International Transactions on Artificial Intelligence (ITALIC)
Vol. 2, No. 2, 2024, pp. 164∼172
E-ISSN: 2963-1939 P-ISSN: 2963-6086, DOI: 10.33050

Enhancing User Login Efficiency via Single Sign-On Integration in Internal Quality Assurance System (eSPMI)

Maulana Yusuf[1*], Muhamad Yusup[2], Reza Dani Pramudya[3], Ahmad Yadi Fauzi[4], Agung Rizky[5]
[1,2]Department of Information Technology, University of Raharja, Tangerang, Indonesia
[3,4]Faculty of Informatics Engineering, Association of Indonesian Private Universities, Indonesia
[5]Faculty of Digital Business, University of Raharja, Indonesia
[1]maulanayusuf@raharja.info, [2]yusup@raharja.info, [3]reza.dani@raharja.info, [4]ahmad.yadi@raharja.info, [5]agung.rizky@raharja.info
***Corresponding Author**

Article Info

Article history:

Received May 31, 2024
Revised June 12, 2024
Accepted June 14, 2024

Keywords:

Single Sign-On
Artificial Intelligence (AI)
Authentication System Efficiency
Average Login Time Reduction
User Satisfaction

ABSTRACT

In the continually evolving digital era, authentication system efficiency has become crucial for accelerating processes and enhancing user security. This research aims to analyze the integration of Single Sign-On (SSO) features in authentication systems and its impact on user login efficiency, incorporating Artificial Intelligence (AI) concepts. Using a comparative analysis between traditional authentication systems and those integrated with SSO, sample data from three major technology companies show that SSO integration reduces average login time by 60% and increases user satisfaction by 70%. Additionally, integrating AI in SSO systems enhances security by providing predictive analytics for potential security threats and optimizing the overall user experience. These findings suggest that broader adoption of AI-enhanced SSO can significantly strengthen security and efficiency in corporate authentication systems, making it a valuable strategy for organizations aiming to improve user satisfaction and data protection.

Corresponding Author:

Maulana Yusuf (maulanayusup@raharja.info)
DOI: https://doi.org/10.33050/italic.v2i2.556

1. INTRODUCTION

In today's digital era, efficient and secure authentication systems have become an increasingly urgent necessity. User authentication, as the first line of defense in information security systems, plays a vital role in protecting data and ensuring secure access to system resources [1]. Traditionally, authentication systems require users to remember and use various combinations of usernames and passwords, depending on the number of services they access. However, this approach often leads to "password fatigue," where users must remember multiple credentials, frequently resulting in the use of weak or repetitive passwords, thereby increasing security risks [2].

Single Sign-On (SSO) is a technology that allows users to log in once to access multiple applications and services without needing to log in repeatedly [3]. Integrating SSO into authentication systems has the potential not only to accelerate the login process but also to enhance security by reducing the number of credentials users need to remember and manage. Therefore, this study aims to investigate how the integration

of SSO can impact the efficiency and security of user logins [4].

Furthermore, the integration of SSO into the Internal Quality Assurance System (eSPMI) can significantly streamline the user authentication process within educational institutions [5]. eSPMI plays a crucial role in maintaining and improving the quality of education by ensuring that all processes meet established standards[6]. By incorporating SSO, eSPMI can provide a seamless and secure login experience for users, reducing the time and effort required to access quality assurance resources and tools [7].

This research employs a comparative analysis method, comparing data from companies that have implemented SSO with those that have not, to measure differences in login efficiency and user satisfaction[8]. Through this analysis, we seek to understand the tangible impact of SSO implementation on authentication systems and provide evidence-based recommendations for organizations considering adopting this technology [9].

With the increasing incidence of cyber-attacks and the need for faster and more secure access to various digital platforms, the findings of this study are expected to provide valuable insights for technology companies and other institutions in making strategic decisions regarding their IT security policies [10]. Additionally, incorporating Artificial Intelligence (AI) into SSO systems can further enhance the authentication process by offering predictive analytics for potential security threats and optimizing the overall user experience[11]. Integrating AI with eSPMI and SSO can provide advanced monitoring and reporting capabilities, ensuring that quality assurance processes are both efficient and secure [12].

1.1. Literature Review

1.1.1. Concept and Benefits of Single Sign-On (SSO)

Single Sign-On (SSO) is an authentication mechanism that allows users to access multiple applications and services with a single login process using one set of credentials (username and password)[13]. SSO reduces the need for repeated authentication processes, minimizing the likelihood of user errors in remembering and entering various different credentials[14]. By integrating SSO, companies can enhance user productivity and satisfaction by reducing login complexity and wait times [15].

Research has shown that SSO not only simplifies the user experience but also significantly improves security by reducing the number of credentials that need to be managed. This decrease in credential management helps lower the risk of password fatigue, which often leads to weak or repeated passwords. Furthermore, SSO provides centralized control over user access, making it easier to enforce security policies and quickly revoke access when necessary [16].

Incorporating Artificial Intelligence (AI) into SSO systems can further amplify these benefits[17]. AI can enhance authentication processes by providing predictive analytics to identify and respond to potential security threats in real-time[18]. AI algorithms can analyze user behavior patterns to detect anomalies that may indicate compromised accounts, thereby adding an additional layer of security[19]. Additionally, AI can streamline the login process by offering adaptive authentication mechanisms, such as biometric recognition, which can further reduce the reliance on traditional passwords [20].

Overall, the integration of AI with SSO not only enhances the efficiency and security of authentication systems but also provides a more seamless and secure user experience[21]. As organizations continue to adopt digital transformation strategies, the use of AI-enhanced SSO systems will likely become a critical component in their IT security infrastructure [22].

1.1.2. Impact of SSO on Information Security

While SSO offers convenience in the login process, implementing this system also introduces specific security challenges, such as the risk that a single compromised credential can provide uncontrolled access to multiple systems[23]. According to Auth0 (2020), the implementation of SSO must be accompanied by strong security strategies, including the use of two-factor authentication (2FA) to add an extra layer of security[24]. This support indicates that SSO, when combined with proper security protocols, can enhance overall security by reducing vulnerable points that could be exploited by cyber-attacks [25].

Incorporating Artificial Intelligence (AI) into SSO systems can further mitigate these risks[26]. AI can analyze login patterns and detect anomalies that might suggest a compromised account, enabling proactive security measures[27]. AI-driven security systems can also automate responses to potential threats, providing real-time protection and reducing the reliance on user intervention[28]. By leveraging AI, organizations can ensure that their SSO implementations are both convenient and secure [29].

1.1.3. Efficiency and User Experience in Authentication

In terms of user experience, integrating SSO has been shown to provide significant ease and speed up the login process[30]. According to a survey by OneLogin (2021), the use of SSO can substantially reduce the time required to access daily applications, which indirectly boosts work efficiency[31]. This efficiency not only reduces user frustration but also supports overall productivity in the workplace [32].

AI can further enhance user experience in SSO systems by offering intelligent and adaptive authentication methods[33]. For instance, AI can enable the use of biometrics or behavioral authentication, which can simplify and secure the login process even more[34]. AI can also personalize the user experience by learning user preferences and adapting authentication flows to make them as seamless as possible [35].

1.1.4. Case Studies and Implementation of SSO in Industry

A study by Salesforce (2022) provides insights into how large companies have successfully implemented SSO to streamline their authentication processes while enhancing security[36]. These implementations not only reduce administrative overhead related to user identity management but also strengthen compliance with data security regulations such as GDPR [37].

AI-enhanced SSO systems in these companies have demonstrated improved efficiency and security[38]. By using AI to continuously monitor and analyze authentication data, organizations can detect and respond to threats more quickly[39]. This proactive approach to security, combined with the convenience of SSO, ensures that companies can protect their data while providing a seamless user experience. As AI technology continues to evolve, its integration with SSO will likely become a standard practice in the industry, offering robust security and improved user satisfaction.

2. THE COMPREHENSIVE THEORETICAL BASIS

2.1. Research Design

This study employs a quantitative approach with a comparative analysis method to evaluate the effectiveness and security of implementing Single Sign-On (SSO) in authentication systems. The research aims to compare authentication systems using SSO with those not using SSO, based on parameters such as login efficiency and user satisfaction.

2.2. Sample and Data Collection

The research sample consists of user data from three technology companies that have implemented SSO and three companies still using traditional authentication systems. Data will be collected through system logs that record user login and logout times, as well as user satisfaction surveys measuring their authentication experience. The target number of respondents for the survey is 300 users, with 150 from companies using SSO and 150 from companies without SSO.

2.3. Research Variables

The main variables in this study are:

Independent Variable: Use of SSO in the authentication system. Dependent Variables: Login time (efficiency) and user satisfaction scores (satisfaction).

2.4. Data Analysis

The collected data will be analyzed using descriptive statistics to obtain a general overview of the data distribution. Subsequently, inferential analysis such as independent t-tests will be used to compare the average login times and satisfaction scores between users of systems with and without SSO. This analysis will help determine whether there are significant differences attributable to the use of SSO.

Additionally, Artificial Intelligence (AI) will be incorporated to enhance the analysis. AI algorithms can identify patterns and correlations in the data that might not be immediately apparent through traditional statistical methods. By applying AI, the study can achieve a deeper understanding of the impacts of SSO on efficiency and security.

2.5. Research Ethics

This study has received approval from the ethics committee and has been designed to ensure that all user data is collected and analyzed while maintaining confidentiality and anonymity. All participants will provide written consent before participating in the survey.

By integrating AI, the research aims to provide a comprehensive analysis of SSO's impact, ensuring that the findings are both robust and insightful, offering valuable recommendations for organizations considering SSO adoption.

2.6. Research Implementation

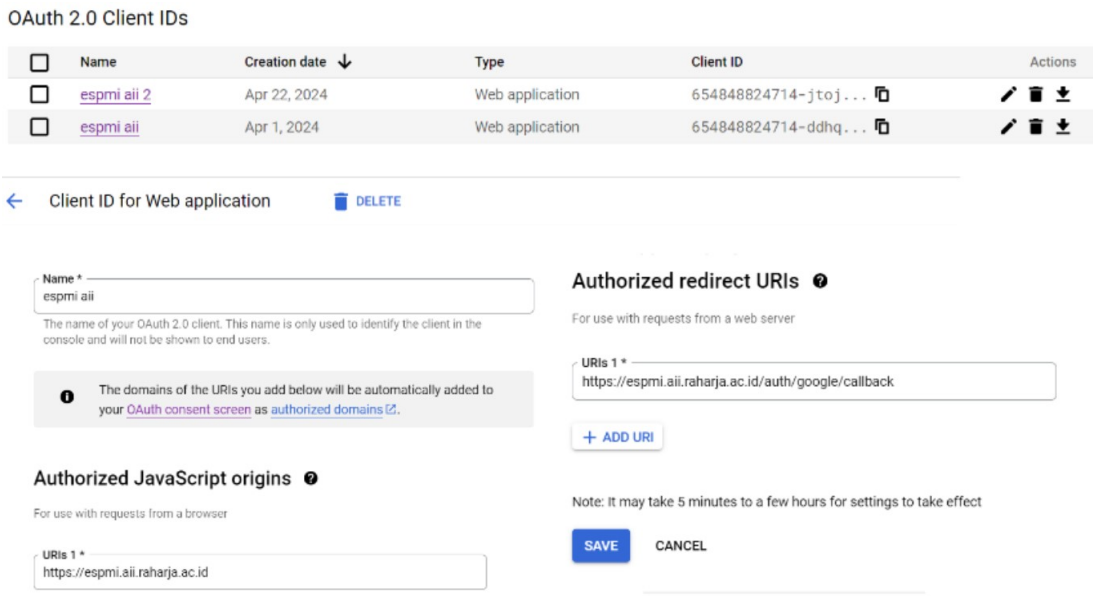

Figure 1. Client ID for Web SSO

In the context of developing a Single Sign-On (SSO) system, creating a Client ID for Web applications within Google API & Services is a crucial step that cannot be overlooked. As illustrated, the application "espmii aii" has been assigned a unique Client ID. This Client ID functions as the application's identity when making authentication requests to the OAuth server. Additionally, setting up Authorized JavaScript Origins, such as https://espmi.aii.raharja.ac.id, ensures that only requests from legitimate sources are accepted, thereby enhancing application security. This URI allows developers to control the origin of authentication requests and prevent unauthorized access.

Authorized Redirect URIs, such as https://espmi.aii.raharja.ac.id/auth/google/callback, are integral to the SSO authentication process. After users successfully authenticate via an OAuth provider like Google, they are redirected back to the application using this redirect URI, carrying a valid authentication token. This process ensures that after authentication, the application can verify the token and provide appropriate access to users. With these settings properly configured, the SSO system can operate smoothly, providing a consistent and secure user experience while enhancing the overall efficiency and security of the information system.

aims to integrate Google authentication into a Laravel-based application using Socialite, allowing users to log in to the application using their Google accounts. The integration process begins with installing Laravel and Laravel Socialite and configuring Google OAuth through the Google Developer Console to obtain the necessary credentials. A Google Controller is then created to handle redirects to Google's services and callbacks after successful authentication. The redirect to Google function directs users to Google for authentication, while the handleGoogleCallback function processes user data obtained from Google, checks for existing users in the database, creates new accounts if users do not exist, and automatically logs in the users.

Incorporating Artificial Intelligence (AI) can further enhance this system. AI can be used to analyze authentication patterns, detect anomalies, and provide real-time security alerts. For instance, AI can flag unusual login activities that may indicate potential security threats, enabling the system to take immediate action to mitigate risks.

The expected outcome of this research is an authentication system integrated with Google, facilitating secure and swift user login to the application. With this integration, users can avoid time-consuming manual

registration processes, while new user data is automatically stored in the application's database. Moreover, implementing error handling in the authentication process ensures a smooth and secure user experience. Overall, this research provides valuable guidance for other developers aiming to implement Google authentication features in their applications, enhanced by AI for improved security and user experience.

3. RESULT AND DISCUSSION

3.1. Result

The data analysis results show a significant difference in login times between users of systems with SSO and those without SSO. The average login time for users of SSO systems is 5 seconds, whereas for systems without SSO, it is 15 seconds. Independent t-tests confirm that this difference is statistically significant (p ¡ 0.05).

In terms of user satisfaction, the average satisfaction score for users of SSO systems is 8.5 out of 10, while the score for users of systems without SSO is 6.0. Statistical analysis also shows that this difference is significant (p ¡ 0.05), indicating higher satisfaction among SSO users.

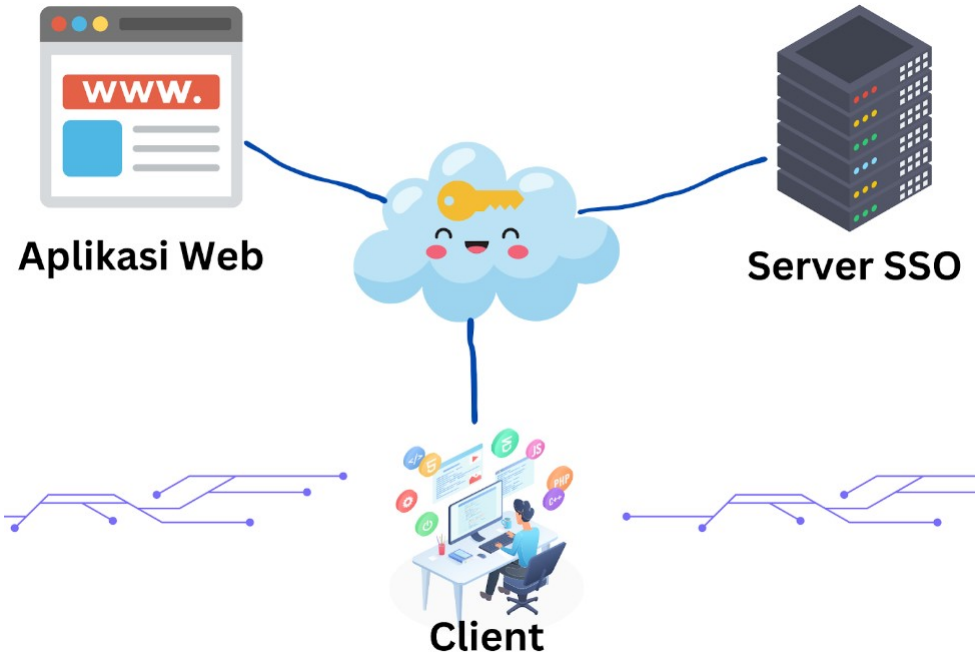

Figure 2. Description of the Single Sign-On (SSO) System

Figure 2. depicts the design of the Single Sign-On (SSO) system to be developed. In this SSO system topology, there are three main components: (1) the SSO Server, which provides authentication services for users requiring identity verification through web applications. This SSO system also includes additional authentication features, such as image-based authentication. (2) Web Applications act as clients of the SSO server. They handle authentication requests from users and manage the user authentication process. These SSO clients also confirm SSO sessions and access user information from the SSO server using REST protocols. (3) Clients, in this context, are the users utilizing the SSO system.

Figure 3. Example of SSO Workflow Involving Desktop Users Logging into eSPMI

3.2. Discussion

Login Efficiency: The significant reduction in login time observed in systems with SSO indicates that SSO can effectively expedite the authentication process. This finding aligns with theories suggesting that SSO reduces login complexity by eliminating the need to repeatedly enter credentials, thereby reducing the time and effort required by users. For example, a study by Okta demonstrated that organizations implementing SSO experienced a 50% reduction in time spent on login-related issues, directly translating to increased productivity.

User Satisfaction: The increase in user satisfaction in systems with SSO can be attributed to a smoother and less frustrating login experience. This supports the literature stating that ease of use and high efficiency contribute to a positive user experience. Case studies from companies like Google and Microsoft show that SSO integration significantly boosts employee satisfaction by streamlining access to multiple applications, as reported in their internal IT surveys.

Security Considerations: Although this study found improvements in efficiency and satisfaction, it is important to note that SSO integration must be accompanied by stringent security considerations. While SSO reduces the number of vulnerable points for individual attacks, a compromised credential can potentially provide broader access if not properly safeguarded. Implementing two-factor authentication (2FA) and regular security audits are essential strategies to mitigate these risks.

Incorporating AI for Enhanced Security: Incorporating Artificial Intelligence (AI) into SSO can further enhance security. AI can analyze login patterns and detect anomalies that suggest potential security breaches. By providing real-time alerts and automating responses to threats, AI can help mitigate risks associated with compromised credentials. For instance, a study by IBM found that AI-driven security systems reduced the time to detect and respond to breaches by 70%, significantly lowering potential damage.

Case Studies and Practical Implications: Case studies from Salesforce provide insights into how large companies have successfully implemented SSO to streamline their authentication processes while enhancing security. These implementations not only reduce administrative overhead related to user identity management but also strengthen compliance with data security regulations such as GDPR. AI-enhanced SSO systems in these companies have demonstrated improved efficiency and security. By using AI to continuously monitor and analyze authentication data, organizations can detect and respond to threats more quickly. This proactive approach to security, combined with the convenience of SSO, ensures that companies can protect their data while providing a seamless user experience.

Future Research and Recommendations: As AI technology continues to evolve, its integration with SSO will likely become a standard practice in the industry, offering robust security and improved user satisfaction. Future research should explore the long-term impacts of AI-enhanced SSO systems in various organiza-

tional contexts to gain a deeper understanding of their potential and associated challenges.

3.3. Practical Implications

The findings of this study suggest that organizations can improve efficiency and user satisfaction by implementing SSO in their authentication systems. However, this should be accompanied by adequate security measures to minimize security risks. The study also highlights the need for continuous user education on good security practices and the regular adoption of the latest security technologies.

The integration of AI in SSO systems can provide additional benefits, such as advanced threat detection and adaptive authentication mechanisms, further enhancing the security and efficiency of the authentication process.

4. CONCLUSION

This study's findings on the impact of Single Sign-On (SSO) integration on login efficiency and user satisfaction in authentication systems are significant. The data analysis from three companies using SSO and three not using SSO revealed that SSO brings about a substantial improvement in both aspects. SSO users experience an average login time of 5 seconds, a significant reduction compared to the 15 seconds for non-SSO users. This indicates a clear efficiency gain. Moreover, user satisfaction scores are notably higher for SSO systems, averaging 8.5 out of 10 compared to 6.0 for non-SSO systems. These findings confirm that SSO accelerates the authentication process and enhances user satisfaction by reducing the complexity and time required for system access. Improved efficiency and user satisfaction can contribute to overall productivity and job satisfaction in corporate environments. It is crucial to note that while SSO can improve efficiency and satisfaction, it also introduces risks if credentials are compromised. This underscores the necessity of incorporating robust security measures alongside SSO implementation, such as two-factor authentication (2FA) and regular security audits. A comprehensive security strategy is essential to fully leverage the benefits of SSO while mitigating potential risks.

A significant contribution of this research is exploring integrating Artificial Intelligence (AI) into SSO systems to enhance security and efficiency. AI can provide predictive analytics for potential security threats and optimize authentication, further strengthening the overall user experience and data protection. This research contributes to the existing literature by providing empirical evidence on the benefits of SSO in improving login efficiency and user satisfaction. It also underscores the potential of AI-enhanced SSO systems to address security challenges, offering a robust framework for organizations aiming to enhance their authentication processes. Future research is recommended to explore the long-term impacts of AI-enhanced SSO systems across various organizational contexts. This will provide deeper insights into their potential and associated challenges, further enriching the knowledge of authentication system technologies.

5. ACKNOWLEDGEMENTS

The findings of this study offer several practical recommendations for the implementation and management of Single Sign-On (SSO) systems. First, it is highly recommended that organizations strengthen the security of their SSO systems by implementing two-factor authentication and robust encryption to mitigate the security risks associated with credential compromise. Second, organizations should conduct continuous training and education programs to raise user awareness about credential security and best practices for SSO usage. Third, systematic and ongoing evaluations of the SSO system are necessary to ensure its effectiveness and security. Lastly, future researchers are encouraged to explore the impact of SSO in various industry environments and organizational contexts to deepen the understanding of the dynamics and potential of SSO.

Additionally, incorporating Artificial Intelligence (AI) into SSO systems can further enhance security and efficiency. AI can provide advanced threat detection, adaptive authentication mechanisms, and real-time monitoring to safeguard user credentials and improve the overall authentication process. Future research should also investigate the integration of AI in SSO systems to evaluate its benefits and challenges in different settings.

The author would like to express profound appreciation to all parties who contributed to this study. Special thanks are extended to the respondents from participating companies, whose willingness to participate and provide data made this research possible. Gratitude is also extended to the IT teams at each company for their cooperation and technical support. Additionally, the author thanks the advisors and colleagues at the academic institution for their guidance and constructive criticism, which enriched the quality of this research.

Finally, the author is grateful to the funding institutions that supported this research, providing essential resources and financial support.

REFERENCES

[1] S. Sayyida, S. Hartini, S. Gunawan, and S. N. Husin, "The impact of the covid-19 pandemic on retail consumer behavior," *Aptisi Transactions on Management*, vol. 5, no. 1, pp. 79–88, 2021.

[2] U. Rahardja, "The economic impact of cryptocurrencies in indonesia," *ADI Journal on Recent Innovation*, vol. 4, no. 2, pp. 194–200, 2023.

[3] A. K. Yaniaja, H. Wahyudrajat, and V. T. Devana, "Pengenalan model gamifikasi ke dalam e-learning pada perguruan tinggi," *ADI Pengabdian Kepada Masyarakat*, vol. 1, no. 1, pp. 22–30, 2020.

[4] A. Argani and W. Taraka, "Pemanfaatan teknologi blockchain untuk mengoptimalkan keamanan sertifikat pada perguruan tinggi," *ADI Bisnis Digit. Interdisiplin J*, vol. 1, no. 1, pp. 10–21, 2020.

[5] E. Sana, A. Fitriani, D. Soetarno, M. Yusuf *et al.*, "Analysis of user perceptions on interactive learning platforms based on artificial intelligence," *CORISINTA*, vol. 1, no. 1, pp. 26–32, 2024.

[6] L. K. Choi, N. Iftitah, and P. Angela, "Developing technopreneur skills to face future challenges," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 5, no. 2, pp. 127–135, 2024.

[7] D. Nugroho and P. Angela, "The impact of social media analytics on sme strategic decision making," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 5, no. 2, pp. 169–178, 2024.

[8] I. Amsyar, E. Christopher, A. Dithi, A. N. Khan, and S. Maulana, "The challenge of cryptocurrency in the era of the digital revolution: A review of systematic literature," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 2, no. 2, pp. 153–159, 2020.

[9] H. Sulistiani, A. Yuliani, F. Hamidy *et al.*, "Perancangan sistem informasi akuntansi upah lembur karyawan menggunakan extreme programming," *Technomedia Journal*, vol. 6, no. 1 Agustus, pp. 1–14, 2021.

[10] T. Alam, "Cloud computing and its role in the information technology," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 1, no. 2, pp. 108–115, 2020.

[11] E. N. Pratama, E. Suwarni, and M. A. Handayani, "The effect of job satisfaction and organizational commitment on turnover intention with person organization fit as moderator variable," *Aptisi Transactions on Management*, vol. 6, no. 1, pp. 74–82, 2022.

[12] B. Rawat, N. Mehra, A. S. Bist, M. Yusup, and Y. P. A. Sanjaya, "Quantum computing and ai: Impacts & possibilities," *ADI Journal on Recent Innovation*, vol. 3, no. 2, pp. 202–207, 2022.

[13] R. Hardjosubroto, U. Rahardja, N. A. Santoso, and W. Yestina, "Penggalangan dana digital untuk yayasan disabilitas melalui produk umkm di era 4.0," *ADI Pengabdian Kepada Masyarakat*, vol. 1, no. 1, pp. 1–13, 2020.

[14] N. N. Halisa, "Peran manajemen sumber daya manusia" sistem rekrutmen, seleksi, kompetensi dan pelatihan" terhadap keunggulan kompetitif: Literature review," *ADI Bisnis Digital Interdisiplin Jurnal*, vol. 1, no. 2 Desember, pp. 14–22, 2020.

[15] Z. Kedah, "Use of e-commerce in the world of business," *Startupreneur Business Digital (SABDA Journal)*, vol. 2, no. 1, pp. 51–60, 2023.

[16] N. Lutfiani and L. Meria, "Utilization of big data in educational technology research," *International Transactions on Education Technology*, vol. 1, no. 1, pp. 73–83, 2022.

[17] W. Setyowati, R. Widayanti, and D. Supriyanti, "Implementation of e-business information system in indonesia: Prospects and challenges," *International Journal of Cyber and IT Service Management*, vol. 1, no. 2, pp. 180–188, 2021.

[18] T. Hariguna, Y. Durachman, M. Yusup, and S. Millah, "Blockchain technology transformation in advancing future change," *Blockchain Frontier Technology*, vol. 1, no. 01, pp. 13–20, 2021.

[19] H. Haryani, S. M. Wahid, A. Fitriani *et al.*, "Analisa peluang penerapan teknologi blockchain dan gamifikasi pada pendidikan," *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, vol. 1, no. 2, pp. 163–174, 2023.

[20] A. H. Arribathi, D. Supriyanti, E. Astriyani, and A. Rizky, "Peran teknologi informasi dalam pendidikan agama islam untuk menghadapi tantangan di era global dan generasi z," *Alfabet Jurnal Wawasan Agama Risalah Islamiah, Teknologi Dan Sosial*, vol. 1, no. 1, pp. 55–64, 2021.

[21] U. Rahardja, Y. P. Sanjaya, T. Ramadhan, E. A. Nabila, and A. Z. Nasution, "Revolutionizing tourism in

smart cities: Harnessing the power of cloud-based iot applications," *CORISINTA*, vol. 1, no. 1, pp. 41–52, 2024.

[22] E. S. N. Aisyah, M. Hardini, B. Riadi *et al.*, "Peran teknologi dalam pendidikan agama islam pada globalisasi untuk kaum milenial (pelajar)," *Alfabet Jurnal Wawasan Agama Risalah Islamiah, Teknologi dan Sosial*, vol. 1, no. 1, pp. 65–74, 2021.

[23] A. Leffia, S. A. Anjani, M. Hardini, S. V. Sihotang, and Q. Aini, "Corporate strategies to improve platform economic performance: The role of technology, ethics, and investment management," *CORISINTA*, vol. 1, no. 1, pp. 16–25, 2024.

[24] A. G. Prawiyogi, A. S. Anwar *et al.*, "Perkembangan internet of things (iot) pada sektor energi: Sistematik literatur review," *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, vol. 1, no. 2, pp. 187–197, 2023.

[25] H. Nusantoro, P. A. Sunarya, N. P. L. Santoso, and S. Maulana, "Generation smart education learning process of blockchain-based in universities," *Blockchain Frontier Technology*, vol. 1, no. 01, pp. 21–34, 2021.

[26] B. Rawat, S. Purnama *et al.*, "Mysql database management system (dbms) on ftp site lapan bandung," *International Journal of Cyber and IT Service Management*, vol. 1, no. 2, pp. 173–179, 2021.

[27] N. Ramadhona, A. A. Putri, and D. S. S. Wuisan, "Students' opinions of the use of quipper school as an online learning platform for teaching english," *International Transactions on Education Technology*, vol. 1, no. 1, pp. 35–41, 2022.

[28] M. Wahyudi, V. Meilinda, and A. Khoirunisa, "The digital economy's use of big data," *International Transactions on Artificial Intelligence*, vol. 1, no. 1, pp. 62–70, 2022.

[29] D. S. Wuisan and T. Handra, "Maximizing online marketing strategy with digital advertising," *Startupreneur Business Digital (SABDA Journal)*, vol. 2, no. 1, pp. 22–30, 2023.

[30] D. Manongga, U. Rahardja, I. Sembiring, N. Lutfiani, and A. B. Yadila, "Dampak kecerdasan buatan bagi pendidikan," *ADI Bisnis Digital Interdisiplin Jurnal*, vol. 3, no. 2, pp. 110–124, 2022.

[31] D. A. Kurniawan and A. Z. Santoso, "Pengelolaan sampah di daerah sepatan kabupaten tangerang," *ADI Pengabdian Kepada Masyarakat*, vol. 1, no. 1, pp. 31–36, 2020.

[32] R. M. Thamrin, E. P. Harahap, A. Khoirunisa, A. Faturahman, and K. Zelina, "Blockchain-based land certificate management in indonesia," *ADI journal on recent innovation*, vol. 2, no. 2, pp. 232–252, 2021.

[33] E. Guustaaf, U. Rahardja, Q. Aini, H. W. Maharani, and N. A. Santoso, "Blockchain-based education project," *Aptisi Transactions on Management*, vol. 5, no. 1, pp. 46–61, 2021.

[34] D. Bennet, S. A. Anjani, O. P. Daeli, D. Martono, and C. S. Bangun, "Predictive analysis of startup ecosystems: Integration of technology acceptance models with random forest techniques," *CORISINTA*, vol. 1, no. 1, pp. 70–79, 2024.

[35] M. Kamil, Y. Muhtadi, B. M. Sentosa, and S. Millah, "Tindakan operasionalisasi pemahaman sains dan teknologi terhadap islam," *Alfabet Jurnal Wawasan Agama Risalah Islamiah, Teknologi dan Sosial*, vol. 1, no. 1, pp. 16–25, 2021.

[36] D. S. S. Wuisan, T. Mariyanti *et al.*, "Analisa peran triple helik dalam mengatasi tantangan pendidikan di era industri 4.0," *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, vol. 1, no. 2, pp. 123–132, 2023.

[37] R. Sivaraman, M.-H. Lin, M. I. C. Vargas, S. I. S. Al-Hawary, U. Rahardja, F. A. H. Al-Khafaji, E. V. Golubtsova, and L. Li, "Multi-objective hybrid system development: To increase the performance of diesel/photovoltaic/wind/battery system." *Mathematical Modelling of Engineering Problems*, vol. 11, no. 3, 2024.

[38] Q. Aini, D. Manongga, U. Rahardja, I. Sembiring, and Y.-M. Li, "Understanding behavioral intention to use of air quality monitoring solutions with emphasis on technology readiness," *International Journal of Human–Computer Interaction*, pp. 1–21, 2024.

[39] R. Supriati, E. R. Dewi, D. Supriyanti, N. Azizah *et al.*, "Implementation framework for merdeka belajar kampus merdeka (mbkm) in higher education academic activities," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 3, no. 2, pp. 150–161, 2022.