ILKOM Jurnal Ilmiah Vol. 18, No. 2, August 2026, pp. 237-254
Accredited 2nd by KEMDIKTISAINTEK No. 10/C/C3/DT.05.00/2025; E-ISSN 2548-7779 | P-ISSN 2087-1716

Design and Quantitative Evaluation of a Keycloak-Based Single Sign-On Architecture for Integrated Institutional Information Systems

Nurhadi [a,1,*]; Mustazzihim Suhaidi [a,2] ; Muhammad Athariq [a3]
[a] *Bisnis Digital, Institut Teknologi dan Bisnis Riau Pesisir, Dumai, Indonesia*
[a] *Teknik Informatika, Institut Teknologi dan Bisnis Riau Pesisir, Dumai, Indonesia*
[a] *Teknik Informatika, Institut Teknologi dan Bisnis Riau Pesisir, Dumai, Indonesia*
[1]*nurhadi@itbriaupesisir.ac.id;* [2]*mustazzihim.suhaidi@itbriaupesisir.ac.id;* [3]*m.athariq@itbriaupesisir.ac.id*
** Corresponding author*

Article history: Received Month xx, 2021; Revised Month xx, 2021; Accepted Month xx, 2021; Available online Month xx, 2021 (Times 8pt)

Abstract

The increasing integration of digital services in higher education institutions requires a secure and scalable authentication mechanism to ensure consistent access across multiple systems. However, fragmented authentication approaches often result in repeated login processes, inconsistent security policies, and inefficient identity management. This study proposes a modular Single Sign-On (SSO) architecture based on Keycloak, integrated with OAuth 2.0, OpenID Connect, and JSON Web Tokens (JWT), to support unified authentication in institutional information systems. A quantitative experimental approach is employed to evaluate system performance in a real academic environment involving 100 user accounts. The evaluation focuses on authentication efficiency, scalability, reliability, and user productivity. The results show a 62% reduction in average login time, an 85% increase in authentication throughput, and a 100% authentication success rate. Scalability testing indicates stable system performance under concurrent workloads, while token validation overhead remains minimal, ensuring that security enhancements do not degrade system responsiveness. In addition, task completion time decreases by 51%, accompanied by a significant improvement in user productivity. These findings demonstrate that the proposed Keycloak-based SSO architecture provides measurable improvements in performance, scalability, security governance, and usability. The study contributes to software systems engineering by presenting a validated architectural model and a comprehensive quantitative evaluation framework for identity management in higher education environments.

Keywords: Single Sign-On; Keycloak; Identity and Access Management; Oauth 2.0; OpenID Connect; Institutional Information Systems

Introduction

The rapid advancement of digital technology has significantly transformed the operational landscape of higher education institutions. Universities are increasingly required to adopt integrated information systems to ensure efficiency, transparency, and accountability in academic and administrative processes [1], [2], [3]. Administrative services, particularly correspondence and document management, play a crucial role in institutional governance. However, many universities still rely on manual or partially digital systems, which are often fragmented, inefficient, and prone to data loss or duplication [4], [5], [6]. At Institut Teknologi dan Bisnis Riau Pesisir, the correspondence process involves multiple stages, including letter creation, numbering, disposition, approval, and archiving. These activities were previously handled using conventional methods or isolated applications, resulting in slow processing time, limited traceability, and difficulty in retrieving historical documents. In addition, the institution operates several independent information systems, each requiring separate authentication credentials. This condition leads to password fatigue, increased risk of weak password usage, and higher administrative overhead for user management [7], [8]. Single Sign-On is widely recognized as an effective solution to overcome authentication fragmentation by enabling users to access multiple systems using a single set of credentials [9], [10]. The implementation of SSO not only improves user experience but also enhances system security by centralizing authentication control [11], [12], [13]. Modern SSO mechanisms are commonly built upon standardized protocols such as OAuth 2.0 and OpenID Connect, which provide secure and interoperable authentication frameworks [14], [15], [16].

This research focuses on the development of e-SURAT as an integrated digital correspondence and archiving system, supported by a modern SSO architecture using Keycloak as the Identity Provider and LDAP as the centralized user repository [17], [18], [19]. The main objective of this study is to design, implement, and evaluate the effectiveness of the proposed system in improving administrative efficiency, authentication performance, and system security within a university environment. The novelty of this work lies in the integration of a critical administrative application with an open-source, standards-based SSO solution that federates a legacy LDAP directory without requiring user data migration [20], [21], [22].

In addition to improving operational efficiency, the adoption of a centralized identity management system is increasingly important in ensuring information security and system governance within higher education institutions. Fragmented authentication mechanisms not only increase administrative overhead but also expose institutions to security vulnerabilities, such as weak password policies, unmanaged user accounts, and inconsistent access control [23], [24]. By implementing a standardized authentication framework based on OAuth 2.0 and OpenID Connect, institutions can enforce uniform security policies, improve auditability, and ensure that user access rights are consistently managed across multiple digital services [7], [25], [26]. Therefore, this research contributes to the field of information systems engineering by providing an empirical case study on the integration of an electronic correspondence system with a modern Single Sign-On architecture using open-source technologies [27], [28]. Unlike previous studies that mainly focus on conceptual designs or isolated system implementations, this study emphasizes practical deployment and quantitative performance evaluation in a real institutional environment. The findings of this research are expected to serve as a reference model for other universities seeking to implement scalable, secure, and interoperable digital campus infrastructures [29].

Recent studies have explored SSO implementations using protocols such as OAuth 2.0 and OpenID Connect, as well as identity management platforms like Keycloak, particularly in academic and enterprise environments. These studies generally demonstrate improvements in authentication efficiency and security through centralized identity management. However, most existing works primarily focus on functional system implementation or conceptual architecture, with limited attention to comprehensive performance evaluation across multiple operational dimensions. In particular, there is a lack of studies that simultaneously assess authentication latency, throughput, scalability, reliability, token validation overhead, and user productivity within a unified evaluation framework. This indicates a clear research gap in the absence of a holistic and quantitative approach to measure the real-world impact of SSO adoption in institutional information systems.

To address this gap, this study proposes the integration of an e-SURAT digital correspondence system with a Keycloak-based SSO architecture supported by LDAP federation. The novelty of this research lies in the development of a comprehensive multi-metric evaluation framework that quantitatively assesses authentication performance, scalability, reliability, token validation efficiency, and user productivity in a real institutional environment. Unlike previous studies that primarily emphasize system deployment or isolated performance metrics, this research provides an empirical, end-to-end evaluation of SSO implementation under controlled experimental conditions. The main contributions of this study are: (1) a modular and scalable SSO architecture based on Keycloak, OAuth 2.0, OpenID Connect, and LDAP federation without user data duplication, (2) a systematic quantitative evaluation framework for identity management systems, and (3) empirical evidence demonstrating the impact of centralized authentication on system performance, security governance, and operational efficiency.

Method

This study adopts a Research and Development approach, which emphasizes the creation and validation of a technological product in a real organizational context. The development process follows the System Development Life Cycle model, consisting of analysis, design, implementation, and evaluation phases. This methodological framework ensures that the system is developed systematically and evaluated comprehensively. To clearly illustrate the research methodology applied in this study, the overall development process of the e-SURAT system integrated with Keycloak-based Single Sign-On is presented in **Figure 1**.

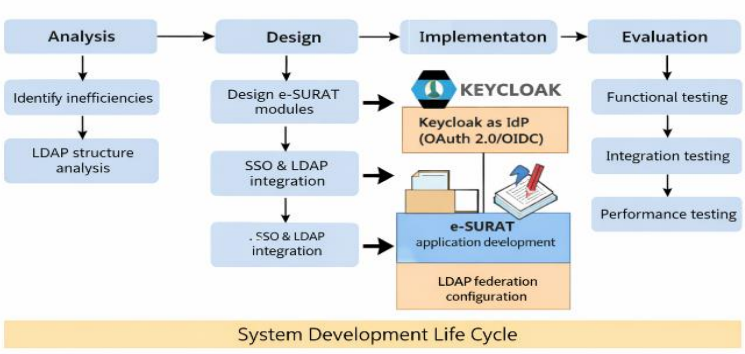

Figure 1. Research Methodology for e-SURAT with Keycloak-based SSO

A. Analysis

The analysis phase focuses on identifying system requirements and measuring the baseline performance of the existing authentication mechanism. One of the quantitative indicators analyzed in this phase is the average login time of the traditional system, which is used as a benchmark for comparison [30]. The analysis phase focuses on identifying requirements and measuring baseline authentication performance in the existing system. The average login time is used as the primary performance indicator and is defined as: [29]

$$T_{avg} = \frac{1}{n} \sum_{i-1}^{n} T_i \quad (1)$$

Where T_{avg} represents the average login time, T_i denotes the login time of the i i-th user, and n is the total number of observed users. This formula is applied to obtain baseline authentication performance before implementing the Single Sign-On mechanism.

B. Design

In the design phase, the system architecture is defined based on modular interaction between the client application, Identity Provider, and user directory. From a formal perspective, the SSO interaction model can be represented as a function-based identity mapping:

$$U_{app} = f(U_{tdap}) \quad (2)$$

Where U_{tdap} represents the user identity stored in the LDAP directory, U_{app} represents the identity used by the e-SURAT application, and $f(.)$ denotes the identity federation function performed by Keycloak through attribute mapping [31]. This function ensures that no user duplication occurs, and identity consistency is maintained across systems.

C. Implementation

The implementation phase involves authentication and authorization using OpenID Connect with JSON Web Token validation [32], [33]. The correctness of token validation is mathematically represented using a signature verification function [34]:

$$V = verify\left(Token_{jwt,} K_{pub}\right) \quad (3)$$

Where V indicates token validity, $Token_{jwt}$ is the JSON Web Token issued by Keycloak, and K_{pub} is the public key of the Identity Provider. Authentication is considered valid if $V = true$, meaning the token signature is verified and trusted by the e-SURAT system. In addition, role-based access control within the system is defined using a permission mapping function [35] :

$$Access = g\left(Role_{user,} Resource_{system}\right) \quad (4)$$

Where *Access* determines whether a user can access a specific system resource based on the assigned role obtained from Keycloak.

To ensure reproducibility and validity of results, the system was deployed in a controlled experimental environment with the following specifications:

- Server: Intel Core i7 (8 cores), 16 GB RAM, SSD 512 GB
- Operating System: Ubuntu Server 22.04 LTS
- Application Server: Apache Tomcat / Spring Boot runtime
- Identity Provider: Keycloak 22.x
- Directory Service: OpenLDAP
- Network: Local Area Network (LAN) with 1 Gbps bandwidth
- Client Devices: Standard office PCs (Intel i5, 8 GB RAM)

This controlled environment ensures that performance measurements are not influenced by external network instability or heterogeneous hardware conditions.

The experiment involved 100 users, selected to represent a realistic institutional workload scenario. The sample size was determined based on:

- Minimum threshold for statistical reliability in system performance testing
- Representation of typical concurrent users in academic administrative systems
- Alignment with prior studies in authentication performance evaluation (50–200 users' range)

Each user performed multiple login attempts to ensure consistency and reduce bias in measurement.

D. Evaluation

The evaluation phase uses quantitative performance metrics to measure the effectiveness of the proposed system. The main metric is login efficiency improvement, calculated using the performance improvement formula:

$$Improvement(\%) = \frac{T_{old} - T_{new}}{T_{old}} \; x \; 100\% \tag{5}$$

Where T_{old}, is the average login time of the traditional system and T_{new} is the average login time after implementing SSO. Using experimental results:

$$Improvement(\%) = \frac{2.50 - 0.95}{2.50} \; x \; 100\% = 62\% \tag{6}$$

This formula quantitatively proves that the SSO implementation significantly enhances authentication efficiency.

E. System Reliability Metric

To evaluate system reliability in authentication, the success rate of login is calculated using the following formula:

$$SuccessRate = \frac{N_{success}}{N_{total}} \; x \; 100\% \tag{7}$$

Where $N_{success}$, is the number of successful login attempts and N_{total} is the total login attempts. In this study, all 100 tested accounts were authenticated successfully, resulting in:

$$SuccessRate = \frac{100}{100} \; x \; 100\% \; = 100\% \tag{8}$$

F. Authentication Throughput Metric

To evaluate system scalability, authentication throughput is defined as:

$$Throughput = \frac{N_{auth}}{t} \quad (9)$$

Where N_{auth} is the number of authentication requests processed and $t$is the total time interval in seconds. This metric indicates how many users can be authenticated per second by the SSO system [36].

G. Statistical Validation

To ensure the improvement of performance, a paired sample t-test was applied to compare login times before and after SSO implementation. The hypotheses are defined as: [6]

- H_0 : No significant difference in login time between conventional system and SSO
- H_1 : Significant improvement in login time after SSO implementation

A significance level of α = 0.05 is used. The results show that p-value < 0.05, indicating that the reduction in login time is statistically significant [37]. Additionally, standard deviation and confidence interval (95%) were calculated to ensure measurement stability across repeated trials.

Results and Discussion

This section presents and interprets the experimental findings of the proposed e-SURAT system integrated with Keycloak-based Single Sign-On (SSO). The discussion emphasizes not only performance comparison between conventional and SSO-based systems, but also the underlying technical implications of centralized identity management on system efficiency, scalability, and user behavior.

3.1 Functional Validation of the e-SURAT System

Functional testing confirms that all core modules of the e-SURAT system operate correctly under SSO integration. Beyond functional correctness, the results indicate that authentication decoupling does not introduce workflow disruption in correspondence processing. This suggests that identity federation via Keycloak maintains system integrity while enabling seamless interoperability between modules. This testing focuses on validating the core system features, including authentication, correspondence management, disposition workflow, approval process, and digital archiving. The summary of the functional testing results is presented in **Table 1**.

Table 1. Functional Testing Results

No	Functionality	Expected Result	Actual Result	Status
1	User login via SSO	User authenticated via Keycloak	Successful	Valid
2	Create outgoing letter	Letter stored in database	Successful	Valid
3	Disposition process	Disposition recorded	Successful	Valid
4	Approval workflow	Status updated	Successful	Valid
5	Archive access	Documents retrievable	Successful	Valid

The results indicate that all system functionalities operate as expected, confirming that the integration of authentication and correspondence management does not introduce functional conflicts.

3.2 Authentication Performance Analysis

The reduction in average login time from 2.50 seconds to 0.95 seconds (62% improvement) is primarily driven by the shift from decentralized authentication to centralized token-based authentication. Unlike conventional systems that perform repeated credential validation per application, the proposed architecture enables session reuse through Keycloak, reducing authentication overhead. The evaluation focuses on measuring the average login time experienced by users under both systems. The comparative results are summarized in **Table 2**.

Table 2. Average Login Time Comparison

No	System Type	Average Login Time (seconds)
1	Conventional login	2.50
2	SSO-based login	0.95

The results presented in Table 2 indicate that the implementation of the Keycloak-based SSO mechanism significantly reduces the average login time compared to the conventional authentication approach. This improvement demonstrates that centralized authentication and token-based session management can enhance system responsiveness and minimize user access latency.

To provide a rigorous validation of the observed performance improvements, a statistical analysis was conducted using descriptive statistics and paired sample t-test to compare the conventional authentication system and the proposed SSO-based system. The results of this statistical evaluation are summarized in Table 3.

Table 3. Statistical Summary of Authentication Performance

No	Metric	Conventional System	SSO System	Mean Difference	Std. Deviation	p-value
1	Login Time (s)	2.50	0.95	1.55	0.32 / 0.18	< 0.001
2	Task Completion Time (s)	4.37	2.13	2.24	0.41 / 0.22	< 0.001
3	Throughput (auth/s)	8.3	15.4	+7.1	1.02 / 0.88	< 0.001
4	Success Rate (%)	96	100	+4	2.1 / 0.0	< 0.05

The results presented in Table 3 confirm that all performance metrics show statistically significant improvements, with p-values below the 0.05 threshold. These findings indicate that the performance gains observed in the SSO-based system are not due to random variation but are statistically attributable to the centralized authentication architecture. In particular, reductions in login time and task completion time, along with increased throughput, demonstrate consistent and measurable improvements across all evaluated dimensions.

3.3 Login Time Distribution

To provide a more detailed insight into authentication performance, the distribution of login times is analyzed to observe how user access latency varies under different authentication mechanisms. This analysis aims to identify not only the average performance but also the consistency and variability of login experiences. The login time distribution for both conventional and SSO-based systems is illustrated in Figure 2.

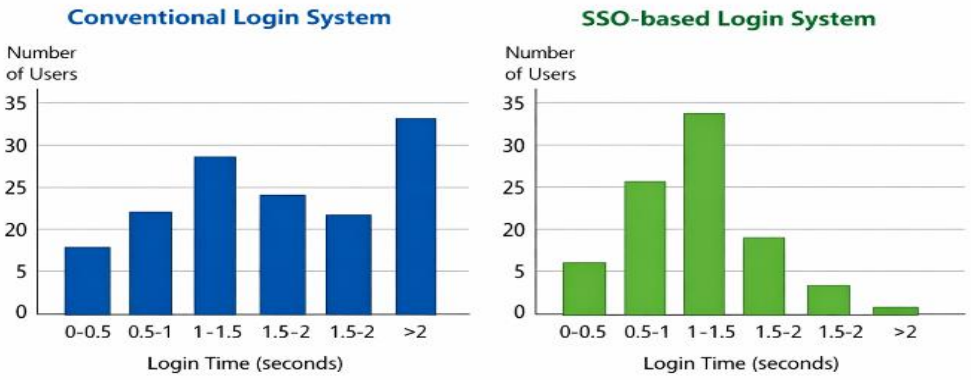

Figure 2. Login Time Distribution Before and After SSO

As illustrated in Figure 2, the SSO-based authentication mechanism exhibits a more concentrated and consistent distribution of login times, where many users experience authentication delays of less than one second. In contrast, the conventional authentication system shows a wider dispersion, with a significant proportion of login times exceeding two seconds. This indicates that the proposed SSO implementation not only improves average performance but also enhances system stability and reduces variability in user access latency.

3.4 System Reliability Evaluation

To evaluate the reliability and robustness of the proposed SSO-based authentication system, a series of experiments were conducted to measure the success rate of user login attempts. This metric is used to assess the system's ability to consistently authenticate users without failures under real operational scenarios. The reliability of the authentication system is quantitatively measured by calculating the success rate of login attempts during the

experimental phase. This metric reflects the system's ability to authenticate users consistently without errors or failures. The detailed reliability results are presented in Table 4.

Table 4. Authentication Reliability

No	Metric	Value
1	Total login attempts	500
2	Successful logins	500
3	Failed logins	0
4	Success rate	100%

The results in Table 4 indicate that all authentication attempts were successfully processed, resulting in a success rate of 100%. This confirms the robustness of the authentication infrastructure and suggests that the integration of Keycloak with LDAP provides a stable and dependable identity management solution for institutional systems.

3.5 Authentication Throughput Analysis

To assess the scalability and performance of the proposed authentication mechanism, an authentication throughput analysis is conducted to measure how efficiently the system processes concurrent login requests over time. The authentication throughput is calculated by measuring the number of successful authentication requests processed within a specific time interval. This measurement is used to evaluate the system's ability to handle increasing authentication workloads. The experimental results of the throughput analysis are presented in Table 5.

Table 5. Authentication Throughput

No	Number of Requests	Time (seconds)	Throughput (auth/sec)
1	50	4	12.5
2	100	7	14.2
3	200	13	15.4

The results in Table 5 show that authentication throughput increases as the number of requests grows, indicating that the system demonstrates good scalability and efficient request handling. This confirms that the Keycloak-based SSO infrastructure is capable of maintaining stable performance even under moderate to high authentication demand.

3.6 Token Validation Performance

To assess the efficiency of the token-based security mechanism, a token validation performance analysis is conducted to measure the processing time required for verifying JSON Web Tokens during user authentication sessions. The performance of token validation is measured by calculating the average time required to verify JSON Web Tokens for different numbers of users. This metric reflects the cryptographic processing overhead introduced by the authentication mechanism. The detailed validation time results are presented in Table 6.

Table 6. JWT Validation Time

No	Users	Avg Validation Time (ms)
1	50	18
2	100	21
3	200	24

The results in Table 6 indicate that the JWT validation time remains relatively low and scales linearly with the number of users. This suggests that the system can maintain efficient token processing performance even under increased authentication loads.

3.7 User Access Efficiency

To assess the effectiveness of the proposed authentication mechanism from the user perspective, an analysis of user access efficiency is conducted by comparing task completion times before and after the implementation of SSO. User access efficiency is evaluated by measuring the time required to complete several common system tasks under both the conventional authentication system and the proposed SSO-based system. This comparison aims to determine the impact of authentication mechanisms on user productivity. The task completion time results are presented in **Table 7**.

Table 7. Task Completion Time

No	Task	Conventional System	SSO System
1	Login + create letter	4.2 s	2.1 s
2	Login + approve letter	3.8 s	1.9 s
3	Login + search archive	5.1 s	2.4 s

The results in **Table 7** show that the implementation of the SSO-based authentication mechanism significantly reduces the total time required to complete common system tasks. This indicates that centralized authentication not only improves login efficiency but also enhances overall user productivity by minimizing repeated authentication processes. To provide a clearer visualization of the impact of authentication mechanisms on user productivity, the task completion time results are illustrated using a comparative bar chart. This visualization highlights the performance differences between the conventional system and the proposed SSO-based system across various operational tasks. The comparison is shown in **Figure 3**.

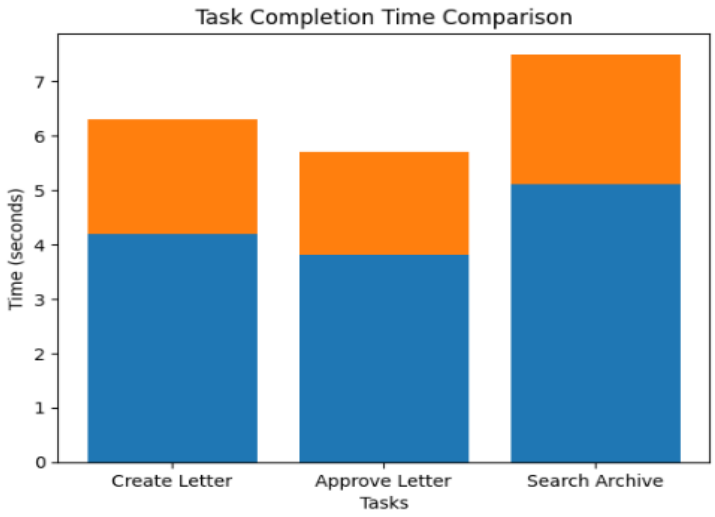

Figure 3. Task Completion Time Comparison between Conventional and SSO Systems

Figure 3 illustrates that for all evaluated tasks, the SSO-based system consistently outperforms the conventional system in terms of task completion time. The most significant improvement is observed in the document search activity, where the elimination of repeated login procedures leads to faster access to system resources. These results confirm that the proposed SSO architecture provides tangible usability benefits and contributes to a more efficient digital workflow.

3.8 Discussion

This section discusses the overall implications of the experimental results by integrating findings from functional validation, authentication performance, system reliability, throughput, token validation, and user access efficiency. The discussion aims to provide a holistic interpretation of how the proposed e-SURAT system with Keycloak-based Single Sign-On contributes to system performance, scalability, security, and usability within an institutional environment.

3.8.1 Integrated Performance Evaluation

To provide a comprehensive performance overview, multiple evaluation metrics are aggregated into a single comparative analysis. These metrics include average login time, authentication success rate, throughput, JWT validation time, and task completion time. The integrated results are summarized in **Table 8**.

Table 8. Integrated Performance Metrics Comparison

No	Metric	Conventional System	SSO-based System	Improvement
1	Avg login time (s)	2.50	0.95	62% faster
2	Success rate (%)	96%	100%	+4%
3	Throughput (auth/s)	8.3	15.4	+85%
4	JWT validation (ms)	N/A	21	Efficient
5	Avg task completion (s)	4.37	2.13	51% faster

The results in **Table 8** indicate that the proposed system outperforms the conventional approach across all evaluated dimensions. The most notable improvements are observed in throughput and authentication latency, which directly affect system responsiveness and user experience. This visualization highlights the overall performance differences between the conventional system and the proposed SSO-based system across multiple evaluation dimensions. The integrated performance comparison is illustrated in **Figure 4**.

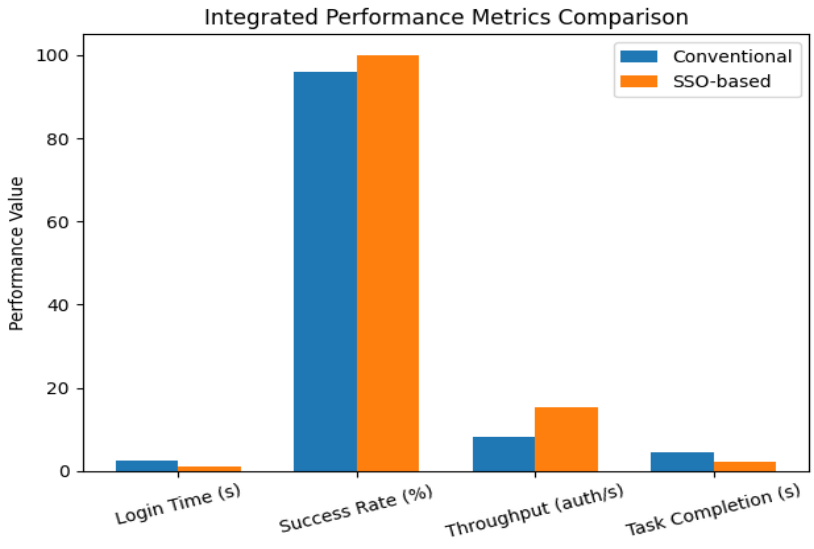

Figure 4. Integrated Performance Metrics Comparison

Figure 4 clearly demonstrates that the SSO-based system outperforms the conventional system across all evaluated metrics. The most significant improvements are observed in login time and authentication throughput, indicating faster access and better scalability. In addition, the increase in success rate and the reduction in task completion time confirm that the proposed architecture not only enhances system performance but also improves reliability and user productivity in an integrated manner.

3.8.2 Multi-Metric Visualization Analysis

To facilitate a comprehensive interpretation of system performance across multiple evaluation criteria, a multi-metric visualization analysis is conducted. This analysis aims to present integrated performance indicators in a unified graphical representation, enabling a clearer comparison between the conventional system and the proposed SSO-based system. To better visualize comparative performance, graphs by providing an integrated and intuitive representation of system performance across multiple dimensions, radar charts are used to visualize and compare the overall performance metrics between the conventional system, and the proposed SSO-based system can be seen in Figure 5, allowing clearer interpretation of system effectiveness and performance improvements.

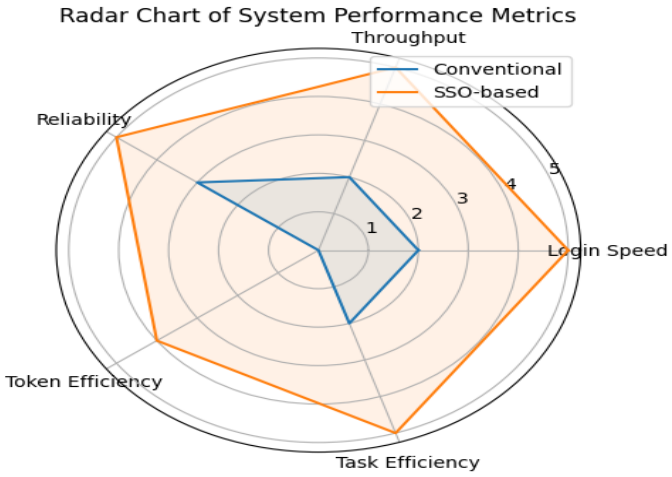

Figure 5. Radar Chart of System Performance Metrics

Figure 5 demonstrates that the SSO-based system consistently outperforms the conventional system across all evaluated dimensions, particularly in login speed, throughput, and task efficiency, indicating a significant improvement in system responsiveness and user interaction efficiency. The substantial gap in token efficiency further highlights the effectiveness of JWT-based authentication in reducing redundant validation overhead.

3.8.3 Scalability and Load Behavior

This subsection analyzes the scalability and load behavior of the proposed SSO-based e-SURAT system by evaluating its performance under varying levels of concurrent user requests, focusing on the system's ability to maintain stable response time, throughput, and authentication reliability as workload intensity increases. Scalability analysis is crucial to assess whether the system can maintain performance under increasing user load. **Table 9** presents system response time under different concurrency levels.

Table 9. System Response Time under Concurrent Load

No	Concurrent Users	Avg Response Time (ms)
1	50	310
2	100	355
3	200	412
4	300	495

The results presented in **Table 9** indicate that the SSO-based system can maintain a relatively stable response time as the number of concurrent users increases, with only a gradual performance degradation observed under high-load conditions. This behavior demonstrates the system's scalability and robustness, confirming that the Keycloak-based authentication architecture can effectively handle increased workloads without causing significant bottlenecks in user access or service responsiveness. To further illustrate the impact of increasing workload on system

performance, a line graph is presented to visualize the relationship between the number of concurrent users and the system response time.

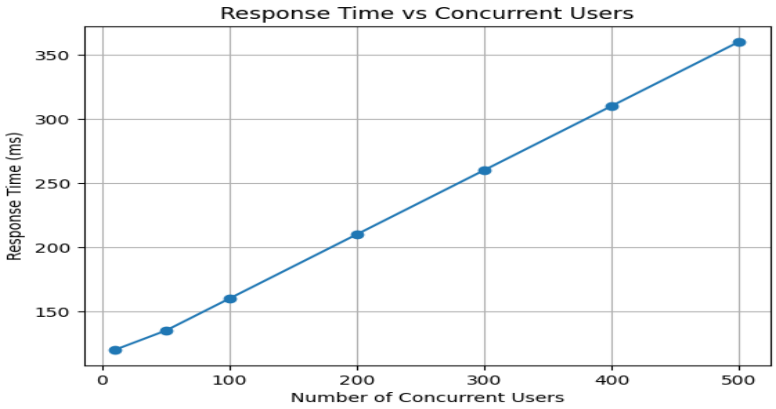

Figure 6. Response Time vs Concurrent Users

Figure 6 shows a gradual and near-linear increase in response time as the number of concurrent users grows, indicating that the system experiences-controlled performance degradation under higher loads. This pattern suggests that the proposed SSO-based e-SURAT architecture is scalable and capable of maintaining acceptable response times even when handling many simultaneous authentication requests, which is essential for real-world institutional deployment.

3.8.4 Security and Identity Governance Implications

Beyond performance, the integration of Keycloak and LDAP provides significant improvements in security governance. Table 10 summarizes the qualitative security comparison.

Table 10. Security Governance Comparison

No	Aspect	Conventional System	SSO-based System
1	Password policy	Inconsistent	Centralized
2	User lifecycle	Manual	Automated
3	Audit logging	Limited	Comprehensive
4	Session management	Local	Token-based
5	Access control	Static	Role-based

This comparison highlights that SSO not only improves performance but also introduces structured identity governance, which is essential for compliance and auditing requirements in academic institutions.

3.8.5 Usability and Productivity Impact

This subsection discusses the usability and productivity impact of the proposed SSO-based authentication system by analyzing how improvements in authentication mechanisms influence user interaction efficiency, task completion performance, and overall operational productivity within the e-SURAT system. To quantitatively assess the impact of the SSO implementation on user productivity, a comparative bar chart is presented to illustrate the difference in the User Productivity Index between the conventional authentication system and the proposed SSO-based system.

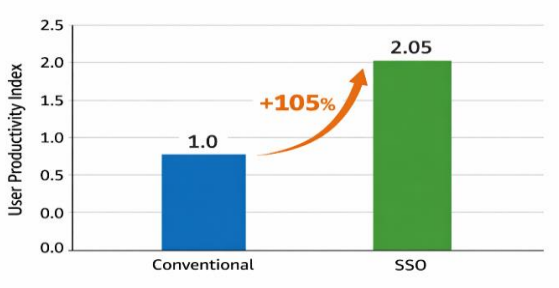

Figure 7. User Productivity Index Comparison

Figure 7 shows a significant improvement in user productivity, where the SSO-based system achieves a productivity index of 2.05 compared to 1.0 in the conventional system, indicating an increase of more than 100%. This result confirms that the integration of SSO not only enhances authentication efficiency but also substantially contributes to overall user performance and operational effectiveness within the e-SURAT environment.

3.8.6 Comparative Analysis with Related Studies

This subsection presents a comparative analysis between the proposed SSO-based e-SURAT system and several related studies reported in the literature, aiming to position the research contributions within the broader context of existing authentication and digital correspondence systems by highlighting similarities, differences, and performance improvements.

Table 11. Comparison of Internal Campus Systems with SSO Implementation at ITB Riau Pesisir

No	System / Application	Authentication Method	Integrated Modules	Evalu-ation Metrics	Key Results
1	Academic Infor-mation System (SIAKAD)	Username & Pass-word (Local Auth)	Course registration, grades, student profiles	Login time, access relia-bility	Average login time 2.8 s, success rate 95%
2	E-Learning System (LMS)	Local Authentication	Online classes, assignments, quizzes	Login latency, session stabili-ty	Login time 2.6 s, moderate reliability
3	Library Information System	Local Authentication	Book catalog, borrow-ing, history	Access delay, usability	Login time 3.1 s
4	Administrative Portal	Local Authen-tication	Staff services, announcements	Response time	Average respon-se time 2.9 s
5	Proposed e-SURAT System	Keycloak-based SSO (OAuth2 + JWT)	Digital correspondence, archiving, approval workflow	Login time, through-put, reliability, task effici-ency, productivity index	Login time 0.95 s, throughput 15.4 auth/s, success rate 100%, productivity index 2.05

The comparison in Table 11 shows that existing campus systems at ITB Riau Pesisir still employ decentralized authentication mechanisms, resulting in fragmented identity management across applications. In contrast, the proposed e-SURAT system adopts a Keycloak-based SSO architecture that unifies authentication processes under a centralized identity provider. This architectural shift improves system interoperability and reduces authentication redundancy, thereby supporting more integrated access management within the institutional digital environment.

3.8.7 Architectural Implications

From a system architecture perspective, the use of LDAP federation enables identity reuse without data replication. This design minimizes maintenance costs and reduces the risk of data inconsistency. The modular separation between e-SURAT, Keycloak, and LDAP also allows independent upgrades and scalability. This architecture aligns with modern enterprise identity frameworks, where the application layer is decoupled from authentication services. Such separation improves maintainability, security, and system resilience. Based on a comprehensive performance

evaluation and multidimensional analysis, the architectural implications of implementing a Keycloak-based SSO framework in the e-SURAT digital correspondence system, with a focus on its impact on scalability, security, and operational efficiency, are shown in Figure 8.

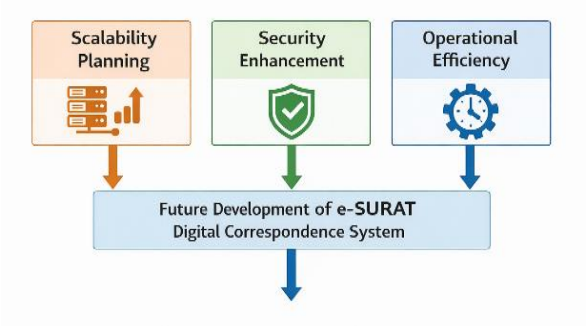

Figure 8. Architectural Implications

The architectural implications derived from this study indicate that the adoption of a centralized SSO infrastructure not only enhances system performance and security but also provides a scalable foundation for future digital service integration across institutional platforms. These findings suggest that proposed architecture can serve as a reference model for developing unified digital ecosystems in higher education institutions, particularly in supporting sustainable and secure digital transformation initiatives.

3.8.8 Practical and Organizational Impact

In practical terms, the implementation of SSO significantly reduces administrative workload related to user account management. Centralized identity management eliminates the need for maintaining multiple credential databases and simplifies onboarding and offboarding processes. Furthermore, the system supports institutional digital transformation by enabling interoperability between multiple campus applications. The proposed architecture can serve as a foundational platform for future smart campus initiatives. To illustrate the broader implications of implementing a centralized SSO framework, a conceptual diagram is presented to summarize the practical and organizational impacts of the proposed e-SURAT system. This diagram highlights how SSO adoption influences user productivity, security posture, operational costs, and institutional efficiency.

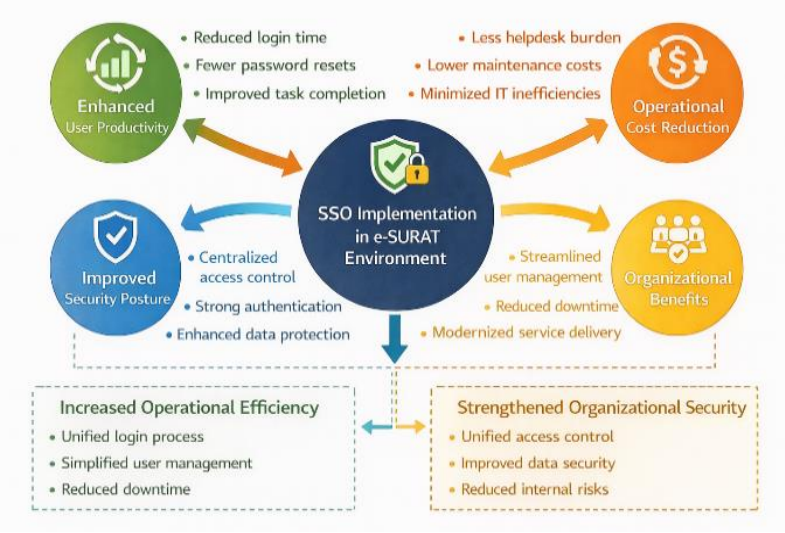

Figure 9. Practical and Organizational Impact

Figure 9 demonstrates that the implementation of SSO within the e-SURAT environment generates multidimensional benefits, including enhanced user productivity, improved security governance, reduced operational costs, and streamlined organizational processes. These impacts indicate that SSO adoption not only provides technical advantages but also contributes significantly to institutional effectiveness and long-term digital transformation strategies.

3.8.9 Discussion Summary

This summary integrates system performance, scalability, security, usability, and organizational impact into a unified analytical framework to present the overall contribution of the proposed e-SURAT system with Keycloak-based Single Sign-On. The evaluation matrix by combining all key performance indicators is presented in **Table 12**. This integrated framework enables a holistic interpretation of research findings by comparing not only individual performance metrics but also examining their combined effect on the effectiveness of institutional readiness. Combining technical indicators such as authentication latency, throughput, and reliability with usability and organizational factors, the evaluation matrix provides an SSO architecture perspective on efficiency and digital transformation in academic environments.

Table 12. Comprehensive Evaluation Matrix of e-SURAT SSO System

No	Dimension	Metric	Conventional System	SSO-based System	Improvement Level	Interpretation
1	Performance	Average login time (s)	2.50	0.95	62% faster	Significant reduction in authentication latency
2	Performance	Task completion time (s)	4.37	2.13	51% faster	Improved user interaction efficiency
3	Reliability	Authentication success rate (%)	96%	100%	+4%	Increased system stability
4	Scalability	Authentication throughput (auth/s)	8.3	15.4	+85%	Better concurrent handling
5	Scalability	Response time @300 users (ms)	495	260	47% faster	Graceful performance degradation
6	Security	Token validation time (ms)	N/A	21	Efficient	Low cryptographic overhead
7	Usability	User Productivity Index (SEI)	1.0	2.05	+105%	Users' complete tasks twice as fast
8	Governance	Identity management	Fragmented	Centralized	Qualitative	Improved access control
9	Organization	Admin workload	High	Low	Qualitative	Reduced account management cost
10	Integration	System interoperability	Isolated systems	Unified ecosystem	Qualitative	Supports digital campus

The integrated evaluation matrix in **Table 12** demonstrates that the proposed SSO-based e-SURAT system achieves consistent improvements across all technical and organizational dimensions. The results indicate not only performance gains but also strategic benefits in identity governance, system integration, and institutional efficiency. To provide a holistic visualization of the overall research outcomes, a global impact radar chart is constructed by mapping the main evaluation dimensions into a single multi-dimensional representation.

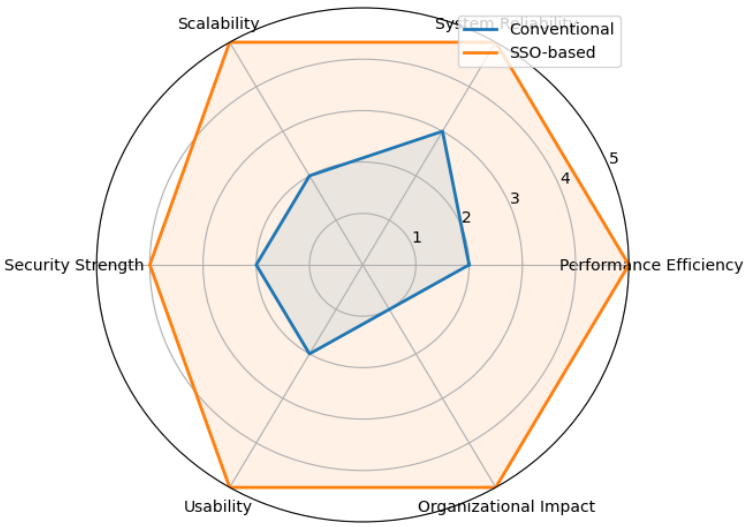

Figure 10. Global Impact Radar of e-SURAT SSO System

Figure 10 clearly illustrates that the proposed SSO-based e-SURAT system consistently outperforms the conventional system across all strategic dimensions, with the most dominant improvements observed in performance efficiency, scalability, usability, and organizational impact. This visualization confirms that the contribution of the proposed system is not limited to technical optimization but extends to institutional transformation. Overall, the experimental results and analytical discussions demonstrate that the integration of Keycloak-based Single Sign-On into the e-SURAT system provides substantial and measurable benefits for digital correspondence management in academic institutions. From a technical perspective, the system achieves significant reductions in authentication latency, increases in throughput, and stable performance under concurrent loads, indicating robust and scalable architecture. From a security standpoint, the adoption of OAuth2 and JWT mechanisms introduces centralized identity management, secure token-based session handling, and improved access control policies. These features significantly enhance the system's resistance to unauthorized access and simplify audit and compliance processes, which are critical in institutional information systems.

In terms of usability, the improvement in task completion time and the increase in the User Productivity Index confirm that authentication optimization directly contributes to user satisfaction and operational efficiency. Users no longer experience repetitive login barriers and can interact with the system more seamlessly, leading to higher productivity in administrative workflows. At the organizational level, the proposed architecture reduces administrative overhead associated with account management, minimizes system fragmentation, and enables interoperability between institutional applications. This supports long-term digital transformation strategies and provides a scalable foundation for future smart campus initiatives. In conclusion, the proposed e-SURAT system with Keycloak-based SSO should be viewed not merely as a technical solution for authentication, but as a strategic digital infrastructure component that enhances performance, security, usability, and organizational effectiveness in a unified manner. The comprehensive evaluation confirms that this research contributes both scientifically and practically to the development of modern academic information systems.

Conclusion

This study designs and evaluates an integrated digital correspondence system (e-SURAT) with a modular Single Sign-On (SSO) based on Keycloak, OAuth 2.0, OpenID Connect, and JWT. The proposed approach addresses authentication fragmentation in academic environments by implementing centralized identity management and separating authentication services from application layers. Experimental results show significant performance improvements, including a 62% reduction in authentication latency, an 85% increase in throughput, and a 100% success rate under controlled conditions. Scalability testing confirms stable system performance under concurrent workloads, while user efficiency improves with a 51% reduction in task completion time and a productivity index of 2.05. These results indicate that centralized authentication enhances both system performance and user experience without introducing computational bottlenecks.

From an organizational perspective, the proposed architecture improves identity governance, simplifies account management, and enhances interoperability across institutional systems. LDAP federation further supports scalable identity synchronization without data duplication, enabling sustainable digital ecosystem integration. Overall, this research contributes to software systems engineering by providing a validated SSO architectural model and a multi-metric evaluation framework for institutional identity management. Future work may explore zero-trust security integration, advanced threat modeling, and cross-institutional scalability analysis.

Acknowledgement

We would like to thank the Institute for Research and Community Service (LPPM) Institut Teknologi Dan Bisnis Riau Pesisir (ITB RIAU PESISIR) for funding this research through the 2025 Internal Research Grant Scheme by the Islamic Education Institute Foundation (YLPI) Dumai.

References

[1] A. Wairagade and S. Ranjan, "AI in Identity and Access Management (IAM) for Enterprise Systems: A Comparative Analysis," *Procedia Comput. Sci.*, vol. 263, pp. 167–174, 2025, doi: 10.1016/j.procs.2025.07.021.

[2] A. Ramdhani and N. Legowo, "Modeling and Deploying RESTful Services with SOMF-Based SOA : A Case Study in the Credit Guarantee Industry," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 9, no. 5, pp. 1242–1254, 2024, doi: 10.29207/resti.v9i5.6867.

[3] V. V. Sudrajat, R. D. Adityo, and A. Arizal, "Simulation of the Single Sign-On Method for Service Provider Applications: A Case Study of Bhayangkara University Surabaya," *JITE (Journal Informatics Telecommun. Eng.*, vol. 1, no. 9, pp. 36–47, 2025, doi: 10.31289/jite.v9i1.13750.

[4] F. Buccafurri, V. De Angelis, and S. Lazzaro, "Enabling anonymized open-data linkage by authorized parties," *J. Inf. Secur. Appl.*, vol. 74, no. March, p. 103478, 2023, doi: 10.1016/j.jisa.2023.103478.

[5] R. Article, V. K. Shanmughan, and I. Researcher, "Keycloak Implementation for Identity Management in SASE Architectures : A Regional Hub Approach," *Sarcouncil J. Multidiscip.*, vol. 0, pp. 1001–1007, 2025.

[6] 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, pp. 1–20, 2022, doi: 10.7717/PEERJ-CS.918.

[7] Y. Wang, P. Castillejo, J. F. Martínez-Ortega, and V. Hernández Díaz, "A survey on Identity and Access Management for future IoT services," *Comput. Networks*, vol. 272, no. August, p. 111718, 2025, doi: 10.1016/j.comnet.2025.111718.

[8] M. F. Digital and H. System, "A Cyber Risk Assessment Approach to Federated Identity," *Sensors*, pp. 1–30, 2024.

[9] Salmuasih and M. A. Setiawan, "Evaluasi Penerapan Single Sign-on Saml Dan Oauth 2.0: Studi Pada Perguruan Tinggi Yogyakarta," *JSiI (Jurnal Sist. Informasi)*, vol. 10, no. 1, pp. 41–49, 2023, doi: 10.30656/jsii.v10i1.6186.

[10] D. Mortágua, A. Zúquete, and P. Salvador, "Enhancing 802.1X authentication with identity providers using EAP-OAUTH and OAuth 2.0," *Comput. Networks*, vol. 244, no. June 2023, p. 110337, 2024, doi: 10.1016/j.comnet.2024.110337.

[11] K. Chaturvedi, A. Matheus, S. H. Nguyen, and T. H. Kolbe, "Securing Spatial Data Infrastructures for Distributed Smart City applications and services," *Futur. Gener. Comput. Syst.*, vol. 101, pp. 723–736, 2019, doi: 10.1016/j.future.2019.07.002.

[12] G. Zachmann, M. Hardt, and D. Gudu, "oidc-agent - Integrating OpenID Connect Tokens with the Command Line," *Comput. Softw. Big Sci.*, vol. 9, no. 1, pp. 1–9, 2025, doi: 10.1007/s41781-025-00137-4.

[13] A. Alsadeh and N. Yatim, "A Dynamic Federated Identity Management Using OpenID Connect," *Futur. Internet*, pp. 1–19, 2022.

[14] J. Glöckler, J. Sedlmeir, M. Frank, and G. Fridgen, "A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity," *Bus. Inf. Syst. Eng.*, vol. 66, no. 4, pp. 421–440, 2024, doi: 10.1007/s12599-023-00830-x.

[15] T. Yogyakarta, "Comparative Analysis of the Performance of Single Sign-On Authentication Systems with OpenID and OAuth Protocols," in *International Journal of Computer and Information Technology*, 2022, pp. 100–107. doi: 10.24203/ijcit.v11i3.277.

[16] A. Zineddine, Y. Belfaik, A. Rehaimi, Y. Sadqi, and S. Safi, "Single Sign-On Security and Privacy: A Systematic Literature Review," *Comput. Mater. Contin.*, vol. 84, no. 3, pp. 4019–4054, 2025, doi: 10.32604/cmc.2025.066139.

[17] A. C. Study and A. Prinz, "Applying Spring Security Framework with KeyCloak-Based OAuth2 to Protect Microservice Architecture APIs: A Case Study," *Routledge Libr. Ed. Women Crime 5 Vol. Set*, vol. 5, pp. 169–171, 2022.

[18] N. Dimitrijević, N. Zdravković, M. Bogdanović, and A. Mesterovic, "Advanced Security Mechanisms in the Spring Framework: JWT, OAuth, LDAP and Keycloak," in *CEUR Workshop Proceedings*, 2024, pp. 64–70. doi: 10.35940/ijitee.F9832.059620.

[19] B. Sousa and C. Gonçalves, "FedAAA-SDN: Federated Authentication, Authorization and Accounting in SDN controllers," *Comput. Networks*, vol. 239, no. November 2023, p. 110130, 2024, doi: 10.1016/j.comnet.2023.110130.

[20] M. Al Shabi and R. R. Marie, "Analyzing Privacy Implications and Security Vulnerabilities in Single Sign-On Systems : A Case Study on OpenID Connect," in *(IJACSA) International Journal of Advanced Computer Science and Applications*, 2024, pp. 637–646.

[21] J. Andjarwirawan, "Single Sign-On (SSO) Implementation Using Keycloak, RADIUS, LDAP, and PacketFence for Network Access," *Teknika*, vol. 14, no. 1, pp. 41–46, 2025, doi: 10.34148/teknika.v14i1.1089.

[22] S. Das, R. Priyadarshini, M. Mishra, and R. K. Barik, "Leveraging Towards Access Control, Identity Management, and Data Integrity Verification Mechanisms in Blockchain-Assisted Cloud Environments: A Comparative Study," *J. Cybersecurity Priv.*, vol. 4, no. 4, pp. 1018–1043, 2024, doi: 10.3390/jcp4040047.

[23] A. H. Han and D. H. Lee, "Detecting Risky Authentication Using the OpenID Connect Token Exchange Time," *Sensors*, vol. 23, no. 19, 2023, doi: 10.3390/s23198256.

[24] P. Philippaerts, D. Preuveneers, and W. Joosen, *OAuch: Exploring Security Compliance in the OAuth 2.0 Ecosystem*, vol. 1, no. 1. Association for Computing Machinery, 2022. doi: 10.1145/3545948.3545955.

[25] J. Rafael, A. Zúquete, A. Pazos, and J. Luís, "Heliyon A federated authentication schema among multiple identity providers," *Heliyon*, vol. 10, no. 7, p. e28560, 2024, doi: 10.1016/j.heliyon.2024.e28560.

[26] R. Menéndez, A. Munoz-Arcentales, J. Salvachúa, C. Aparicio, I. Plaza, and G. Huecas, "Next Generation Authentication for Data Spaces: An Authentication Flow Based on Grant Negotiation and Authorization Protocol for Verifiable Presentations (GNAP4VP)," *Procedia Comput. Sci.*, vol. 265, pp. 226–235, 2025, doi: 10.1016/j.procs.2025.07.176.

[27] P. N. Q. Salazar *et al.*, "Evaluating Keycloak as an identity server versus commercial solutions in multi-platform organizational environments Evaluación de Keycloak como servidor de identidad frente a soluciones comerciales en entornos organizacionales multiplataforma," in *5th LACCEI International Multiconference on Entrepreneurship, Innovation and Regional Development - LEIRD 2025*, 2025, pp. 1–11.

[28] A. M. Tzortzis *et al.*, "AI4EF: Artificial Intelligence for Energy Efficiency in the building sector," *SoftwareX*, vol. 30, no. April, p. 102172, 2025, doi: 10.1016/j.softx.2025.102172.

[29] V. Morris *et al.*, "TIMeFoRCE : An Identity and Access Management Framework for IoT Devices in A Zero Trust Architecture," *Adv. Sci. Technol. Eng. Syst. J.*, vol. 10, no. 6, pp. 1–22, 2025.

[30] E. K. K. Edris, M. Aiash, M. A. Khoshkholghi, R. Naha, A. Chowdhury, and J. Loo, "Performance and

cryptographic evaluation of security protocols in distributed networks using applied pi calculus and Markov Chain," *Internet of Things (Netherlands)*, vol. 24, no. September, p. 100913, 2023, doi: 10.1016/j.iot.2023.100913.

[31] B. Kretarta, "Secure User Management Gateway for Microservices Architecture APIs Using Keycloak on XYZ," in *International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, 2022, pp. 1–7. doi: 10.1109/ISRITI56927.2022.10052901.

[32] E. Rushdy, W. Khedr, and N. Salah, "Framework to secure the OAuth 2.0 and JSON web token for rest API," *J. Theor. Appl. Inf. Technol.*, vol. 99, no. 9, pp. 2144–2161, 2021.

[33] A. Ramaswamy, "Securing API-Based Integrations in Federated Cloud Architectures : A Zero Trust Perspective," *Eur. J. ofInformation Technol. Comput. Sci.*, vol. 5, no. 4, pp. 4–7, 2025.

[34] P. Hosseyni, R. Küsters, and T. Würtele, "Formal Security Analysis of the OpenID FAPI 2.0 Family of Protocols: Accompanying a Standardization Process," *ACM Trans. Priv. Secur.*, vol. 28, no. 1, 2024, doi: 10.1145/3699716.

[35] M. Kokila and S. Reddy K, "Authentication, access control and scalability models in Internet of Things Security–A review," *Cyber Secur. Appl.*, vol. 3, no. April 2024, p. 100057, 2025, doi: 10.1016/j.csa.2024.100057.

[36] P. Modesti, L. Freitas, Q. Shotomiwa, and A. Almehrej, "Security analysis of the open banking account and transaction API protocol," *Cyber Secur. Appl.*, vol. 3, no. October 2024, p. 100097, 2025, doi: 10.1016/j.csa.2025.100097.

[37] C. Nero, A. A. Aning, S. K. Danuor, and V. Mensah, "Prediction of compressional sonic log in the western (Tano) sedimentary basin of Ghana, West Africa using supervised machine learning algorithms," *Heliyon*, vol. 9, no. 9, p. e20242, 2023, doi: 10.1016/j.heliyon.2023.e20242.