JURNAL UPI

Journal of Computer Engineering, Electronics and Information Technology (COELITE)

Journal homepage: https://ejournal.upi.edu/index.php/COELITE

Towards an Integrated Authentication System: Single Sign-On (SSO) Architecture for Higher Education Applications

Yusza Reditya Murti [1], Fadil Al Afgani [2], Teguh Rijanandi [3]

[1] Digital Business Study Program, School of Economics & Business, Telkom University
[2] Bachelor of Software Engineering Program, School of Computing, Telkom University
[3] Master of Cybersecurity Program, School of Computing, Telkom University
Correspondence E-mail: yuszaa@telkomuniversity.ac.id

ABSTRACT

Post-COVID-19, universities face increasing demands to enhance digital services through applications like Academic Information Systems (SIAKAD) and Learning Management Systems (LMS). Multiple applications require users to manage numerous login credentials, causing "password fatigue," reduced efficiency, and security risks. This study designed a Single Sign-On (SSO) architecture integrating authentication across internal applications, third-party systems, and Wi-Fi networks. The solution leverages Keycloak as Identity Provider (IdP), utilizing OpenID protocol for application integration and EAP-PEAP for Wi-Fi authentication. Results demonstrate successful authentication process simplification and increased user satisfaction through reduced repeated logins. System Usability Scale (SUS) testing yielded an average score of 74.22, meeting acceptable standards for enhanced user experience. Performance testing showed the system handles up to 12,000 authentication sessions with manageable CPU and RAM fluctuations. This research successfully developed an effective SSO solution addressing higher education authentication challenges. The architecture improves operational efficiency, simplifies login processes, and strengthens security while ensuring seamless integration through standard protocols and user-friendly interfaces.

ARTICLE INFO

Article History:
Submitted/Received 17 Sep 2025
First Revised 24 Sep 2025
Accepted 29 Sep 2025
First Available online 30 Sep 2025
Publication Date 01 Oct 2023

Keyword:
Single Sign-On (SSO)
Wi-Fi EAP-PEAP Protocol
Higher Education Authentication
System Usability Scale (SUS)
OpenID

1. INTRODUCTION

Post-COVID-19 pandemic, higher education institutions (universities) are faced with the demand for enhanced digital services through various operational applications, such as the Academic Information System (SIAKAD) and the Learning Management System (LMS). Adopting this technology aims to improve the efficiency of academic and administrative processes within the university environment. [1]. However, the large number of applications has created challenges for users (students, lecturers, and educational staff) who must manage multiple login credentials. [2], [3], [4]. This situation makes it difficult for users to remember passwords and requires them to log in repeatedly to various systems. Consequently, users experience "password fatigue," which drives them to use weak passwords or repeat the same password for convenience, thereby increasing system security risks [4]. Furthermore, repeated logins between applications reduce user satisfaction and increase system vulnerabilities. On the administrative side, the dynamic of user access rights (roles) changes and user management, such as account deactivation or adjusting permissions, further burdens the system's operational functions [1], [5].

To address these challenges, this research aims to design and implement a Single Sign-On (SSO) architecture for the university environment. The SSO architecture developed in this research is expected to integrate all applications used in the university. This solution not only simplifies the login process but also integrates user data into a single location (one database), reduces administrative burden, and improves security. Additionally, this research aims to design an SSO system that is easy to implement, using standard protocols that can integrate various third-party applications used in higher education environments, such as WordPress-based websites, Moodle-based LMS, Google Workspace, Microsoft Education Workspace, and Wi-Fi authentication using the Protected Extensible Authentication Protocol (EAP-PEAP).

Numerous studies have implemented SSO in higher education ecosystems using various protocol approaches, such as in the research in [2], [3], [4], and [6]. The concept of Single Sign-On (SSO) presents a strategic solution to overcome this issue, allowing users to access various resources with a single authentication process. [7], [8]. The specific implementation of SSO on Wi-Fi networks can improve security by integrating strong authentication protocols such as Protected Extensible Authentication Protocol (EAP-PEAP), which protects user credentials through an encrypted tunnel. [9], [10], [11]. The studies [3], [5], [12], and [13] Has developed SSO system architectures using various approaches. These previous findings form the theoretical foundation for the design of the solution in this study.

The solution proposed in this study is the development of an SSO architecture that integrates access for all internal applications, third-party applications, and Wi-Fi networks in a university environment. This study introduces a novel approach by integrating Single Sign-On (SSO) with Wi-Fi authentication using EAP-PEAP (Extensible Authentication Protocol-Protected EAP) in the context of Indonesian higher education. The SSO architecture in this study uses the OpenID protocol. This protocol was chosen because of its ability to easily integrate with various applications and third-party applications, such as WordPress-based websites and blogs, Moodle-based LMS, and Google Workspace. Therefore, the unique contribution of this research is not merely another SSO implementation, but a validated, scalable blueprint that bridges the gap between digital service access and physical network infrastructure within a singular, secure authentication framework for an academic environment.

Overall, this research aims to design and build a comprehensive SSO architecture that includes four main components: (a) Utilizing Keycloak as a centralized Identity Provider (IdP) connected to a directory service (LDAP) and a network authentication server (RADIUS). [7], b)

DOI: https://doi.org/10.17509/coelite.v4i2.90335
p- ISSN 2829-4157 e- ISSN 2829-4149

Integrating Keycloak and EAP-PEAP for Wi-Fi authentication, (c) Developing an SSO Portal Application to facilitate user access to all services without repeated logins, and (d) Integrating user management, activity monitoring, and access control with SIAKAD. This SSO system is expected to improve operational efficiency and user convenience in higher education institutions, while strengthening security and access management aspects.

2. METHODS

This study uses the Design Science Research Methodology (DSRM) method in designing a Single Sign-On (SSO) system architecture adapted to a college or university environment. The DSRM approach was chosen because of its ability to produce technological artifacts that are solution-oriented and relevant to practical problems through a systematic and structured process. [14], [15]. This methodology includes five main stages, namely Problem Identification and Motivation, Definition of Solution Objectives, Design and Development, Demonstration, and Evaluation. Each DSRM stage in this study can be seen in **Table 1** below.

Table 1. Stages of the DSRM Method

Research Steps	Definition
Problem Identification and Motivation	Identifying challenges and requirements through literature studies and semi-structured interviews with users at three universities.
Definition of Solution Objectives	Define the solution objectives, namely designing an SSO architecture that supports system integration, improves security, reduces authentication time, and improves user experience.
Design and Development	Designing an SSO architecture, considering several important aspects such as security, interoperability, performance, and ease of use. Development was carried out using the Software Development Life Cycle (SDLC) model.
Demonstration	Implementing the designed SSO architecture in a limited environment at a college to test the system functionality.
Evaluation	Conducting performance evaluations [7], [12] and usability evaluations [16], [17] or user experience to measure the effectiveness, efficiency, and user satisfaction with the implemented system.

3. RESULTS AND DISCUSSION

3.1. Requirements Analysis

The first crucial step before designing a Single Sign-On (SSO) system architecture for higher education is to conduct a comprehensive requirements analysis. The goal is to ensure the solution truly meets the needs of users and the organization. Universities typically have complex digital ecosystems consisting of various user types, including students, lecturers, employees/staff, top management, and administrators, all requiring access to various applications and services. The primary need is a centralized authentication system that eliminates repetitive logins, improves security, and simplifies user management.

The analysis results indicate that universities need to integrate SSO with various applications, such as the Academic Information System (SIAKAD), the learning management

DOI: https://doi.org/10.17509/coelite.v4i2.90335
p- ISSN 2829-4157 e- ISSN 2829-4149

system (Moodle), Google or Microsoft Workspace services, and the content management system (WordPress). To ensure all applications are seamlessly connected, support for standard protocols such as OpenID Connect and SAML is required.

Furthermore, universities have users with varying roles. Therefore, the system must be able to manage authorization levels and access rights appropriate to the needs of each role. On the other hand, user data synchronization is crucial. SSO needs to be connected to a central database and able to integrate with directory services like LDAP to ensure consistent user data across platforms.

Increasing use of mobile devices and wireless networks, network authentication integrated with SSO is also a necessity. Users must be able to access services securely across various devices, such as smartphones and laptops. Security is also a top priority. The system needs to implement strong authentication protocols, data encryption, and mechanisms to prevent unauthorized access. Furthermore, the architecture must be scalable to accommodate the growing number of users and applications, given that continuous access to educational resources is vital. Finally, user experience is crucial. An intuitive and consistent interface will accelerate adoption across the campus community. An ideal SSO Portal Application offers a seamless login process and a uniform interface across all access points.

By considering all the above aspects, the designed SSO system architecture is expected to serve as a strong and flexible foundation for an integrated authentication system in higher education environments, providing an optimal user experience while maintaining high security standards.

3.2. Logic Architecture Design

The diagram in **Figure 1** shows a Single Sign-On (SSO) architecture designed for a higher education environment. The developed SSO architecture uses Keycloak as the SSO server, which serves as the authentication center for various applications. All users, including students, lecturers, staff, top management, and administrators, can access all applications and services through the SSO Portal Application, which serves as the main gateway for all systems.

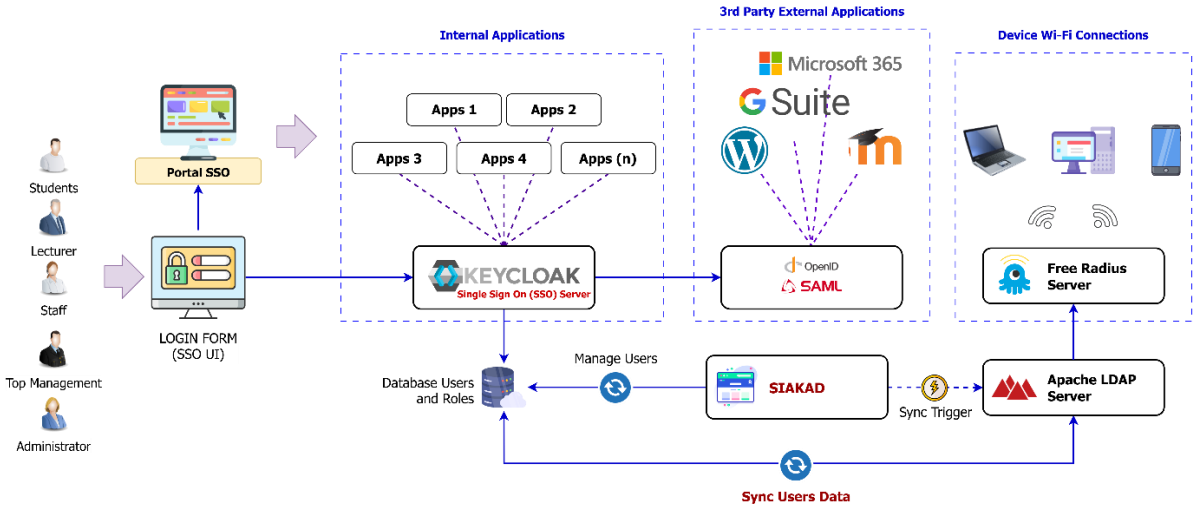

Figure 1. Logic Architecture Design SSO

SSO Architecture supports several standard protocols, including OpenID and SAML, which support various service connections, including WordPress, Google Suite, and Moodle. Keycloak serves as an identity provider that manages authentication for several different applications (Apps 1-n) through secure, token-based connections. On the data management

DOI: https://doi.org/10.17509/coelite.v4i2.90335
p- ISSN 2829-4157 e- ISSN 2829-4149

side, this architecture utilizes the Academic Information System (SIAKAD) database to store user information. This database is integrated with the Apache LDAP Server for directory services, with bidirectional synchronization ensuring consistent user data across the system. Furthermore, the Free Radius Server enables network authentication for wireless access and devices.

This architecture demonstrates a well-designed identity and access management system where user credentials are verified once through Keycloak, allowing users to log in only once to access all applications and services across the university. SIAKAD functions not only as an application but also as a user management interface, triggering synchronization with an LDAP server when user data changes. Overall, this design addresses common challenges in higher education IT environments by providing secure, centralized authentication while maintaining flexibility for diverse applications and user roles. Implementation of standard protocols (OpenID, SAML) ensures interoperability with existing and future systems, ensuring the architecture remains scalable and ready to support the growth of the institution's digital ecosystem.

3.3. Wi-Fi Connection Interface

In this section, we will show several screenshots of the settings interface on an Android device when you want to connect to EAP-PEAP (Protected Extensible Authentication Protocol) based Wi-Fi. **Figure 2** illustrates the Wi-Fi connection process for EAP-PEAP. The connection process differs from a standard captive portal. With EAP-PEAP, users simply enter their SSO username and password directly into the operating system's built-in network configuration, rather than through a browser-based pop-up window that displays a landing page, as with typical captive portal technologies. Furthermore, the SSO concept for applications utilizes KeyCloak as the application's back-end authentication, which relies on the user's master database, similar to authentication on this network. An explanation of SSO for applications is outlined in the next sub-chapter on the SSO Portal Application.

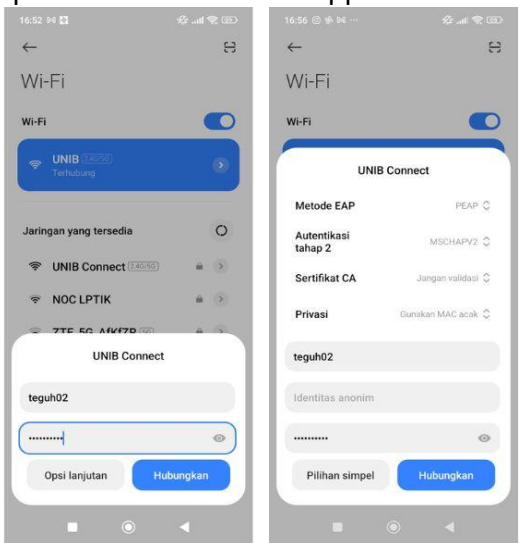

Figure 2. EAP-PEAP-based Wi-Fi connection interface on Android devices

3.4. Portal Single Sign-On (SSO)

The Single Sign-On (SSO) portal serves as the main homepage for all campus members to access digital services centrally. **Figure 3** shows the SSO portal application interface, which is designed to be concise and familiar. It includes several features, such as notifications to keep

DOI: https://doi.org/10.17509/coelite.v4i2.90335
p- ISSN 2829-4157 e- ISSN 2829-4149

users informed, a search feature to help users find application features and services, a list of application services to make it easier for users to switch between applications, and a news feature to provide users with the latest information and news.

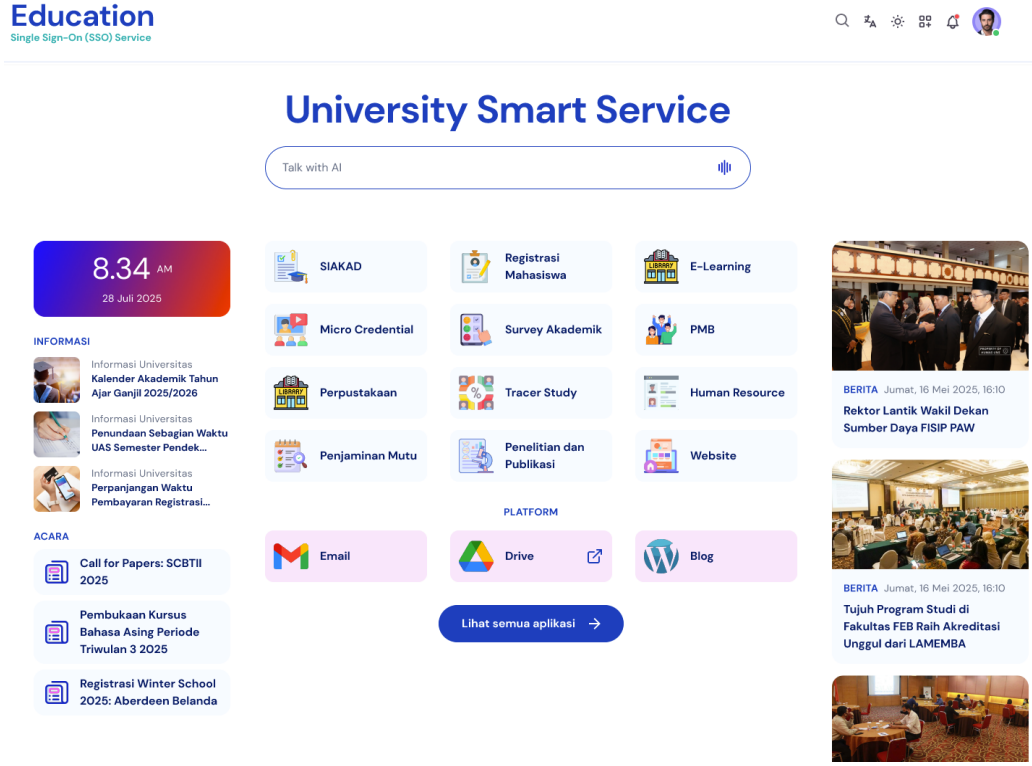

Figure 3. Interface of the SSO Portal Application

With SSO integration through Keycloak, users only need to log in once and move between applications without having to enter their credentials repeatedly. With a consistent user interface, comfortable color contrast, and typography that's readable across devices, the portal serves not only as a gateway but also as a hub for daily university activities, combining information, assignments, and applications in a simple, secure, and scalable experience tailored to the university's needs. **Figure 4** Academic Information System (SIAKAD) interface in two different display formats: the desktop view on the left and the mobile view on the right.

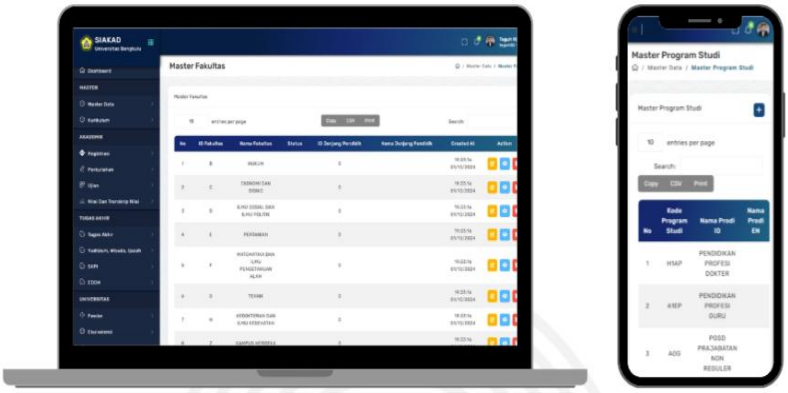

Figure 4. Academic Information System Interface (SIAKAD)

3.5. User Management and Integration

Figure 5 shows how user identities are managed and synchronized across the university's digital ecosystem. The process begins with SIAKAD (Academic Information System), which has

DOI: https://doi.org/10.17509/coelite.v4i2.90335
p- ISSN 2829-4157 e- ISSN 2829-4149

a "Manage User" function to manage user data. This user data is then stored in the SIAKAD Database (Users Database). From this database, there is a "Sync Data" process that ensures user data is synchronized to the Apache LDAP Server. The Apache LDAP Server serves as a central directory that stores user authentication information.

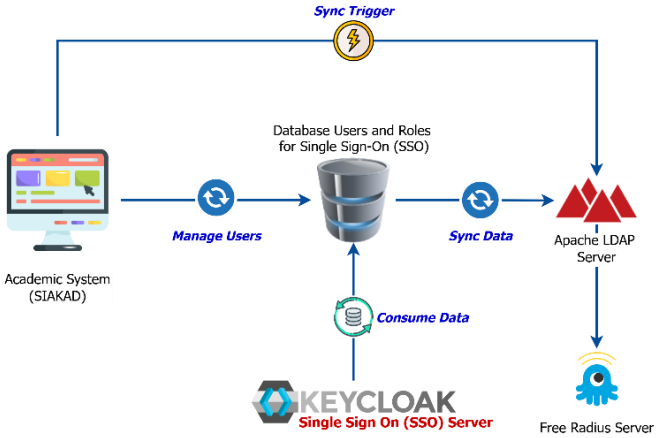

Figure 5. User Management and Integration

This server is connected to a Free Radius Server that handles device authentication, such as smartphones and laptops, via a wireless connection. With this architecture, users can access the system using the same credentials from various devices. The "Sync Trigger" flow shown from the Apache LDAP Server back to SIAKAD is used to ensure data consistency between systems. This allows changes made to the LDAP server to be forwarded back to SIAKAD to maintain data integrity. Overall, this diagram illustrates an integrated approach to user management and system integration that enables centralized identity management, Single Sign-on (SSO), and efficient data synchronization between various system components.

3.6. Deployment

The deployment section will explain the Single Sign-On (SSO) architecture concept designed in this research. A more complete explanation of the architecture is as follows. **Figure 6** illustrates several SSO components designed in this research. First, all user information is stored in a database called IAM, which is then accessed by the Keycloak server and the FreeRADIUS server, both of which serve as backends for the application and network SSO concept

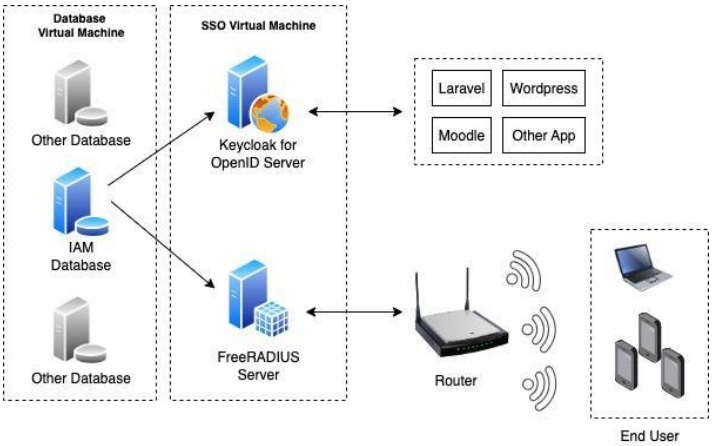

Figure 6. Single Sign-On (SSO) architecture diagram to be designed

DOI: https://doi.org/10.17509/coelite.v4i2.90335
p- ISSN 2829-4157 e- ISSN 2829-4149

First, the Keycloak server, utilizing the OpenID protocol, is used as a bridge for authentication across multiple applications. Furthermore, the FreeRADIUS server serves as a bridge for authentication sent by network devices such as routers when a new user attempts to connect to the internet. Freeradius determines whether the user's username and password are valid or invalid, allowing the user to connect or not. With this single database concept, it is hoped that network and application access will require only a single access point, as proposed by the SSO concept.

3.7. Performance Testing

In this performance testing phase, we will discuss the performance of the server design, based on the deployment points outlined previously. The performance testing is explained below. Based on **Table 2** displays several user histories that were successful ("Access-Accept") or unsuccessful ("Access-Reject") in connecting to the network, and the data is displayed in the date range of July 17, 2025, to July 31, 2025. The data is generated by FreeRadius, which is stored in the IAM database

Table 2. History of session status of users who have connected to the SSO Wi-Fi network

Date	Status	Total
17/07/25	Access-Reject	898
18/07/25	Access-Accept	146
18/07/25	Access-Reject	53
21/07/25	Access-Accept	8
21/07/25	Access-Reject	6
22/07/25	Access-Accept	50
22/07/25	Access-Reject	189
23/07/25	Access-Accept	405
23/07/25	Access-Reject	475
24/07/25	Access-Reject	2064
25/07/25	Access-Accept	469
25/07/25	Access-Reject	318
26/07/25	Access-Accept	1891
26/07/25	Access-Reject	2
27/07/25	Access-Reject	273
28/07/25	Access-Accept	3044
28/07/25	Access-Reject	387
29/07/25	Access-Accept	1372
29/07/25	Access-Reject	5830
30/07/25	Access-Accept	9293
30/07/25	Access-Reject	792
31/07/25	Access-Accept	12702
31/07/25	Access-Reject	2139

DOI: https://doi.org/10.17509/coelite.v4i2.90335
p- ISSN 2829-4157 e- ISSN 2829-4149

Figure 7 illustrates a diagram based on the historical data presented in **Table 2**. **Figure 7** shows differences in the number of user sessions with successful and unsuccessful statuses. The highest number of sessions was shown on July 29, 2025, for rejected statuses with 6,000 sessions, and on July 31, 2025, for successful statuses with 12,000 sessions.

Furthermore, the CPU and RAM usage history during testing, according to the session status history data described previously in **Table 2**, is as follows, as illustrated in Table 3 below.

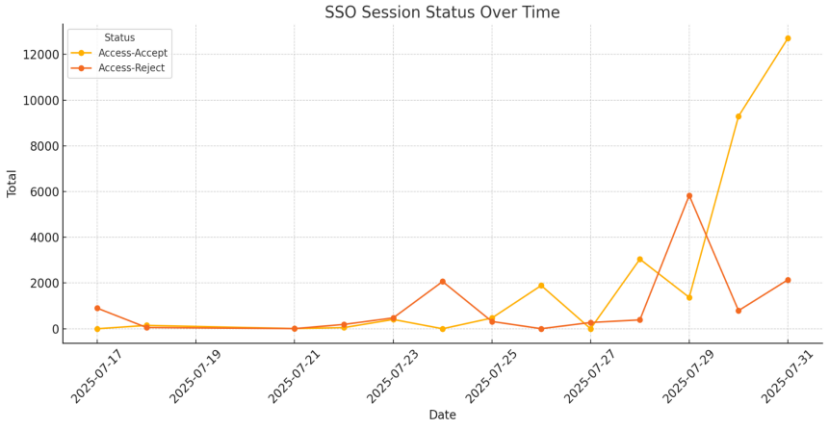

Figure 7. Total SSO session diagram

Table 3, described previously, presents the results of CPU and RAM usage collected by researchers based on the test results presented in **Table 2**. Both tables display data spanning July 17, 2025, to July 31, 2025. Table 3 shows significant changes in CPU and RAM usage on the SSO server for both Wi-Fi network authentication and application authentication. This is illustrated graphically in **Figure 8**

Table 3. History of CPU and RAM usage of the SSO *Wi-Fi* server and Application

Time	Total CPU Usage	Total RAM Usage
17/7/2025	0,03106271916	0,03266300862
18/7/2025	0,0624801238	0,06771712939
19/7/2025	0,06295687135	0,06997227645
20/7/2025	0,06343454732	0,07057634019
21/7/2025	0,06392178921	0,07418943244
22/7/2025	0,06437081225	0,07606327389
23/7/2025	0,06492218995	0,06193965521
24/7/2025	0,06528185305	0,05901939347
25/7/2025	0,06574194144	0,06649759883
26/7/2025	0,04961246821	0,05091507292
27/7/2025	0,04995151753	0,04043856865
28/7/2025	0,04999030708	0,03767043748
29/7/2025	0,05049999576	0,05111074034
30/7/2025	0,05105480152	0,05040540034
31/7/2025	0,05140933625	0,05999610294

DOI: https://doi.org/10.17509/coelite.v4i2.90335
p- ISSN 2829-4157 e- ISSN 2829-4149

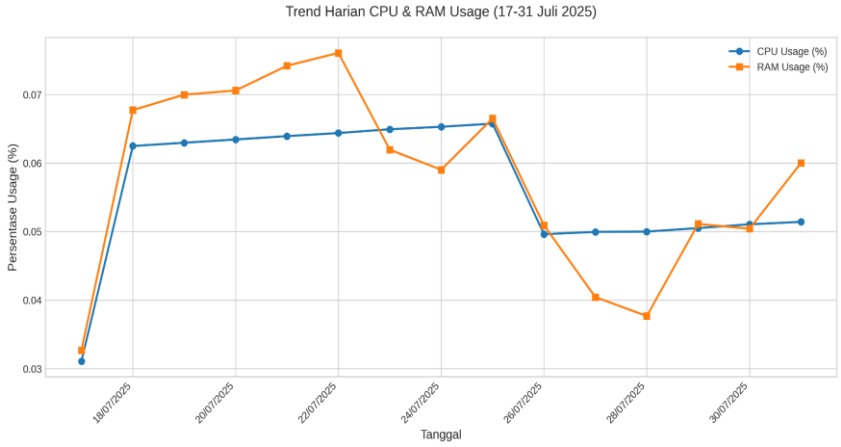

Figure 8. Diagram of RAM and CPU usage history according to the tests carried out in Table 2

As seen in **Figure 8**, CPU and RAM usage are very significant. For example, on July 22, 2025, RAM usage reached nearly 100% of its normal usage. However, on July 28, 2025, RAM usage dropped drastically to below 40%.

The performance evaluation of the proposed SSO architecture demonstrates exceptional operational efficiency and scalability. Utilizing a modest server configuration of 4 vCPUs and 8 GB RAM, the system successfully managed a peak load of 12,000 authentication sessions. Throughout this load, the resource utilization remained stable, with CPU and RAM consumption fluctuating between 40% and 80%, well below critical thresholds that would indicate performance degradation. When contextualized against established benchmarks in the literature [18], which report higher resource utilization for similar infrastructures, these results are notably superior. This favorable comparison confirms that the architected solution is not only functionally robust but also highly resource-efficient.

3.8. Usability Testing

The System Usability Scale (SUS) is a measurement instrument developed by Brooke (1996) to evaluate user perceptions of the ease of use of a system or application [16]. This measurement instrument uses ten standardized items on a five-point Likert scale, resulting in a score between 0 and 100. **Figure 9** illustrates the SUS testing process used in this study. The SUS testing in this study aimed to measure the level of system acceptance and usability of the SSO Portal Application interface design from the perspective of the academic community..

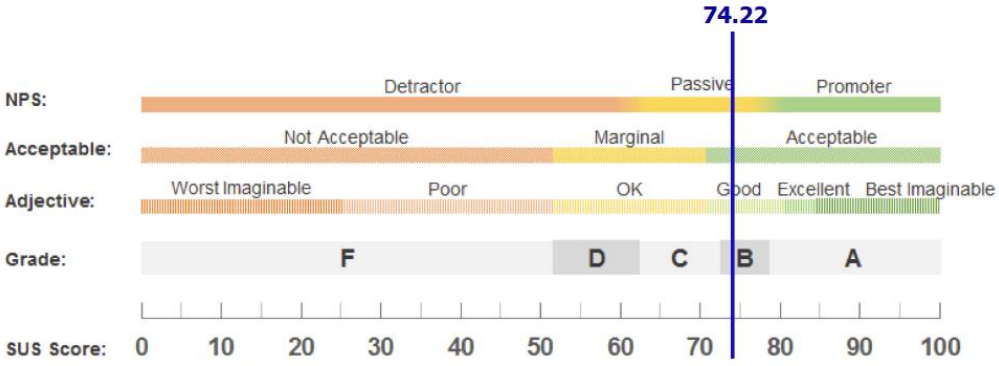

Figure 9. SUS Score Scale Result

DOI: https://doi.org/10.17509/coelite.v4i2.90335
p- ISSN 2829-4157 e- ISSN 2829-4149

The survey involved 441 respondents from three universities, consisting of students, faculty, and staff. The survey results showed an average SUS score of 74.22, with scores distributed by respondent group as follows: students (72.48), staff (75.73), and faculty (74.43). The detailed results of the SUS scores are presented in **Table 4**.

Figure 9 displays the SUS Score Scale results. The average SUS score of 74.22 places the SSO Portal Application in the B category, interpreted as "Good" based on the research [16]. This result indicates that the system has met acceptable standards (Accept), as it exceeds the acceptable usability threshold of 68. The Net Promoter Score (NPS) remains in the "Passive" category [17], indicating that user satisfaction levels have not yet reached the optimal level of loyalty for recommending the system to other potential users.

Table 4. Detailed Results of the SUS Scores

User	Jumlah Responden	SUS Score	Grade	SUS Score Range	Adjective	Accepteable	NPS
Mahasiswa	282	72.48	C+	71.1–72.5	Good	Acceptable	Passive
Staf	71	75.74	B	74.1–77.1	Good	Acceptable	Passive
Dosen	88	74.43	B	74.1–77.1	Good	Acceptable	Passive
TOTAL	**441**	**74.22**	**B**	**74.1–77.1**	**Good**	**Acceptable**	**Passive**

The usability testing results, reflected in the System Usability Scale (SUS) score of 74.22, indicate a “Good” user experience, yet the system falls within the “Passive” category, suggesting room for improvement. These results indicate that the SSO Portal Application has successfully met basic user functional needs but still requires improvements in the user experience to achieve maximum satisfaction. One possible reason for this score is the relative novelty of the Single Sign-On (SSO) system, as students and Civitas academica may not yet be fully familiar with this new approach. This lack of familiarity could contribute to the system not reaching the “Promoter” level. Similar challenges were observed in the [19], where a C+ average score was recorded, highlighting that users may require time to adjust to new systems. Furthermore, recent studies have also emphasized the need for enhanced authentication efficiency and user-centered SSO design to improve scalability and user acceptance in multi-cloud environments [20].

To bridge this gap and elevate user experience from passive acceptance to active advocacy, a multifaceted strategy is proposed for future work. First, targeted UI/UX refinements will be implemented based on detailed user feedback sessions, focusing on simplifying the portal dashboard, clarifying navigation cues, and streamlining the authentication flow between services. Second, a comprehensive and ongoing socialization campaign is crucial. This will include interactive workshops, video tutorials, and clear documentation to familiarize the academic community with the system's benefits and functionality, thereby reducing hesitancy and building confidence. Third, establishing a continuous feedback loop through embedded feedback buttons and periodic surveys will allow for real-time issue resolution and iterative design improvements. The impact of these enhancements will be rigorously measured through follow-up SUS and NPS evaluations, creating a data-driven cycle of refinement. This proactive and user-centric approach is essential for transitioning the SSO system from a functional tool to a seamlessly integrated and positively perceived cornerstone of the digital campus ecosystem

DOI: https://doi.org/10.17509/coelite.v4i2.90335
p- ISSN 2829-4157 e- ISSN 2829-4149

Test results indicate that the SSO Portal Architecture and Application implemented in higher education institutions have been well-received by the majority of users. However, there are differences in experience between user groups. The test results serve as the basis for further development, focusing more attention on the user interface and adjusting functionality to make the system more user-friendly.

4. CONCLUSION

This research has successfully designed and implemented a comprehensive Single Sign-On (SSO) architecture to address authentication challenges in a post-COVID-19 higher education environment. The success of the system implementation can be seen from the achievement of all established research objectives. The SSO architecture, developed using Keycloak as an Identity Provider (IdP), has proven capable of integrating various internal applications, such as SIAKAD, third-party applications like WordPress, Moodle, and Google Workspace, as well as Wi-Fi network access via the EAP-PEAP protocol, into a single, centralized, effective, and efficient platform.

The evaluation results demonstrate significant success in achieving the research objectives. Usability testing using the System Usability Scale (SUS) with 441 respondents from three universities showed an average score of 74.22, which indicates the system is in the "Good" category and has met acceptable standards by exceeding the acceptable usability threshold of 68. Although there are variations in scores between user groups with students (72.48), staff (75.74), and lecturers (74.43), these results demonstrate that the system has succeeded in meeting the basic functional needs of the entire academic community.

5. ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to all parties who contributed to the completion of this research. Their support was crucial in refining our ideas and ensuring the relevance of this work to real-world challenges in educational technology infrastructure.

6. AUTHORS' NOTE

This article has been reviewed using the plagiarism detection software iThenticate, and the results show a similarity index of 4%, which is within acceptable academic standards. The authors declare that all sources have been properly cited, and the work presented is original and free from plagiarism.

7. REFERENCES

[1] A. R. Pratama, F. M. Firmansyah, and F. Rahma, "Security awareness of single sign-on account in the academic community: the roles of demographics, privacy concerns, and Big-Five personality," *PeerJ Comput Sci*, vol. 8, p. e918, Mar. 2022, doi: 10.7717/PEERJ-CS.918/SUPP-2.

[2] Salmuasih and M. A. Setiawan, "Evaluasi Penerapan Single Sign-On Saml Dan Oauth 2.0: Studi Pada Perguruan Tinggi Yogyakarta," *JSiI (Jurnal Sistem Informasi)*, vol. 10, no. 1, pp. 41–49, Mar. 2023, doi: 10.30656/JSII.V10I1.6186.

[3] N. M.-J. E. dan T. Informasi and undefined 2024, "Implementasi Single Sign On (SSO) Menggunakan Protokol OAuth Pada Sistem Informasi Kampus," *jurnal.uniki.ac.idI MuslimJurnal Elektronika dan Teknologi Informasi, 2024•jurnal.uniki.ac.id*, vol. 5, no. 2, 2024, Accessed: Aug. 16, 2025. [Online]. Available: https://jurnal.uniki.ac.id/index.php/jet/article/view/515

[4] M. Yusuf, M. Yusup, R. D. Pramudya, A. Y. Fauzi, and A. Rizky, "Enhancing User Login Efficiency via Single Sign-On Integration in Internal Quality Assurance System (eSPMI)," *International Transactions on Artificial Intelligence*, vol. 2, no. 2, pp. 164–172, Jun. 2024, doi: 10.33050/ITALIC.V2I2.556.

[5] S. Student and M. Tech, "Design and Implementation of Enhanced Single Sign on System for Education Systems," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 5, no. 6, pp. 769-772–769 – 772, Jun. 2017, doi: 10.17762/IJRITCC.V5I6.851.

[6] A. Ghiffari and P. Hendradi, "Implementasi Single sign on (SSO) Menggunakan Representational State Transfer (REST) dan Open Authorization (OAuth 2.0) (Studi kasus: Universitas Muhammadiyah Magelang)," *Smart Comp :Jurnalnya Orang Pintar Komputer*, vol. 12, no. 2, pp. 356–366, Apr. 2023, doi: 10.30591/SMARTCOMP.V12I2.4939.

[7] J. Andjarwirawan, "Single Sign-On (SSO) Implementation Using Keycloak, RADIUS, LDAP, and PacketFence for Network Access," *Teknika*, vol. 14, no. 1, pp. 41–46, Mar. 2025, doi: 10.34148/TEKNIKA.V14I1.1089.

[8] G. Wang, J. Yu, and Q. Xie, "Security analysis of a single sign-on mechanism for distributed computer networks," *IEEE Trans Industr Inform*, vol. 9, no. 1, pp. 294–302, 2013, doi: 10.1109/TII.2012.2215877.

[9] T. N. Hidayat and I. Riadi, "Optimation Wireless Security IEEE 802.1X using the Extensible Authentication Protocol-Protected Extensible Authentication Protocol (EAP-PEAP)," *Int J Comput Appl*, vol. 174, no. 11, pp. 25–30, Jan. 2021, doi: 10.5120/IJCA2021920988.

[10] A. K. Yadav, M. Misra, P. K. Pandey, P. Ranaweera, M. Liyanage, and N. Kumar, "A Secure Authentication Protocol for IoT-WLAN Using EAP Framework," *IEEE Trans Dependable Secure Comput*, vol. 22, no. 1, pp. 49–65, 2025, doi: 10.1109/TDSC.2024.3388467.

[11] D. Mortágua, A. Zúquete, and P. Salvador, "Enhancing 802.1X authentication with identity providers using EAP-OAUTH and OAuth 2.0," *Computer Networks*, vol. 244, p. 110337, May 2024, doi: 10.1016/J.COMNET.2024.110337.

[12] S. K. Bhosale, "Architecture of a single sign on (SSO) for Internet banking," *IET Conference Publications*, no. 535 CP, pp. 103–105, 2008, doi: 10.1049/CP:20080155.

[13] S. Suoranta, K. Manzoor, A. Tontti, J. Ruuskanen, and T. Aura, "Logout in single sign-on systems: Problems and solutions," *Journal of Information Security and Applications*, vol. 19, no. 1, pp. 61–77, Feb. 2014, doi: 10.1016/J.JISA.2014.03.005.

[14] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of Management*

Information Systems, vol. 24, no. 3, pp. 45–77, Dec. 2007, doi: 10.2753/MIS0742-1222240302;PAGE:STRING:ARTICLE/CHAPTER.

[15] A. Hevner and S. Chatterjee, "Design Science Research Frameworks," pp. 23–31, 2010, doi: 10.1007/978-1-4419-5653-8_3.

[16] J. R. Lewis, "The System Usability Scale: Past, Present, and Future," *Int J Hum Comput Interact*, vol. 34, no. 7, pp. 577–590, Jul. 2018, doi: 10.1080/10447318.2018.1455307;WGROUP:STRING:PUBLICATION.

[17] G. W. Sasmito, L. O. M. Zulfiqar, and M. Nishom, "Usability Testing based on System Usability Scale and Net Promoter Score," *2019 2nd International Seminar on Research of Information Technology and Intelligent Systems, ISRITI 2019*, pp. 540–545, Dec. 2019, doi: 10.1109/ISRITI48646.2019.9034666.

[18] S. Fugkeaw, S. Rattagool, P. Jiangthiranan, and P. Pholwiset, "FPRESSO: Fast and Privacy-Preserving SSO Authentication With Dynamic Load Balancing for Multi-Cloud-Based Web Applications," *IEEE Access*, vol. 12, pp. 157888–157900, 2024, doi: 10.1109/ACCESS.2024.3485996.

[19] O. Suria, "A Statistical Analysis of System Usability Scale (SUS) Evaluations in Online Learning Platform," *Journal of Information Systems and Informatics*, vol. 6, no. 2, pp. 992–1007, Jun. 2024, doi: 10.51519/JOURNALISI.V6I2.750.

[20] Al-Mousa, M., & Al-Debei, M. M. (2021). Design and implementation of secure single sign-on (SSO) system for cloud-based educational platforms. International Journal of Advanced Computer Science and Applications, 12(8), 457–465. https://doi.org/10.14569/IJACSA.2021.0120853