's true identity is congruent with their stated identity and prevent unlawful users from infiltrating the Web application system via key authentication mechanisms. SSO systems simplify log-in procedures by issuing authentication tokens to Service Providers (SPs) (Yamaji et al., 2010).

4.4.4 Operational Efficiency

SSO reduces the complexity of usage and management of users' credentials (Rieger, 2009). Furthermore, a decreased operational risk is achieved through access checks and access remediation if/when needed. This is achieved through a multiple-tiered security hierarchy infrastructure for web applications (Naito et al., 2007), allowing for dynamic changes in the multi-level analysis (Martínez-Ortiz, 2019). Furthermore, SSO serves as a solution for conducting performance testing on web applications, allowing data access from anywhere and getting the latest information (Setiawan, 2016). With easy access to distributed data sources, simplified manual use of authentication is achieved (Langenberg & Dryndos, 2016). Alessandro et al. (2017) further revealed that SSO has increased efficiency, effectiveness, transparency, and interoperability thanks to cloud computing. It can also help to organise existing user data, ensuring the efficiency of data security due to the usage of centralised storage (Setiawan et al., 2016). Operationally wise, the SSO is cost-effective (Stojanovski, 2022; Langenberg & Dryndos, 2016; Nishimura & Sato, 2008)

4.4.5 Trust and Privacy

Trust and privacy are another optimal benefit to the SSO. According to Goncalves et al. (2022), SSO provides a feasible approach to convey trust in federated environments. This allows for the federation of identity, attribute, authentication, and authorisation information while delivering truly extended Single sign-on solutions (Ormancey, 2008). Chavan (2018) further revealed that SSOs ensure the security of web applications. This is achieved through respect for user privacy ensured by secured cookies and the capability to detect system vulnerabilities (Komorowski et al., 2016; Mainka, 2013; Samar, 1999). The practicality of the SSO approach to convey trust with minimum impact in conformity and effective end-to-end data tracking was revealed as another benefit by Goncalves et al. (2022) and Rath et al. (2023). Additionally, Anwander et al. (2013) revealed that it enables service providers to make fine-grained authorisation decisions for individual access to protected online resources. This improves security by providing extra protection (Park & Redford, 2007). SSOs are also beneficial as they give users trust through certificate authentication and methods for sharing authentication information between servers (Nishimura & Sato, 2008).

4.5 Implications for Built Environment Research and Scholarly Publishing

According to Yamaji et al. (2010), in a federation, SSO for web apps can be performed by authenticating at the user's home organisation, known as the identity provider (IdP), and authorising at the service provider (SP). For the built environment scholar, this federated approach is not simply a technical convenience; it serves as the conduit that unites fragmented domains of knowledge. A unified identity provider enables researchers to seamlessly navigate the digital academic landscape, whether extracting spatial data from an engineering repository, cross-referencing public policy literature, or retrieving environmental impact assessments, akin to the fluidity necessary for designing sustainable physical environments. By removing login friction, publishers can foster an uninhibited flow of data, enabling architectural researchers to swiftly pair technical materials science records with spatial blueprints a cross-disciplinary dissemination process crucial for advancing responsive urban design.

From a technical data architecture perspective, the discovery of duplicated journals within the database points to underlying data management issues. Duplicate entries, such as the Microelectronics Journal appearing under two different ISSNs, can create confusion for users, libraries, and indexing services. It complicates tasks like tracking citations, managing institutional subscriptions, and ensuring accurate referencing. This finding suggests a need for stricter data quality control and regular database audits to ensure the integrity of the journal catalog. Resolving these duplications is a necessary step toward improving the overall reliability and usability of the platform. For publishers hosting vital structural engineering and spatial science repositories, rectifying these database anomalies is an infrastructure necessity; it guarantees that cross-disciplinary architectural teams can locate and reference critical built-environment findings without navigating fragmented indexing trails.

To systematically resolve these deficiencies and keep pace with modern technical standards, publishers must look toward advanced structural options. Akman and Dalkılıç (2025) emphasise that real-time communication protocols, such as WebSockets, and dynamic QR-code techniques are essential components in the design of multi-domain SSO systems to eradicate human credential input. Simultaneously, accommodating the growing

demand for infrastructure autonomy requires a shift in storage design, as Horký and Caha (2024) observe that self-hosted architectures and interchangeable storage layers, when combined with SSO providers, allow organisations total control over their data ecosystems. Moreover, [to fully modernize access control models independent of traditional, centralized vulnerabilities,] Balatska et al. (2024) underscore the significance of blockchain technology, wherein decentralised identity frameworks, smart contracts, and non-fungible tokens (NFTs) are emerging as novel elements for administering access control independent of centralised databases. Adopting these decentralized access infrastructures will fundamentally streamline the dissemination of technical architectural research, providing a secure, high-speed framework for transferring extensive spatial models and building information data across diverse scientific disciplines.

5. Conclusions

This research provides a comprehensive exploration of the interoperability challenges in the login systems, utilising Elsevier journals as a case study, with a focus on enhancing user experience through interoperable login mechanisms. The study systematically reviewed 176 journals in the fields of engineering and technology, assessing their login interfaces and the extent to which they support SSO and other interoperability features. The study revealed that Elsevier journals largely lack support for SSO, requiring users to log in separately for each journal, leading to fragmented and inefficient access. Although users can reuse the same credentials, they must still re-register across different journals. Crucially, while this investigation maps the technical parameters of these interfaces, it did not directly measure actual user experience, user satisfaction, or numeric research productivity metrics; therefore, it cannot empirically conclude that a lack of SSO explicitly hinders research dissemination. Instead, the observed lack of authentication interoperability may create additional access friction for users and hamper the seamless academic workflow researchers, academics, and students expect from modern digital platforms. Some factors influencing the login system design are identity management, protocol standards and security considerations, web and application design, etc.

The challenges of implementing SSO cuts across security considerations, policies and guidelines, User Experience and Satisfaction, Web Application and Integration, etc. The benefits of SSO include enhanced user experience, simplified identity management, and operational efficiency and so on. In critically evaluating these structural dynamics, it is necessary to explicitly discuss the limitations of the study more explicitly and suggest directions for future research. To this end, it must be acknowledged that the study focused primarily on Elsevier's engineering and technology journals, meaning the findings may not be fully generalizable to other academic fields or publishers. To address these structural constraints, further studies could extend this research by comparing Elsevier's login system with those of other academic publishing platforms to identify best practices. There is also scope to explore the integration of advanced authentication methods, such as biometric or multi-factor authentication, to enhance both security and user experience.

To modernise the architecture publication environment, publishers should investigate decentralised and passwordless access mechanisms. Balatska et al. (2024) assert that the incorporation of blockchain technology into SSO systems presents distinctive remedies for current deficiencies and introduces enhanced capabilities for identity protection. Moreover, Akman and Dalkılıç (2025) assert that passwordless methods, including QR code-based mobile authentication, not only augment user experience but also bolster security by diminishing dependence on conventional passwords. Implementing these advanced interoperable frameworks will greatly enhance information transfer among the disciplines

of the built environment. Finally, studies that investigate the perspectives of end-users through surveys or interviews could provide deeper insights into their experiences and expectations regarding login systems. Synthesizing these thematic elements, the significance of this study lies in its contribution to access policy development for publishers hosting vital spatial, architectural, and environmental science literature. By addressing the lack of interoperability in login systems, the study highlights areas for improvement that can lead to more efficient access to scholarly resources. This is especially important in the context of the digital age, where seamless access to academic content is critical for research productivity and knowledge dissemination. The study recommends adopting a unified login system, such as SSO, across its journal platforms to streamline user access. This would reduce the need for repeated logins, improve user satisfaction, and enhance the overall efficiency of academic workflows. Additionally, implementing interoperable authentication systems that allow for integration with institutional credentials or third-party providers, like ORCID, could further simplify the login process.

Funding
No funding was received to develop this editorial article.

Data Availability Statement
Not Applicable.

Conflicts of Interest
The authors declare no conflict of interest.

6. References

Abdul Rahman, A. R., & Mohezar, S. (2020). Ensuring continued use of a digital library: a qualitative approach. The Electronic Library, 38(3), pp 513–530. https://doi.org/10.1108/el-12-2019-0294

Albouq, S. S., Abi Sen, A. A., Almashf, N., Yamin, M., Alshanqiti, A., & Bahbouh, N. M. (2022). A survey of interoperability challenges and solutions for dealing with them in IoT environment. IEEE Access. https://doi.org/10.1109/ACCESS.2022.3162219

Akhawe, D., Barth, A., Lam, P. E., Mitchell, J., & Song, D. (2010). Towards a Formal Foundation of Web Security. 2010 23rd IEEE Computer Security Foundations Symposium. https://doi.org/10.1109/csf.2010.27

Akman, R., & Dalkılıç, G. (2025). MSSO:QR-based passwordless single sign-on architecture for multi-domain applications. 2025 18th International Conference on Information Security and Cryptology (ISCTürkiye). https://doi.org/10.1109/ISCTRKIYE68593.2025.11224825

Alessandro, B., Barbara, R., & Alberto, P. (2017). E-government and cloud: Security implementation for services. 2017 Fourth International Conference on EDemocracy & EGovernment (ICEDEG), EDemocracy & EGovernment (ICEDEG), 2017 Fourth International Conference On, 79–85. https://doi.org/10.1109/ICEDEG.2017.7962516

Alruwaili, F. F. (2020). Artificial intelligence and multi agent based distributed ledger system for better privacy and security of electronic healthcare records. PeerJ Computer Science, 6, e323. https://doi.org/10.7717/peerj-cs.323

Anantha Bangalore, & Sood, A. K. (2009). Securing Web Servers Using Self Cleansing Intrusion Tolerance (SCIT). https://doi.org/10.1109/depend.2009.15

Anwander, M., Braun, T., Hurni, P., Staub, T., & Wagenknecht, G. (2013). User and Machine Authentication and Authorization Infrastructure for Distributed Wireless Sensor Network Testbeds. Journal of Sensor and Actuator Networks, 2(1), 109–121. https://doi.org/10.3390/jsan2010109

Ashikuzzaman, M. (2018, July 21). Open Access: An overview. Library & Information Science Education Network. Retrieved 25th May 2025 from https://www.lisedunetwork.com/open-access/#:~:text=The%20open-access%20movement%20aims%20to%20address%20the%20challenge

Ayadi, I., Serhrouchni, A., Pujolle, G., & Simoni, N. (2011). HTTP Session Management: Architecture and Cookies Security. https://doi.org/10.1109/sar-ssi.2011.5931364

Bacher R. (2012). Web2cToGo: Bringing the web2cToolkit to mobile devices. PCaPAC 2012 - 9th International Workshop on Personal Computers and Particle Accelerator Controls. 2(1), pp 4-6. Retrieved 25th May 2025 from https://proceedings.jacow.org/pcapac2012/papers/weic01.pdf

Balatska, V., Poberezhnyk, V., Petriv, P., & Opirskyy, I. (2024). Blockchain application concept in SSO technology context. CEUR Workshop Proceedings, 3654 , pp 38–49. Retrieved 25th May 2025 from https://sci.ldubgd.edu.ua/jspui/handle/123456789/13457

Basney, J., Cao, P., & Fleury, T. (2020). Investigating Root Causes of Authentication Failures Using a SAML and OIDC Observatory. https://doi.org/10.1109/dependsys51298.2020.00026

Bhana, B., & Flowerday, S. V. (2021). Usability of the log-in authentication process: Passphrases and passwords. Information & Computer Security, 30(2), pp 280–305. https://doi.org/10.1108/ics-07-2021-0093

Bilal, M., Asif, M., & Bashir, A. (2018). Assessment of Secure OpenID-Based DAAA Protocol for Avoiding Session Hijacking in Web Applications. Security and Communication Networks, 2018, 1–10. https://doi.org/10.1155/2018/6315039

Bilal, M., Showngwe, S. C., Bashir, A., & Ghadi, Y. Y. (2023). Assessing Secure OpenID-Based EAAA Protocol to Prevent MITM and Phishing Attacks in Web Apps. Computers, Materials & Continua/Computers, Materials & Continua (Print), 75(3), pp 4713–4733. https://doi.org/10.32604/cmc.2023.037071

Boonmee, C., Tharaphant, P., & Damtongsuk, P. (2011). Development of user authentication for web application sign-on mechanism using oasis SAML standard with Thai citizen ID card. Proceedings of the European Conference on e-Government, ECEG. 6(0) pp 80-86. Retrieved 25th May 2025 from https://alarcos.esi.uclm.es/ALARNET2/FILES/Congresos/2011-ECEG-Rebollo.pdf

Brembs, B., Philippe Huneman, Schönbrodt, F. D., Gustav Nilsonne, Susi, T., Siems, R., Pandelis Perakakis, Varvara Trachana, Ma, L., & Rodríguez-Cuadrado, S. (2023). Replacing academic journals. Royal Society Open Science, 10(7). https://doi.org/10.1098/rsos.230206

Budzinski, O., Grebel, T., Wolling, J., & Zhang, X. (2020). Drivers of article processing charges in open access. Scientometrics, 124(3), 2185–2206. https://doi.org/10.1007/s11192-020-03578-3

Capes-Davis, A., & Neve, R. M. (2016). Authentication: A standard problem or a problem of standards? PLOS Biology, 14(6), e1002477. https://doi.org/10.1371/journal.pbio.1002477

Chae, C.-J., Shin, Y., Choi, K., Choi, K.N., Kim, J.-S. (2014). Authentication Algorithm using OAuth Protocol in Cloud Computing Environment. International Journal of Applied Engineering Research. 9, 22. Retrieved 25th May 2025 from https://www.academia.edu/download/99939525/pdf.pdf

Chalandar, M. E., Darvish, P., & Rahmani, A. M. (2007). A centralised cookie-based single sign-on in distributed systems. https://doi.org/10.1109/itict.2007.4475639

Chavan, A. M. (2018). Web application security: CAS and beyond. https://doi.org/10.1117/12.2312062

Chen J., Akers W., Chen Y. & Watson III W. (2002) JPARSS: A Java Parallel Network Package for Grid Computing. 2002 Proceedings of the Joint Conference on Information Sciences. 3(0) pp 944-947. Retrieved 25th August, 2025 from https://lnk.ink/keWXk

Chiu, M.-C., Huang, J.-H., Gupta, S., & Akman, G. (2021). Developing a personalised recommendation system in a smart product service system based on unsupervised learning model. Computers in Industry, 128, 103421. https://doi.org/10.1016/j.compind.2021.103421

Christen, P., Ranbaduge, T., & Schnell, R. (2020). Linking Sensitive Data. Springer International Publishing. https://doi.org/10.1007/978-3-030-59706-1

Clifford, B. (2021, 20th May). Accessibility in academic publishing: More than just compliance. OUPblog. . Retrieved 25th August, 2025 from https://blog.oup.com/2021/05/accessibility-in-academic-publishing-more-than-just-compliance/

Daniel, A. O., Precious, O. I., Oluwapelumi, O., & Ebenezer, O. F. O. (2023). Adaptive Multiple User-Device Interface Generation for Websites. IUP Journal of Computer Sciences, 17(4). . Retrieved 25th August, 2025 from https://www.proquest.com/openview/609ac196a5ed05f56ef15568d3ba0722/1?pq-origsite=gscholar&cbl=2029993

de Mello, B. H., Rigo, S. J., da Costa, C. A., da Rosa Righi, R., Donida, B., Bez, M. R., & Schunke, L. C. (2022). Semantic interoperability in health records standards: a systematic literature review. Health and Technology, 12(2), pp 255–272. https://doi.org/10.1007/s12553-022-00639-w

Deeptha, R., & Mukesh, R. (2015). Single Sign-on Mechanism for Secure Web Service Access through ISSO. Journal of Communications Software and Systems, 11(1), 8. https://doi.org/10.24138/jcomss.v11i1.112

Edwards, D. J. (2018). Dissemination of research results: On the path to practice change. The Canadian Journal of Hospital Pharmacy, 68(6), 465–469. https://doi.org/10.4212/cjhp.v68i6.1503

Encheva, S., Sharil Tumin, Simos, T. E., & Psihoyios, G. (2008). Collaborative Multi-Domains Users' Authentication Framework for Shareable Web Applications. AIP Conference Proceedings. https://doi.org/10.1063/1.3037073

Esposito, C., Ficco, M., & Gupta, B. B. (2021). Blockchain-based authentication and authorisation for smart city applications. Information Processing & Management, 58(2), 102468. https://doi.org/10.1016/j.ipm.2020.102468

Ferry, E., O Raw, J., & Curran, K. (2015). Security evaluation of the OAuth 2.0 framework. Information and Computer Security, 23(1), pp 73–101. https://doi.org/10.1108/ics-12-2013-0089

Fett, D., Kusters, R., & Schmitz, G. (2014). An Expressive Model for the Web Infrastructure: Definition and Application to the Browser ID SSO System. 2014 IEEE Symposium on Security and Privacy. https://doi.org/10.1109/sp.2014.49

Fu, L. (2019). Design and Implementation of Super Mall System Based on SOA Distributed Architecture. https://doi.org/10.1109/icitbs.2019.00094

Giannakoulopoulos, A., Minas Pergantis, & Aristeidis Lamprogeorgos. (2024). User Experience, Functionality and Aesthetics Evaluation in an Academic Multi-Site Web Ecosystem. Future Internet, 16(3), 92–92. https://doi.org/10.3390/fi16030092

Giraldi, L., Giovannetti, M., & Cedrola, E. (2023). User Experience on E-learning Platforms in Higher Education. https://doi.org/10.21203/rs.3.rs-2753702/v1

Goncalves, C., Sousa, B., & Antunes, N. (2022). BIANFE: Object identification and authentication in federated scenarios. https://doi.org/10.1109/ccnc49033.2022.9700542

Gonçalves, C., Sousa, B., & Antunes, N. (2022). OIDC-TCI: OIDC with Trust Context Information. IEEE Xplore. https://doi.org/10.23919/WMNC56391.2022.9954295

Gonzalez, P., Wilson, G., & Purvis, A. (2022). Peer review in academic publishing: Challenges in achieving the gold standard. Journal of University Teaching and Learning Practice, 19(5). https://doi.org/10.53761/1.19.5.1

Gougousis, A., & Bailly, N. (2016). LifeWatchGreece Portal development: architecture, implementation and challenges for a biodiversity research e-infrastructure. Biodiversity Data Journal, 4, e9434. https://doi.org/10.3897/bdj.4.e9434

Gupta, K. M., Reddy, K. S., Lagadapati, V., Kumar, R. L., & Suryanarayana, G. (2023). Peer to Peer Credentials Sharing using RSA and Session Token Techniques. https://doi.org/10.1109/iccmc56507.2023.10083606

Hermawan, W. (2023). Single Sign On Using Keycloak Integrated Public Key Infrastructure for User Authentication In Indonesia's Electronic Based Government System. Advance Sustainable Science Engineering and Technology, 5(2), 0230204. https://doi.org/10.26877/asset.v5i2.15795

Hodapp, D., & Hanelt, A. (2022). Interoperability in the era of digital innovation: An information systems research agenda. Journal of Information Technology, 37(4), 026839622110643. https://doi.org/10.1177/02683962211064304

Hossain, N., Hossain, Md. A., Hossain, Md. Z., Sohag, Md. H. I., & Rahman, S. (2018, August 1). OAuth-SSO: A Framework to Secure the OAuth-Based SSO Service for Packaged Web Applications. IEEE Xplore. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00227

Huang, W., & Xu, J. (2009). An authentication agent for web-based system. https://doi.org/10.1109/icnidc.2009.5361056

Horký, V., & Caha, T. (2024). Web application for secure file transfer. Department of Telecommunications, FEEC, Brno University of Technology. Retrieved 20th May 2025 https://dspace.vut.cz/server/api/core/bitstreams/9a6b9729-3e98-4d40-ac7e-4ef678924929/content

Hühnlein, D., Wich, T., Johannes Schmölz, & Haase, H.-M. (2014). The evolution of identity management using the example of web-based applications. It - Information Technology, 56(3), 134–140. https://doi.org/10.1515/itit-2013-1036

Jannett, L., Vladislav Mladenov, Mainka, C., & Schwenk, J. (2022). DISTINCT: Identity Theft using In-Browser Communications in Dual-Window Single Sign-On. Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. https://doi.org/10.1145/3548606.3560692

Kah Ho, L., & Katuk N. (2018). Users' acceptance study of oauth manager module for social log-in in mobile environment. Journal of Telecommunication, Electronic and Computer Engineering 4(1) pp 41-45. Retrieved 13th September 2025 from https://jtec.utem.edu.my/jtec/article/view/4314

Katuk, N., Fong, C. S., & Chun, K. L. (2015). Security of social network credentials for accessing course portal: Users' experience. AIP Conference Proceedings. https://doi.org/10.1063/1.4937033

Khan, R. (2021). Importance of digital library in education. International Journal of Research in Library Science, 7(4). https://doi.org/10.26761/ijrls.7.4.2021.1467

Kim, K., Jo, S., Lee, H. & Ryu, W. (2010). Implementation for federated single sign-on based on network identity. INC2010 - The International Conference on Networked Computing, Proceeding. 2(0) pp 248-250. Retrieved 13th September 2025 from https://ieeexplore.ieee.org/abstract/document/5484825

Kiran, S., Mohapatra, A., & Swamy, R. (2015). Experiences in performance testing of web applications with Unified Authentication platform using Jmeter. https://doi.org/10.1109/istmet.2015.7359004

Komorowski, M., Coppens, P., Van den Broeck, W., & Braet, O. (2016). Lowering the barriers for online cross-media usage: Scenarios for a Belgian single sign-on solution. Telematics and Informatics, 33(4), pp 916–924. https://doi.org/10.1016/j.tele.2016.02.005

Komura, T, Nagai, Y., Hashimoto, S., Aoyagi, M., & Takahashi, K. (2009). Proposal of Delegation Using Electronic Certificates on Single Sign-On System with SAML-Protocol. https://doi.org/10.1109/saint.2009.53

Kornievskaia, O., Honeyman, P., Doster, B., & Coffman, K. (2001). Kerberized credential translation: Olution to web access control. Proceedings of the 10th USENIX Security Symposium. 36

Langenberg, D., & Jerzy Dryndos. (2009). Technical architecture for configurable working environments for SMEs. https://doi.org/10.1109/itmc.2009.7461381

Librero, A. F. D. (2012). Augmenting the learning management system of UP Open University. Asian Association of Open Universities Journal, 7(1), pp 55–62. https://doi.org/10.1108/aaouj-07-01-2012-b005

Loomba, J.J., Wasson, G. S., Ravi, Dash, P. K., Patterson, S. G., Potter, M. M. A., Krisch, J. E., Tenzer, M. M., Johnston, K. C., & Brown, D. E. (2021). The iTHRIV Commons: a cross-institution information and health research data sharing architecture and web application. Journal of the American Medical Informatics Association, 29(4), pp 631–642. https://doi.org/10.1093/jamia/ocab262

Mainka C., Mladenov V., Guenther T. & Schwenk J. (2015). Automatic recognition, processing and attacking of single sign-on protocols with burp suite. Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI). 14(1) pp 117-131. Retrieved 13th September 2025 from https://dl.gi.de/items/05ec142c-fac1-48fb-95ef-f7abb638b2e9

Mainka, C., Mladenov V., Somorovsky, J., & Schwenk, J. (2013). Penetration test tool for XML-based web services. CEUR Workshop Proceedings 4(0) pp 31-35. Retrieved 13th September 2025 from https://ceur-ws.org/Vol-965/mainproceeding.pdf#page=31

Makwana, J. (2022). Author and Researcher Identifier Services: A Case of Open Researcher and Contributor ID (ORCID). Retrieved 20th May 2025 from https://www.researchgate.net/profile/Sanjeev-Jain-17/publication/366528755_Author_and_Researcher_Identifier_Services_A_case_of_Open_Researcher_and_Contributor_ID_ORCID/links/63a537ff097c7832ca5baa1e/Author-and-Researcher-Identifier-Services-A-case-of-Open-Researcher-and-Contributor-ID-ORCID.pdf

Maler, E., & Reed, D. (2008). The Venn of Identity: Options and Issues in Federated Identity Management. IEEE Security & Privacy Magazine, 6(2), pp 16–23. https://doi.org/10.1109/msp.2008.50

Manzoor, A., Shah, M. A., Khattak, H. A., Din, I. U., & Khan, M. K. (2019). Multi-tier authentication schemes for fog computing: Architecture, security perspective, and challenges. International Journal of Communication Systems, e4033. https://doi.org/10.1002/dac.4033

Martínez-Ortiz, I., Pérez-Colado, I. J., Rotaru, D. R., Freire, M., & Baltasar Fernández-Manjón. (2019). From Heterogeneous Activities to Unified Analytics Dashboards. Global Engineering Education Conference. https://doi.org/10.1109/educon.2019.8725222

Moey, L. K., Katuk, N., & Omar, Mohd. H. (2016). Social log-in privacy alert: Does it improve privacy awareness of facebook users? 2016 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE). https://doi.org/10.1109/iscaie.2016.7575044

Mollakuqe, E., & Dimitrova, V. (2024). Comparative analysis of identity management, access control, and authorisation practices in public and private universities. Open Research Europe, 4, 23.

Moore, S. A. (2020). Individuation through infrastructure: Get full text research, data extraction and the academic publishing oligopoly. Journal of Documentation, ahead-of-print(ahead-of-print). https://doi.org/10.1108/jd-06-2020-0090

Murri, R., Kunszt, P. Z., Maffioletti, S., & Tschopp, V. (2011). GridCertLib: A Single Sign-on Solution for Grid Web Applications and Portals. Journal of Grid Computing, 9(4), 441–453. https://doi.org/10.1007/s10723-011-9195-y

Naito, H., Shoji, K., Hirano, Y., & Mase, K. (2007). Multiple-Tiered Security Hierarchy for Web Applications Using Central Authentication and Authorization Service. https://doi.org/10.1109/saint-w.2007.80

Nishimura, T., & Sato, H. (2008). LESSO: Legacy Enabling SSO. https://doi.org/10.1109/saint.2008.76

Omotunde, H., & Ahmed, M. (2023). A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond. https://doi.org/10.58496/MJCS/2023/016

Okonta, E. D., Oluigbo, C. U., Okeke, F. O., Nnaa, D. V., Mgbemena, E. E., & Alhassan, S. I. (2025). A digital framework for streamlining the registration process for architects in Nigeria. Journal of Umm Al-Qura University for Engineering and Architecture. Advance online publication. https://doi.org/10.1007/s43995-025-00254-6

Ormancey, E. (2008). CERN single sign on solution. Journal of Physics Conference Series, 119(8), 082008–082008. https://doi.org/10.1088/1742-6596/119/8/082008

Owczarek, D., Wojciechowski, J., J. Murlewski, Sakowicz, B., & Napieralski, A. (2006). Electronic Document Management System. https://doi.org/10.1109/mixdes.2006.1706695

Pal, S., Hitchens, M., Rabehaja, T., & Mukhopadhyay, S. (2020). Security Requirements for the Internet of Things: A Systematic Approach. Sensors, 20(20), 5897. https://doi.org/10.3390/s20205897

Panda, Subhajit & Kaur, Navkiran. (2023). Enhancing User Experience and Accessibility in Digital Libraries through Emerging Technologies. https://doi.org/10.5281/zenodo.10211088.

Pandey, P., & Nisha, T. N. (2021). Challenges in Single Sign-On. Journal of Physics: Conference Series, 1964(4), 042016. https://doi.org/10.1088/1742-6596/1964/4/042016

Park, H., & Redford, S. (2007). Client certificate and IP address based multi-factor authentication for J2EE web applications. Proceedings of CASCON. https://doi.org/10.1145/1321211.1321229

Patil, A., Pandit, R., & Patel, S. (2014). Implementation of security framework for multiple web applications. https://doi.org/10.1109/iccci.2014.6921787

Peker, S., & Gonca Gokce Menekse Dalveren. (2023). Usability assessment of scholarly publishers' online journal interfaces. Journal of Data, Information and Management, 5(4), pp 363–374. https://doi.org/10.1007/s42488-023-00110-z

Pérez Méndez, A., Marín López, R., & López Millán, G. (2016). Providing efficient SSO to cloud service access in AAA-based identity federations. Future Generation Computer Systems, 58, pp 13–28. https://doi.org/10.1016/j.future.2015.12.002

Powell, J., Hoover, C., Gordon, A., & Mittrach, M. (2019). Bridging identity challenges: why and how one library plugged ORCiD into their enterprise. Library Hi Tech, 37(3), pp 625–639. https://doi.org/10.1108/lht-04-2018-0046

Qbea'h, M., Alkaabi, J., Almansouri, S., Alneyadi, A., & Alderei, M. (2023). Classification of Authentication Approaches to Stop the Next Breaking: Challenges, Benefits, Drawbacks, Awareness, and Recommendations. https://doi.org/10.1109/icca59364.2023.10401373

Rath, S., Panda, S., Sacchettini, J. C., & Berthel, S. J. (2023). DAIKON: A Data Acquisition, Integration, and Knowledge Capture Web Application for Target-Based Drug Discovery. ACS Pharmacology & Translational Science. https://doi.org/10.1021/acsptsci.3c00034

Refka Abdellaoui, & Pasquet, M. (2010). Secure Communication for Internet Payment in Heterogeneous Networks. HAL (Le Centre Pour La Communication Scientifique Directe). https://doi.org/10.1109/aina.2010.45

Rehnbäck, O. (2023). A case study of unauthorised log-in attempts againsthoneypots via remote desktop. Retrieved 13th September 2025 from https://urn.kb.se/resolve?urn=urn:nbn:se:ltu:diva-99239

Rieger, S. (2009). User-Centric Identity Management in Heterogeneous Federations. https://doi.org/10.1109/iciw.2009.85

Riesch, P. J., & Du, X. (2012). Audit based privacy preservation for the OpenID authentication protocol. https://doi.org/10.1109/ths.2012.6459873

Rita, Valle, P. H., Santos, K. S., & Nakagawa, E. Y. (2024). Systems Interoperability Types: A Tertiary Study. ACM Computing Surveys. https://doi.org/10.1145/3659098

Samar, V. (1999, June 1). Single sign-on using cookies for Web applications. IEEE Xplore. https://doi.org/10.1109/ENABL.1999.805192

Scherer, D., Byrne, K., Hahnel, M., & Valen, D. (2020). Collaborative Approaches to Integrate Repositories within the Research Information Ecosystem: Creating Bridges for Common Goals. The Serials Librarian, 1–10. https://doi.org/10.1080/0361526x.2020.1728169

Sciarretta, G., Armando, A., Carbone, R., & Silvio Ranise. (2016). Security of Mobile Single Sign-On: A Rational Reconstruction of Facebook Log-in Solution. https://doi.org/10.5220/0005969001470158

Sciarretta, G., Carbone, R., Ranise, S., & Armando, A. (2017). Anatomy of the Facebook solution for mobile single sign-on: Security assessment and improvements. Computers & Security, 71, pp 71–86. https://doi.org/10.1016/j.cose.2017.04.011

Sciarretta, G., Carbone, R., Ranise, S., & Viganò, L. (2020). Formal Analysis of Mobile Multi-Factor Authentication with Single Sign-On Log-in. ACM Transactions on Privacy and Security, 23(3), pp 1–37. https://doi.org/10.1145/3386685

Setiawan, A., Hendayun, M. & Yanti, S.F. (2016). Implementation of single sign on using the concept of method oauth (open authorisation) on the web portal. Journal of Theoretical and Applied Information Technology. 7(2) pp 339-346. Retrieved 20th May 2025 from

https://www.researchgate.net/publication/305416954_Implementation_of_single_sign_on_using_the_concept_of_method_oauth_open_authorization_on_the_web_portal
Shahzad, K., & Khan, S. A. (2022). Factors affecting the adoption of integrated semantic digital libraries (SDLs): a systematic review. Library Hi Tech. https://doi.org/10.1108/lht-05-2022-0231
Sharma, P., & Sihag, V. K. (2016). Hybrid Single Sign-On Protocol for Lightweight Devices. 2016 IEEE 6th International Conference on Advanced Computing (IACC), pp 679–684. https://doi.org/10.1109/iacc.2016.131
Shehzad, H. M. F., Ibrahim, R. B., Yusof, A. F., Khaidzir, K. A. M., Iqbal, M., & Razzaq, S. (2021). The role of interoperability dimensions in building information modelling. Computers in Industry, 129, 103444. https://doi.org/10.1016/j.compind.2021.103444
Short, H., Manzi, A., V De Notaris, Keeble, O., A Kiryanov, Mikkonen, H., Tedesco, P., & Wartel, R. (2017). x509-free access to WLCG resources. Journal of Physics Conference Series, 898, 102001–102001. https://doi.org/10.1088/1742-6596/898/10/102001
Siau, K., & Dewester, D. (2010). Ibm power systems and service oriented architecture at bank of America's foreign items systems office. ICIS 2010 Proceedings - Thirty First International Conference on Information Systems.
Singh, K. (2012). xAccess: A unified user-centric access control framework for web applications. https://doi.org/10.1109/noms.2012.6211948
Smyth, B., & Pironti, A. (2013). Truncating TLS connections to violate beliefs in web applications. 7th USENIX Workshop on Offensive Technologies, WOOT 2013
Stojanovski, T. (2022). A New Web Application Extensibility Platform. https://doi.org/10.1109/icitee56407.2022.9954044
Sudhodanan, A., Armando, A., Carbone, R., & Compagna, L. (2016). Attack Patterns for Black-Box Security Testing of Multi-Party Web Applications. https://doi.org/10.14722/ndss.2016.23286
Sun, S.-T., Hawkey, K., & Beznosov, K. (2012). Systematically breaking and fixing OpenID security: Formal analysis, semi-automated empirical evaluation, and practical countermeasures. Computers & Security, 31(4), pp 465–483. https://doi.org/10.1016/j.cose.2012.02.005
Susanto, A., & Mulyono, N. B. (2018). Information Management of Web Application Based Environmental Performance Management in Concentrating Division of PTFI. E3S Web of Conferences, 31, 12001. https://doi.org/10.1051/e3sconf/20183112001
Syarif A., Arief A. N., Muhammad N. S., Arief A. S., & Ohliati, J. (2022). Implementation of Single Sign-on System for User Management at PT.XYZ. 2022 International Conference on Information Management and Technology (ICIMTech). https://doi.org/10.1109/icimtech55957.2022.9915069
Thibault, R. T., Amaral, O. B., Argolo, F., Bandrowski, A. E., Davidson, A. R., & Drude, N. I. (2023). Open Science 2.0: Towards a truly collaborative research ecosystem. PLOS Biology, 21(10), e3002362. https://doi.org/10.1371/journal.pbio.3002362
Tie-jun, Y., & Xiu-juan, Y. (2013). Method of single sign-on for independent web systems based on AJAX. https://doi.org/10.1109/iccsnt.2013.6967119
Vernadat, F. B. (2007). Interoperable enterprise systems: Principles, concepts, and methods. Annual Reviews in Control, 31(1), pp 137–145. https://doi.org/10.1016/j.arcontrol.2007.03.004
Wang, M., Sharmin, S., Wang, M., & Yu, F. (2021). A Mixed-Method Usability Study on User Experience with Systematic Review Software. Proceedings of the Association for Information Science and Technology, 58(1), 346–356. https://doi.org/10.1002/pra2.462
Wang, Y., Wen, Q., & Zhang, H. (2010). A Single Sign-On Scheme for Cross Domain Web Applications Using Identity-Based Cryptography. IEEE Xplore. https://doi.org/10.1109/NSWCTC.2010.120
Wei, H., Hassanshahi, B., Bai, G., Krishnan, P., & Vorobyov, K. (2021). MoScan: a model-based vulnerability scanner for web single sign-on services. Proceedings of the 30th ACM SIGSOFT International Symposium on Software Testing and Analysis. https://doi.org/10.1145/3460319.3469081
Wiefling, S., Jørgensen, P. R., Thunem, S., & Iacono, L. L. (2022). Pump Up Password Security! Evaluating and Enhancing Risk-Based Authentication on a Real-World Large-Scale Online Service. ACM Transactions on Privacy and Security. https://doi.org/10.1145/3546069
Xing, L., Chen., Y., Wang, X., & Chen, S. (2013). InteGuard: Toward Automatic Protection of Third-Party Web Service Integrations. 20th Annual Network and Distributed System Security Symposium, NDSS 2013.
Yamaji, KK, Kataoka, T., Nakamura, M., Tananun Orawiwattanakul, & Noboru Sonehara. (2010). Attribute Aggregating System for Shibboleth Based Access Management Federation. https://doi.org/10.1109/saint.2010.14
Yanfa, X., & Wenju, Z. (2016). Research on Enterprise Virtual Video Communication System Based on WEB Technology. International Journal of Simulation: Systems, Science & Technology. https://doi.org/10.5013/ijssst.a.17.03.14

Ye, Q., Bai, G., Wang, K., & Dong, J. S. (2015). Formal Analysis of a Single Sign-On Protocol Implementation for Android. 2015 20th International Conference on Engineering of Complex Computer Systems (ICECCS). https://doi.org/10.1109/iceccs.2015.20

Yusuf, M., Muhamad, Y., Reza, D. P., Ahmad, Y. F., & Agung, R. (2024). Enhancing User Log-in Efficiency via Single Sign-On Integration in Internal Quality Assurance System (eSPMI). International Transactions on Artificial Intelligence (ITALIC), 2(2), pp 164–172. https://doi.org/10.33050/italic.v2i2.556

Zhang, Y., Sun, L., Liu, X., Ai, Y., & Zhao, Y. (2023). Terminal ID Authentication System Based on Digital Certificate. 21, pp 111–115. https://doi.org/10.1109/icdsi60108.2023.00031

Zhao, G., Ba, Z., Wang, X., Zhang, F., Huang, C., & Tang, Y. (2015). Constructing authentication web in cloud computing. Security and Communication Networks, 9(15), pp 2843–2860. https://doi.org/10.1002/sec.1202

Zhou Y.. & Evans D. (2014). SSOScan: Automated testing of web applications for single sign-on vulnerabilities 2014. Proceedings of the 23rd USENIX Security Symposium. 15 (78) pp 495-510

Zhu, F., & Diao, H. (2010). Single Sign-On Assistant: An Authentication Broker for Web Applications. https://doi.org/10.1109/wkdd.2010.94

Zhu, Q., Li, P., Zhang, S., & Peide, Q. (2005) A unified authorisation platform based on RBAC4WAS model for web application system integration. Proceedings - 2005 International Conference on Cyberworlds, CW 2005. 4(0) pp 505-509. https://ieeexplore.ieee.org/abstract/document/1587587

Zink, T., & Waldvogel, M. (2017). X.509 user certificate-based two-factor authentication for web applications. Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI). Retrieved 20th May 2025 from https://kops.uni-konstanz.de/entities/publication/df9b677a-fd69-4052-82eb-f247092b9542