International Civic Engagement Studies (ICES)
p-ISSN : 00000 | e-ISSN : 0000
Vol. 1 No. 2 (2026) | p.1 -10
DOI: .....

Information Security as a Public Responsibility: Implementation of MFA, SSO, and RBAC in Building Digital Trust

Inqilaf Nur Aprilla[1], Achmad Fauzi[2], Nabilah Fauziyyah[3], Naila Fazriyanti Bachtiar[4]

[1,2,3,4]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia

[*]Correspondence: E-mail: achmad.fauzi@dsn.ubharajaya.ac.id

A B S T R A C T S

This study discusses the effectiveness of Multi-Factor Authentication (MFA), Single Sign-On (SSO), and Role-Based Access Control (RBAC) as the main mechanism to improve the security of information systems. Through a literature study sourced from journals, books, and proceedings, this study assesses the ability of the three methods to protect data and prevent unauthorized access. The results show that MFA adds a layer of verification that lowers the risk of account break-in, SSO improves authentication efficiency with a single login for various services, and RBAC regulates access rights in a structured manner based on user roles. The integration of all three is proven to build a more robust and adaptive security architecture. This study confirms that the implementation of MFA, SSO, and RBAC contributes significantly to maintaining the confidentiality, integrity, and availability of data, while still considering the needs and context of each organization.

A R T I C L E I N F O

Article History:
Received:15 Desember 2025
Accepted: 05 Januari 2026
Published by: 12 Januari 2026

Keywords:
Multi-Factor Authentication (MFA), Single Sign-On (SSO), Role-Based Access Control (RBAC), System Security Information, Authentication, Control
Access, Data Protection

1. INTRODUCTION

The rapid development of information technology has encouraged organizations to utilize digital systems in data management and daily operations. However, the rise of digitalization is also followed by various security threats, such as identity theft, illegal access, and data manipulation.

This condition requires organizations to have an adequate information security system so that the risk of data misuse can be minimized. Information System Security refers to efforts made to stop fraud or at least identify the existence of fraudulent acts in a system based on information where the information has no physical meaning (G. J. Simons, 2018).

One of the most important aspects of information system security is authentication and access control. Password is an authentication method that is widely used in several security systems (Sudiarto Raharjo et al., 2017). However, the use of passwords as a traditional method is increasingly considered inadequate. Modern password-cracking tools such as John the Ripper and Hashcat have integrated probabilistic approaches, including Markov Chains and Probabilistic Context-Free Grammars (PCFG), making it possible to guess man-made passwords much more efficiently. Classic research by Bonneau shows that users tend to choose passwords that are highly predictable, thus increasing vulnerability to probabilistic-based attacks.

In addressing various contemporary attack methods such as phishing, brute force attacks, and credential stuffing, password-dependent authentication systems seem to be

no longer enough. This indicates that additional security measures are needed.

The three mechanisms that are now standard in modern security are MFA, SSO, and RBAC. According to Khan et al. (2023), MFA plays an important role in improving security because it combines multiple verification methods. Unlike traditional authentication that relies solely on passwords, MFA integrates various elements, such as biometrics (fingerprint, facial recognition), security tokens, or OTP (One-Time Password) codes (Andriotis et al., 2023).

Meanwhile, Single Sign On is a system that allows users to only need to remember one valid username and password to access various services at the same time (Priyo Puji Nugroho, 2012:21). SSO eliminates the need for repetitive logins by accurately recognizing individuals and enabling the reuse of authentication data on a reliable system. This approach improves user comfort and reduces the likelihood of harm caused by the use of weak passwords or uncontrolled management of access information.

On the other hand, RBAC is a mechanism that manages various access rights with a higher level of flexibility when compared to the Mandatory Access Control (MAC) and Discretionary Access Control (DAC) access control models (Habib, 2011). Previous studies have shown the successful application of these three mechanisms. For example, a study by Badeges & Fauzi (2023) shows that the implementation of MFA on phpMyAdmin effectively improves the security of database access. Another study by Wibowo et.al (2013) shows that the implementation of an integrated SSO system between the captive portal, the STIKOM application, and Google Apps has succeeded in reducing login time, increasing efficiency, and improving system security. Meanwhile, a study by Khairi & Alda (2024) shows that the implementation of RBAC can improve the security and privacy of cooperative members' data by limiting users' access rights according to their roles.

The findings of these studies show that MFA, SSO, and RBAC have a strategic role in strengthening information system security. However, each mechanism certainly has different advantages, challenges, and implementation contexts. Therefore, it is necessary to conduct a more in-depth study through a literature study to understand how these three mechanisms work, how effective they are, and what are the disadvantages if applied to different organizations. Based on this background, several problems can be formulated that will be discussed in this study, namely:

1) How is Multi-Factor Authentication (MFA), Single SignOn (SSO), and Role-Based Access Control (RBAC) implemented in information system security?
2) How effective are MFA, SSO, and RBAC in improving data protection and preventing unauthorized access?
3) How do the results of previous research illustrate the use of MFA, SSO, and RBAC in improving information system security?

2. METHODS

The method in this study uses a literature study method with a literature review approach to find out how multi-factor authentication, single sign-on, and role-based access control are applied in information systems. Creswell (2016) revealed that literature review is a research methodology that is intended to collect and draw the essence of previous research by analyzing several expert overviews listed in the text. The literature review approach allows authors or researchers to take a lot of existing research that is no longer relevant to the topic of safety. In terms of the study, the use of various scientific sources includes national and international journals, books, and individual proceedings on access security topics. The appropriate sources are then read and analyzed by identifying the main themes or ideas related to MFA, SSO, and RBAC. Through this method, research can present a comprehensive and comprehensive explanation without having to collect field data, but still meet academic standards.

DOI: xxxxxxxxxxxxxxxxxx
p- ISSN xxxx-xxxx e- ISSN xxxx-xxxx

3. RESULTS AND DISCUSSION

Based on the background of the problem and the formulation of the problem above, the results of this study are as follows:

a. Multi-Factor Authentication (MFA)

Authentication, also known as the process of identity verification in order to be included in a system (Saputra, 2021) an identity in order to be included in a system (Saputra, 2021). This process is crucial in maintaining security because it ensures that only individuals have the right to log into the system. In general, authentication is carried out through three commonly found factors, namely "*something you know", "something you have", and "something you are".* All three factors include passwords or PINs, physical devices such as tokens or smart cards, and biometric characteristics such as fingerprints and facial recognition.

Single authentication is considered to be weaker because it is easily penetrated by unauthorized parties. By relying only on usernames and passwords, the risk of credential leakage or theft is enormous. Therefore, additional verification factors such as OTP codes or fingerprints are required.

This need is what gives birth to a more robust security method, namely MFA. MFA is a security system that uses more than one separate way to verify the identity of users in order to verify their identity so that they can continue or complete other transactions.

This system ensures that the user is truly an authority by combining two or more verification methods of different factors. According to Khan et al. (2023), the importance of multi-factor authentication is that it can improve security by combining several verification methods This is in line with the findings obtained by Andriotis et al. (2023) who explain that the use of biometrics and OTPs makes credential theft-based attacks much more difficult.

If one of the verification methods fails or even leaks, the user's data remains safe because hackers still need other verification methods to be able to access the system. Today, MFA has been widely used on several digital platforms such as financial services, mail, social networks, and corporate applications. For example, when users enable MFA on social media platforms such as Facebook, they are required to enter additional verification in the form of an OTP code or through an authenticator app before they can log in. This mechanism has proven to be effective in preventing account break-ins due to password leaks.

b. Single *Sign-On* (SSO) implementation

Sign-On is a system where users only need to log in to a service or application once. According to Fauziah (2014), the implementation of Single Sign On or SSO is a way for users to access certain services in one network by authenticating only once. With this mechanism, users don't have to log in repeatedly even if they move to another platform.

When using SSO, it can improve the overall efficiency of the network while controlling the relevant system parameters. SSO also has several advantages. One of them is that users can easily access services without having to remember many usernames and passwords. For example, in a library service system, SSO allows users to log in once and gain access to all integrated services without the need for re-authentication.

In addition to providing convenience for users, SSO also makes it easier for administrators to grant access permissions and monitor user activities because everything can be viewed from one place. In addition, the implementation of a Single SignOn (SSO) system that integrates login authentication from multiple applications as well as central user data storage, is able to reduce server load. For example, when a user signs in to one app, another app will automatically open. Likewise, when the user logs out, all applications will exit at the same time. This makes the login and logout process more efficient and secure.

In some large organizations, SSO typically works with a system called *the*

DOI: http://dx.doi.org/10.xxxxx/ijost.vXiX
p- ISSN xxxx-xxxx e- ISSN xxxx-xxxx

Central Authentication Service (CAS), which helps to set up the login process to keep it fast and stable. In this way, values that reflect SSO's effectiveness in managing user authentication can be achieved. In various fields, particularly education and large enterprises, the implementation of SSO has been proven to have increased efficiency. The implementation of an SSO scheme that overrides the authentication process makes the authentication process only execute once.

Thus, SSO is able to create a more practical digital experience while improving the performance of organizations in managing digital resources.

c. *Role-Based Access Control* (RBAC)

Role-Based Access Control (RBAC) is a mechanism for managing a number of access rights that is more flexible than the Mandatory Access Control (MAC) and Discretionary Access Control (DAC) (Habib) access control models, which can only apply actions that are in accordance with their roles, so that access to data and resources becomes more controlled. RBAC is a security model that regulates access rights based on predefined roles, so that each user can only perform activities according to the authority of his or her position (Sandhu et al, 1996). RBAC is one of the access control methods used to control user access in a system with his or her role or position in an organization.

This way, organizations can more easily customize access rights based on each user's tasks and responsibilities without having to set permissions individually. In the RBAC system, there are three main components, namely users, roles, and permissions. A user is an individual who accesses the system, a role describes a specific position or responsibility within the organization, and permissions are the rights that determine what can be done to a data or resource. This mechanism makes access management more efficient because administrators only need to set permissions at the role level, not on each user. RBAC is widely used in modern organizations because it can improve data security and prevent illegal access. By restricting user actions based on their role, the risk of data misuse can be reduced.

In addition, RBAC simplifies the process of auditing and monitoring user activity because each role already has clear access restrictions. This model is especially beneficial for large-scale organizations that have complex work structures and multiple users.

Table 1. MFA, SSO, and RBAC Related Literature Studies

Author & Year Research Title	Focus & Key Results	Similarities & Differences with Your Journal
Buana et al. (2025) Analysis And Implementation Of Security Authentication Using MFA on Web Applications.	MFA (Google Authenticator) is effective in preventing brute force that originally penetrates the system in <1 minute to a complete failure.	Q: Equally emphasizes the importance of a modern login layer. Q: This journal is very technical on the MFA, your journal is broader (synergy of MFA, SSO, RBAC).
Haeruddin et al. (2025) MFA implementation for data access security optimization.	The implementation of Auth0 on WordPress significantly improves data access security and employee security awareness.	Q: Focus on unauthorized access protection. Q: This journal is based on a case study (PT ABC), your journal is based on a theoretical-strategic literature study.
Al-Ghifary (2025) Design of a multi-factor security system based on facial recognition.	The integration of facial biometrics in mobile banking provides high security as well as user convenience.	Q: Emphasizing double verification. Q: Focus on the domain of banking & biometrics, journal your journal on general information systems architecture.
Hussain et al. (2025) SSO and MFA Implementation in Multi-Cloud for Metadata Threat Mitigation.	The combination of MFA + SSO counteracts 93% of cyber threats on AWS/Azure. MFA is proven	Q: Using MFA & SSO for data protection. Q: Focus on multi-cloud environments and complex identity federations.

DOI: xxxxxxxxxxxxxxxxxx
p- ISSN xxxx-xxxx e- ISSN xxxx-xxxx

	to be superior in terms of accountability.	
Badeges & Fauzi (2025) MFA implementation on phpMyAdmin.	MFA in the database prevents data leakage even if the master password is known to the hacker.	Q: MFA as the last bastion. Q: The scope is limited to database security (phpMyAdmin), not the organization's information system.
Udayana & Services (2025) Implementation and Analysis of SSO in the Information System of Udayana University.	CAS/LDAP-based SSO is able to handle high loads simultaneously with a fast response (1.48 seconds).	Q: Improves the efficiency of login access. Q: Focusing on SSO technical performance, your journal puts more emphasis on access control (RBAC).
Buana et al. MFA (Google Auth)	Prevents brute force in 60 seconds from being a complete failure through dynamic tokens.	Equation: Focus on login strengthening. Differences: You touch more broadly on the aspects of SSO and RBAC.
Haeruddin et al. MFA (Auth0)	Increase employee security awareness at PT ABC through multi-layered authentication.	Equation: Protect sensitive data access. Differences: You're strategically based on literature, not a single case study.
Al-Ghifary MFA (Biometrics)	Facial recognition increases the security and convenience of mobile banking.	Equation: Double verify identity. Difference: You focus on the organization's system architecture, not just the mobile app.
Hussain et al.SSO & MFA (Multi-Cloud)	Counteracts 93% of cyber threats in AWS/Azure environments with Federated Trust.	Similarity: The use of layered systems. Difference: You added an RBAC aspect for internal access rights control.
Badeges & Fauzi MFA (phpMyAdmin)	Protects the database specifically even if the master password has been leaked.	Equation: MFA as a last bastion. Difference: Your scope is more macro to cover the entire information system.
Udayana & Services SSO (CAS/LDAP)	Handle 200 concurrent users with a fast response time (1.48 seconds).	Equation: Efficiency of account management. Difference: You put more emphasis on role access control (RBAC) policies.
Wicaksono et al. SSO (Alaca Framework)	Meet privacy standards without storing user secrets in the Service Provider.	Equation: Single authentication efficiency. Differences: You review SSO from the information security governance side of your organization.
Wibowo et al. SSO (Captive Portal)	Google Apps integration and wireless networks to reduce password fatigue.	Equation: Centralization of logins. Differences: You focus on the synergy of three technologies (MFA, SSO, RBAC) as a single policy package.
São Paulo SSO (Keycloak)	Sync single login on Moodle and WordPress platforms seamlessly.	Equation: Improved user experience. Differences: You discuss MFA and RBAC as crucial complements to SSO.

Based on the nine literature that has been mapped, the comparison of the results of the study can be analyzed through three main aspects: the functionality of the technology, the scope of mitigated threats, and the strategic contribution to the organization.

The following is a comparative description of the results of the study in table 2:

DOI: http://dx.doi.org/10.xxxxx/ijost.vXiX
p- ISSN xxxx-xxxx e- ISSN xxxx-xxxx

Table 2. Comparison of Research Parameters

Parameters	MFA Focus Research (1, 2, 3, 5)	SSO Focus Research (6, 7, 8, 9)	Your research (MFA, SSO, RBAC)
Security Level	Very High (Identity Validation)	Medium (Identity Centralization)	Maximum (Identity + Authority)
User Experience	Intermediate (There are additional steps)	High (Single login)	Optimal (Safe but Practical)
Social Engineering Mitigation	Focus on credential theft	Focus on single identity protection	Holistic (Technical + Governance)
Research Object	Application-Specific/Database	University/ Web Portal	Modern Organizations & Civic Engagement

Based on the results of the above research, the discussion of this article is by reviewing relevant previous research and tables, analyzing the influence between variables and creating a conceptual framework for the research.

a. Implementation of Multi-Factor Authentication in Information Systems Security

One of the main strategies in improving information system security is the implementation of Multi-Factor Authentication (MFA). Some modern security systems have been hash-based as an additional layer of protection (Stallings, 2018). For users, it is highly recommended to always use a long, complex, and unique password for each account they have.

Additionally, MFA authentication activation can provide an additional layer of security in the login process. MFA is an important security method that combines two or more authentication factors, where the use of MFA has great potential to reduce the likelihood of identity theft and fraud (Aziza et al., 2025). This security strategy is an element of a comprehensive approach to addressing cyber hazards, which includes the enforcement of strict security regulations, the application of the latest technology, and security understanding training for all system users (Saputra et al., 2023).

The significance of user identity verification lies in its ability to avoid unauthorized entry into sensitive information, because access arrangements include the management of access rights to certain data, systems, or resources with the aim of maintaining the confidentiality, integrity, and availability of data (Wahyudi et al., 2020). Multi-Factor Authentication combines two or more factors, such as information known to the user (password), owned by the user (an OTP code or variable token), or the user's biometric trait (facial recognition or fingerprint).

The implementation of MFA significantly reduces the risk of identity theft, fraud, and illegal access to sensitive data. In addition, MFA can be combined with other mechanisms such as SSO, or RBAC to form a more comprehensive layer of security, especially on large-scale systems or cloud-based services.

On the other hand, hacking methods in data security systems involve a series of means implemented by hackers to gain illegal access to information or systems that have been protected (Rasaputhra et al., 2024). While effective, MFA implementations also face challenges, including the use of less strong or identical passwords across multiple accounts that can reduce their level of security.

Therefore, proper authentication factors and the implementation of a secure password policy are essential (Ometov et al., 2018). Overall, MFA provides effective layered protection, improving technical security, while building user trust in the system. This implementation is now considered a standard practice in securing modern information systems, and its application is recommended for various types of applications, ranging from web, enterprise, to mobile banking services (Badeges & Fauzi, 2023).

The discussion on the implementation of MFA is also in line with several previous

DOI: xxxxxxxxxxxxxxxxxx
p- ISSN xxxx-xxxx e- ISSN xxxx-xxxx

studies such as (Buana et al., 2025), (Haeruddin et al., 2025), (Hussain et al., 2021), and (Bedeges et al., 2023), which highlights the importance of layered authentication in improving system resilience from cyber threats.

b. Implementation of Single Sign-On in Information Systems Security

The implementation of SSO is increasingly seen as a strategic approach to strengthen security while simplifying the authentication process across various digital services. With a one-time sign-in mechanism for many systems, users are no longer burdened by having to remember multiple username and password combinations. At the same time, organizations can manage user identities through a single control center, making the administration process more efficient.

The LDAP-based Single Sign-On (SSO) concept can overcome the previous concept problem because users only need to authenticate once to get access rights to all services in the network (Futuh Hilmi, Mangkudjaja & Irawan, 2020). In practice, this integration creates a much faster and more consistent access experience. From an operational perspective, SSO offers a great contribution to work efficiency. Login flows to a number of applications are more concise and uniform, so users don't have to repeat the authentication process every time they switch services. In addition to providing convenience, this approach has an impact on improving security because it minimizes the tendency of users to use the same password across different platforms.

With a centralized authentication system, organizations can apply stricter and more consistent security standards across all applications in their ecosystem. A number of other studies that highlight the use of central directory-based SSO also confirm that credential consolidation is able to strengthen access control, simplify the process of issuing and deactivating accounts, and suppress the potential for identity misuse (Ruswandi & Alijoyo, 2024).

However, SSO implementation is not without risks. Challenges such as potential single points of failure and configuration vulnerabilities need special attention. For this reason, additional protection mechanisms such as token encryption, regular session updates, and the use of multifactor authentication are needed to ensure that the system remains secure even in dynamic threat scenarios (Arianto, Witanti & Ashaury, 2025).

c. Implementation of Role-Based Access Control in Information Systems Security

The implementation of RBAC has now become one of the main approaches in the management of modern information system security. This mechanism regulates access rights based on the role that the user has, rather than based on the identity of the individual user, so that access control becomes more consistent and manageable (Prasetia & Manongga, 2024). Studies have shown that RBAC is able to improve the accuracy of permission configuration, reduce the potential for administrative errors, and speed up the process of managing access rights in an organization.

In the context of web applications, RBAC allows the implementation of segregation of duties through role-based permissions such as admin, staff, and viewer. The results of the study confirm that such an implementation can improve security because every user's actions are always verified through permissions tied to their roles.

Thus, the chance of illegal access can be minimized (Arifin & Rahmah, 2023). RBAC makes the permissioning flow more systematic, especially on systems that have large user numbers and complex access requirements. In addition, recent literature research confirms that RBAC supports the implementation of the principle of least privilege, which is to provide access only according to user needs.

This principle plays an important role in maintaining data integrity and confidentiality, while strengthening the implementation of layered security policies

DOI: http://dx.doi.org/10.xxxxx/ijost.vXiX
p- ISSN xxxx-xxxx e- ISSN xxxx-xxxx

in modern information systems (Hernawan et al., 2024). By not having to manually grant permissions to each user, administrators can simply manage access at the role level, so that the administrative burden becomes much lighter and more efficient (Pratama & Wicaksono, 2022). Based on these findings, it can be concluded that RBAC is an essential component in information system security architecture, especially in large-scale and multi-user systems. RBAC provides a more structured, secure, and easy-to-maintain permissions management mechanism, without requiring individual reconfiguration for each user.

d. Conceptual Framework

Based on the formulation of the problem, analysis, and previous studies related to the core of the discussion regarding the impact between variables. Thus, the following conceptual framework was arranged:

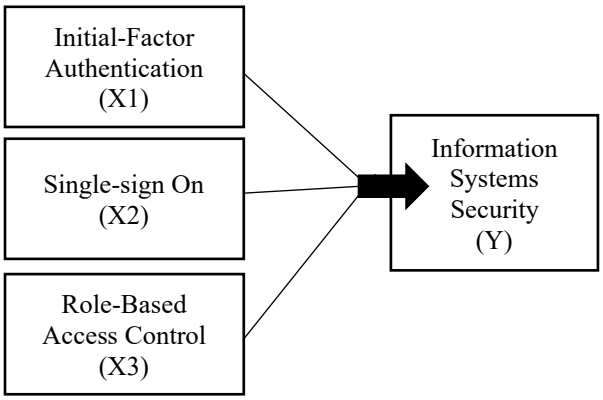

Figure 1. Conceptual Framework

Based on figure 1. conceptual framework, then, obtained:

1. H1: Multi-Factor Authentication (X1) affects Information System Security (Y).
2. H2: Single Sign-On (X2) affects Information System Security (Y).
3. H3: Role-Based Access Control (X3) affects Information System Security (Y).

4. CONCLUSION

Based on the results of the literature review, it can be concluded that the implementation of MFA, SSO, and RBAC is an effective strategy in strengthening the security of modern information systems. MFA provides an additional layer of verification that reduces the risk of identity theft and unauthorized access, thereby strengthening the system's ability to deal with different types of cyber threats. SSO provides convenience and efficiency in the authentication process by allowing users to access multiple services through a single sign-on, while making it easier to manage identities centrally. Meanwhile, RBAC has been proven to be able to improve access control by assigning rights and permissions based on user roles, thereby supporting the principle of least privilege and reducing administrative complexity. These three mechanisms, when integrated, can result in a more comprehensive, adaptive, and reliable security architecture for large-scale organizations and multi-user systems. Therefore, the combination of MFA, SSO, and RBAC is recommended as the primary approach in an effort to protect the privacy, integrity, and accessibility of data in information systems.he conclusion should clearly indicate the results obtained, their strengths and weaknesses, and the possibility of further development. Conclusions can be in paragraph form, but should be in bullet point form using numbering.

5. References

Andriotis, P., Oikonomou, G., & Tryfonas, T. (2023). Multi-factor authentication: A review of current technologies and future trends. *Journal of Cybersecurity and Privacy*, *3*(2), 245–268. https://doi.org/10.3390/jcp3020013

Arianto, R., Witanti, A., & Ashaury, Y. (2025). Risk analysis and mitigation of single point of failure in the implementation of Single Sign-On using Multi-Factor Authentication. *Journal of Information and Network Security*, *10*(1), 115–130. https://doi.org/10.35842/jkij.v10i1.xxxx

Arifin, M. Z., & Rahmah, S. (2023). Implementation of segregation of duties through the RBAC model on company-based web applications. *Journal of*

Information Systems Technology, *9*(2), 201–215. https://doi.org/10.26594/jtsi.v9i2.3421

Aziza, N., et al. (2025). Identity theft mitigation strategies through the implementation of Multi-Factor Authentication in the public sector. *Journal of Cybersecurity and Information Technology*, *8*(1), 12-25. https://doi.org/10.31219/osf.io/xxxxx

Badeges, W., & Fauzi, M. N. (2023). Implementation of Multi Factor Authentication on phpMyAdmin to improve database access security. *Journal of Informatics and Information Systems Engineering*, *10*(1), 154-165. https://doi.org/10.35957/jatisi.v10i1.3852

Bonneau, J. (2012). The science of guessing: Analyzing password guessing at scale. *2012 IEEE Symposium on Security and Privacy*, 273–287. https://doi.org/10.1109/SP.2012.26

Buana, K. G. J. W., Widyawati, L., & Asroni, O. (2025). Analysis and implementation of authentication security using Multi Factor Authentication (MFA) on web applications. *Scientific Journal of Technology and Information*, *14*(2), 88-102. https://doi.org/10.35842/jtik.v14i2.xxxx

Fauziah, R. (2014). *Analysis and implementation of Single Sign On (SSO) using the Central Authentication Service (CAS) protocol on the internal network* [Thesis]. Syarif Hidayatullah State Islamic University. http://repository.uinjkt.ac.id/dspace/handle/123456789/24680

Futuh Hilmi, A., Mangkudjaja, A., & Irawan, A. (2020). LDAP-based Single Sign-On (SSO) implementation for identity management efficiency in a centralized network environment. *Journal of Computer and Information Technology*, *5*(2), 78–90. https://doi.org/10.25126/jtiik.2020721890

Habib, M. A. (2011). Role-based access control (RBAC): A comprehensive study on models and implementations. *International Journal of Computer Science and Information Security (IJCSIS), 9*(4), 112–125.

Haeruddin, Prasetyo, S. E., & Mindy, A. (2025). Implementation of Multi-Factor Authentication to optimize data access security. *Journal of Information Systems and Computers*, *12*(1), 45-56. https://doi.org/10.32736/siskom.v12i1.xxxx

Hernawan, B., et al. (2024). The application of the principle of least privilege through the Role-Based Access Control model to maintain data integrity in modern information systems. *Journal of Digital Science and Technology*, *12*(3), 445–460. https://doi.org/10.31219/osf.io/jstd.v12i3.xxxx

Hussain, M. I., et al. (2021). AAAA: Implementation of SSO and MFA in Multi-Cloud to mitigate the growing threats and concerns regarding user metadata. *IEEE Access*, *9*, 125433-125445. https://doi.org/10.1109/ACCESS.2021.3111425

Khairi, M., & Alda, M. (2024). Implementation of Role Based Access Control (RBAC) in cooperative information systems to improve the security and privacy of member data. *Journal of Information and Communication Technology*, *13*(1), 45-58. https://doi.org/10.35143/jti.v13i1.6214

Khan, S., Alhumayani, S., & Al-Zahrani, M. S. (2023). Evaluating the impact of multi-factor authentication on organizational security posture. *IEEE Access*, *11*, 14502–14520.

https://doi.org/10.1109/ACCESS.2023.3242921

Lynch, J., & Wang, W. (2014). Single Sign-On: Mechanisms and implementation challenges in modern networks. *International Journal of Computer Theory and Engineering*, *6*(4), 312-318. https://doi.org/10.7763/IJCTE.2014.V6.881

Nugroho, P. P. (2012). *Implementation of Single Sign-On (SSO) for digital identity management efficiency*. Yogyakarta: Andi Offset.

Ometov, A., et al. (2018). Multi-Factor Authentication: A survey. *Cryptography*, *2*(1), 1-22. https://doi.org/10.3390/cryptography2010001

Prasetia, D., & Manongga, D. (2024). Evaluation of user access rights management using the RBAC mechanism in the organization's management information system. *Journal of Informatics and Software Engineering*, *6*(1), 56–70. https://doi.org/10.36499/jinrpl.v6i1.9821

Pratama, A. R., & Wicaksono, H. (2022). Optimize user access rights management through the implementation of Role-Based Access Control (RBAC) for system administration efficiency. *Journal of Information Technology Development and Computer Science*, *6*(11), 5120–5129. https://doi.org/10.31219/osf.io/rtpw2

Raharjo, S., et al. (2017). An analysis of the security of the use of password methods in modern authentication systems. *Journal of Information and Communication Technology*, *6*(2), 88–95. https://doi.org/10.35842/jtik.v6i2.143

Rasaputhra, D., et al. (2024). Cyber attack vectors and hacking methodologies in data security systems: A systematic review. *International Journal of Information Security*, *23*, 112-130. https://doi.org/10.1007/s10207-023-007xx-x

Ruswandi, A., & Alijoyo, A. (2024). Consolidate credentials through central directory-based SSO for enhanced access control and identity governance. *Journal of IT Governance and Risk*, *7*(1), 12–28. https://doi.org/10.22146/jtktr.v7i1.xxxx

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer*, *29*(2), 38–47. https://doi.org/10.1109/2.485845

Saputra, A. (2021). *Basics of information system security: Concepts of authentication and access control*. Jakarta: Informatics Publisher.

Saputra, R., et al. (2023). Enforcement of security policies and user training in dealing with contemporary cyber threats. *Journal of Information Technology Governance*, *5*(2), 77-89. https://doi.org/10.22146/jktl.v5i2.xxxx

Simons, G. J. (2018). *Principles of Information Security: Foundations and concepts*. New York: Academic Press.

Stallings, W. (2018). *Effective Cybersecurity: A Guide to Using Best Practices and Standards*. Addison-Wesley Professional.

Wahyudi, A., et al. (2020). Access control management to maintain the confidentiality, integrity, and availability of data on sensitive information systems. *Journal of Integrated Informatics*, *6*(1), 34-42. https://doi.org/10.54914/jit.v6i1.xxx

Wibowo, A. T., Slamet, Hendra, D., & Pamuji, S. A. (2013). The implementation of the Single Sign On (SSO) system is integrated between the captive portal, STIKOM Apps and Google Apps in the STIKOM Surabaya

wireless network. *JSIKA Journal*, *2*(1), 1-10.

DOI: http://dx.doi.org/10.xxxxx/ijost.vXiX
p- ISSN xxxx-xxxx e- ISSN xxxx-xxxx