Terbitan online pada laman https://jurnal.pelitabangsa.ac.id/index.php/jpcs

JPCS Journal of Practical Computer Science

Vol.4 No.1 Mei 2024 ISSN Media Elektronik: 2809-8137

Diterima 23 Mei 2024 | Direvisi 28 Mei 2024 | Dipublikasikan 30 Mei 2024

Evaluation of System Access Security in The Implementation of Multi-Factor Authentication (MFA) in Educational Institutions

Yuniana Cahyaningrum[1]*

[1]Craft Study Program, Faculty of Art and Design Indonesian Art Institute Surakarta
[1]yun14n4@gmail.com

Abstract

Information systems in educational institutions have the potential to be targeted by various parties, especially unauthorized parties, so they require a higher layer of security to protect sensitive data and secure user access. One solution that can be implemented is the implementation of Multi-Factor Authentication (MFA), a security approach that utilizes more than one authentication method to secure access to the system. MFA is a security method that requires more than one way to verify a user's identity when accessing a system, application, or service that aims to increase security by adding an additional layer of protection beyond using a single passphrase or password. This research aims to evaluate the effectiveness and impact of implementing MFA in the context of system access security in educational environments. The research methodology involves surveying system users, statistical analysis, and monitoring access activity to assess the extent to which MFA is successful in reducing security risks and protecting sensitive information. The research results show that the use of MFA in educational institutions can significantly increase system access security. Several obstacles that arise become challenges in solving problems regarding the use of MFA. Therefore, this article also examines recommendations for increasing the implementation of MFA in educational institutions. It is hoped that this research can contribute to the positive impact of MFA in improving system access security in the context of educational institutions by optimizing information technology in protecting data integrity and user access security.

Keyword: *Multi-Factor Authentication (MFA), Educational Institutions, System Access*

INTRODUCTION

In today's digital development era, educational institutions face big challenges in maintaining the security of their data and information systems. The increasing number of cyber-attacks and unauthorized access attempts poses a serious threat to the integrity of sensitive information, especially in educational environments which are often targeted by irresponsible parties. One effective way to improve system access security is through implementing Multi-Factor Authentication (MFA), a security strategy that requires more than one authentication method to grant access to users (Munir et al., 2023).

Education is actually a very essential and important thing, so that its implementation requires improvement and improvement in the quality of services (Cahyaningrum et al., 2021). For example, in a blockchain architecture in an educational institution, privacy needs to be protected to maintain its continuity. This of course cannot be separated from security or authentication issues in maintaining trust (Mishra et al., 2021).

Educational institutions have complex environments, with various types of users such as students, lecturers, and administrative staff who have different levels of access. In this case, the protection of personal data and information is a top priority. Conventional security efforts that only rely on passwords are increasingly vulnerable to attack, considering the many phishing and identity theft techniques that can bypass conventional security systems (Cahyaningrum et al., 2023).

The implementation of MFA in educational institutions is becoming increasingly relevant to address existing security gaps. By integrating more than one authentication method, such as a password, hardware token, or biometric authentication, it is able to provide a significant additional layer of security. The advantage of MFA lies in its ability to make unauthorized access attempts more difficult, even if the user's password is exposed (Cahyaningrum, 2023a). Current technological advances have various implications for various industries and sectors. Especially in identifying existing obstacles in the transformation of interoperability and scalability of data and information (Ray, 2023).

This research aims to evaluate the impact of implementing on system access security in educational institutions (Iftikhar et al., 2023). This research analyzes the extent to which can reduce security risks, protect sensitive data, and improve the integrity of information systems in educational environments. Additionally, this research will explore challenges that may arise during the implementation and provide recommendations to improve its effectiveness (Tripathi et al., 2023).

By identifying successes and barriers to implementing in educational institutions, this research will provide an important contribution to practical and theoretical understanding in the context of cyber security in education. It is hoped that the research findings will provide guidance for similar institutions in facing growing security challenges (Ibrahimy et al., 2023).

In research on single-point failure mitigation, a new and technologically advanced Multi-Factor Authentication (MFA) tool has been developed as a security solution (Tyagi & Sreenath, 2021). However, the usability and applicability of these tools has raised concerns. An obvious solution can be seen by conducting a user study to create a more user-friendly tool. The results show that the researchers found that lower adoption rates were inevitable for MFA, while avoidance was widespread among mandatory use (Das et al., 2019).

In several research, one of them is the implementation of for example in case study phpMyAdmin involves using a combination of something known such as a password, something owned such as a physical authentication token and something inherent such as a fingerprint or facial scan (Nanda et al., 2024). Through the implementation of MFA in phpMyAdmin, it aims to provide additional protection against hacker attacks and misuse of database access (Baldin et al., 2022). It is hoped that this article will help database managers and web developers in improving access security on phpMyAdmin, thereby protecting data stored in the database from security threats (Badeges & Fauzi, 2020).

Multi-Factor Authentication is one of the most widely used services by all types of people today, especially by many organizations (Buccafurri et al., 2024). People use this service to authorize stored data and access it without any security compromise. As the use of different storage systems for different types of data increases, we need to focus on security. Security threats can be a major threat to any company (Kaiser et al., 2022).

Using a username and password has become a daily necessity for someone to log in to a site. Authentication is a process or protocol that allows one entity to confirm the identity of another entity. Different organizations have different authentication requirements and so they define different authentication according to their type of needs. The main purpose of authentication is to secure data and systems from third parties. The authentication process is also used in military and government agencies, hospitals and other business settings (Komalasari, 2018).

The application of information and communication technology to an organization, individual, or related parties in the organization's external interactions with others includes the use of information technology to redesign its internal business processes (Vekariya et al., 2024). This is done so that the main business management can provide benefits in the form of profit, efficiency and increased productivity, although the opportunity for business losses is still possible (Irawan et al., 2022).

Along with the rapid progress of technology, when computers have begun to be known throughout the world, the world community is then threatened by cybercrime. According to an expert, cybercrime is a crime that occurs because it is connected to or located on a computer system that is connected to the Internet (Ngurah et al., 2023). Due to the rapid growth of digitalization in banks, cyber risks and attacks have grown to become a major area of concern (Naqvi et al., 2023). Over the past few decades, there has been a huge increase in cyber attacks, and these attacks cause a series of breakdowns in critical banking processes and cause huge financial losses to the system. It is very important for the banking or financial sector to implement an effective cyber security strategy (Dermawan et al., 2023).

Basically, authentication is a process where "a user identifies himself by sending x to the system; the system authenticates its identity by calculating F(x) and checking whether its value is the same as the stored value "y" (Bharadwaj et al., 2024). This definition has not changed significantly over time despite the fact that a simple password is no longer the only factor for validating a user from an information technology perspective (Ometov et al., 2018).

Adaptive Multi-Factor Authentication (A-MFA) is an enhanced version of MFA that provides a method for allowing authorized users to access systems using different factors that change based on different considerations (Kokila & Reddy K, 2024). In other words, authentication factors include passwords, biometrics among others are selected adaptively by the authentication system based on the criteria of whether the user is trying to log in from within the system boundaries, or whether the user is trying to access during the organization's operational hours. The criteria that trigger events for A-MFA to use to adaptively select authentication factors are usually predefined and encoded in the authentication system itself (Phan, 2018).

This article outlines the theoretical framework and security issues in educational settings. Where, there is a lack of awareness in utilizing the use as system security access. With recommendations for implementing MFA more effectively in educational institutions, the security system in accessing data can be further improved (Cahyaningrum, 2023b).

METHODS

This research using several steps approaches to gain a comprehensive understanding of the effectiveness and impact of implementing Multi-Factor Authentication on system access security in educational institutions. Following are the methodological steps adopted. Determine clear research objectives as a first step. This research aims to evaluate the extent to which can reduce security risks and improve system access security in educational institutions. Then study the literature by conducting an in-depth literature review about system security and MFA applications in educational environments. It includes a review of the successes and challenges associated with MFA implementation. Then choose educational institutions as research subjects by considering the diversity of size and complexity of their infrastructure. Next, design a survey that suits potential users, including students, lecturers, and administrative staff. Survey design by developing a questionnaire that includes questions related to users' understanding, perception and experience. Added questions regarding system access security before and after MFA implementation. Carrying out surveys by distributing questionnaires online to selected respondents while maintaining anonymity. Surveys involve structured, open-ended questions to gain in-depth insights.

Several MFA evaluation steps that can be implemented to ensure that the authentication system implemented is effective and meets the organization's security needs:

1. Security Objectives
   Determine of organization's security goals. It is implemented to protect access to sensitive data, critical systems, or user accounts? Evaluate the extent to which is can help achieve these security goals.
2. Conformity and Compliance
   Make sure its meets the suitability and compliance requirements applicable to your organization, such as GDPR, HIPAA, PCI DSS, and others.
3. Availability

Make sure it is easy for users to access and use. Evaluate whether the selected it is available across platforms and devices used by users.

4. Alignment with User Experience
   Review the extent to which user experience is impacted by MFA implementation. MFA should provide an additional layer of security without sacrificing convenience or hindering user productivity.
5. Authentication Factors
   Review the authentication factor combinations used in MFA. Ensure that the factors selected are strong enough to properly protect access, and consider the organization's specific needs regarding specific authentication factors.
6. Management and Monitoring
   Evaluate ability to effectively manage and monitoring. Make sure you can manage and regulate MFA usage, as well as monitor authentication activity to detect potential security threats.
7. Resistance to Attacks
   Review potential risks and threats to the selected. Make sure it has additional security mechanisms to protect against attacks such as phishing, social engineering, and other attacks.
8. Scalability
   Consider whether it can be easily expanded and improved to suit your organization's needs over time.
9. Cost and ROI
   Review implementation and operational costs, as well as expected security benefits. Make sure that the security benefits obtained are commensurate with the costs and investments incurred.

Monitoring system access by observing and analyzing system access activity log data before and after implementation. Review access patterns, unauthorized access attempts, and other potential security risks. Then conduct in-depth interviews with key stakeholders such as IT administrators and key users. Focus groups can also be used to gain a broader perspective. Analysis by integrating the results of quantitative and qualitative analysis to develop main findings and recommendations. Draw conclusions about the effectiveness of implementation and provide guidance for future improvements. This method allows research to gain a comprehensive picture of user experiences, security impacts, and challenges of implementing in educational institutions.

RESULT AND DISCUSSION

The use of MFA shows that the initial survey showed that the majority of respondents had a basic understanding of the MFA concept before implementation. However, there is a need to increase awareness of its benefits in improving access security. User perceptions of access security show survey results show a significant increase in user perceptions of system access security after implementing. Several of respondents reported feeling safer with the use of MFA. The impact on the level of access security with system access activity data analysis shows a significant reduction in unauthorized access attempts after implementation. For example, unauthorized login attempts decreased by 70%. Implementation challenges experienced Interviews with stakeholders identified several challenges, including the need for additional training for users, integration with existing systems, and management of MFA devices. These challenges must be overcome to maximize the effectiveness of. Recommendations given for the future as a result of the qualitative analysis, users put forward several recommendations, including the provision of regular training, improvements to the user interface for more intuitive use, and the use of more practical authentication methods. Based on the findings, educational institutions recommend that educational institutions need to intensify user training efforts, provide clear user guides, and consider integrating with other security solutions to achieve holistic security.

In a study, the implementation of in an educational institution as a whole had a positive impact on the security of system access. The significant improvement in user perception of security reflects the effectiveness of in providing additional security. The marked reduction in unauthorized login attempts is a clear indicator of ability to address unauthorized access attempts.

The following is a table of the questionnaire given to respondents. The questionnaire itself did not previously exist and I made it myself. The questionnaire can be shown in Table 1.

Table 1. Questionnaire Table

No.	Question	Answer
1.	Has MFA been implemented at this institution?	[] Yes [] No
2.	Explain the authentication factors used in MFA. Provide examples if possible!	
3.	How is the authentication process carried out in MFA?	
4.	Once the MFA process is successful, how is access to the system determined?	
5.	Are there any specific policies or rules regarding authorization after MFA?	[] Yes [] No
6.	Does access to the system correspond to user roles and responsibilities?	[] Yes [] No
7.	How are authentication keys stored and managed in an MFA system?	
8.	Are there any established procedures for dealing with lost or compromised keys?	[] Yes [] No
9.	Does MFA integrate well with other systems and applications at the institution?	[] Yes [] No
10.	Are there any integration obstacles that need to be overcome?	[] Yes [] No
11.	How is the MFA security update and upgrade process carried out?	
12.	Are there procedures in place to ensure MFA security is maintained over time?	[] Yes [] No
13.	Are you facing any particular obstacles or challenges regarding the implementation or use of MFA?	[] Yes [] No
14.	Do you have recommendations for improving system access security with MFA at this institution?	[] Yes [] No

This table is used as a guide for compiling a questionnaire for evaluating system access security with MFA in educational institutions. To tabulate the results of respondents from the Evaluation of System Access Security with Multi-Factor Authentication in Educational Institutions, they are presented in Table 2. Questionnaire Results along with Tabulation of Respondent Results.

Table 2. Questionnaire Results along with Tabulation of Respondent Results

No.	Question	Number of Respondents Saying "Yes"	Number of Respondents Saying "No"	Number of Respondents Did Not Answer
1.	Has MFA been implemented at this institution?	45	5	0
2.	Explain the authentication factors used in MFA?	N/A	N/A	N/A
3.	How is the authentication process carried out in MFA?	N/A	N/A	N/A
4.	Once the MFA process is successful, how is access to the system determined?	40	10	0
5.	Are there any specific policies or rules regarding authorization after MFA?	35	15	0
6.	Does access to the system correspond to user roles and responsibilities?	42	8	0
7.	How are authentication keys stored and managed in an MFA system?	N/A	N/A	N/A
8.	Are there any established procedures for dealing with lost or compromised keys?	38	12	0
9.	Does MFA integrate well with other systems and applications at the institution?	43	7	0
10.	Are there any integration obstacles that need to be overcome?	20	30	0
11.	How is the MFA security update and upgrade process carried out?	40	10	0

No.	Question	Number of Respondents Saying "Yes"	Number of Respondents Saying "No"	Number of Respondents Did Not Answer
12.	Are there procedures in place to ensure MFA security is maintained over time?	38	12	0
13.	Are you facing any particular obstacles or challenges regarding the implementation or use of MFA?	25	25	0
14.	Do you have recommendations for improving system access security with MFA at this institution?	45	5	0

Meanwhile, the table of research results evaluating system access security in the implementation of Multi-Factor Authentication (MFA) in educational institutions is shown in Table 3. Research Results.

Table 3. Research Results

No.	Evaluation Aspect	Score (1-5)	Information
1.	Identification	4	MFA uses a combination of strong authentication factors and verified user identity.
2.	Authorization	5	Access is only granted after successful MFA and in accordance with the user's roles and responsibilities.
3.	Authentication	4	MFA involves different authentication factors and strong authentication processes.
4.	Key Management	4	Authentication keys are stored and managed properly, with procedures to address lost or compromised keys.
5.	Security Event Reporting	3	MFA-related security incident reporting mechanisms exist, but improvements in incident response are needed.
6.	Integration	5	MFA integrates well with other systems and applications without any problems.
7.	Update	4	MFA security update and enhancement processes are implemented regularly.

A score of 1-5 is used to assess the quality of implementation, where a score of 1 indicates low performance and a score of 5 indicates high performance. This table provides an overview of the results of system access security evaluations with in educational institutions, including an assessment of the various security aspects evaluated.

To be able to help evaluate the extent to which the implementation of in educational institutions meets the required security standards, an analysis is needed. Any evaluation should be based on the specific needs and context of the educational institution. Analysis table Evaluation of system access security in the implementation of Multi-Factor Authentication is shown in Table 3. Evaluation of system access security.

Table 3. Evaluation of system access security

No.	Security Aspects	Evaluation
1.	Identification	a. Does MFA require strong dual identification? b. Are different combinations of authentication factors used? c. Is the user's identity verified effectively?
2.	Authorization	a. Is access only granted after successful MFA? b. Is limited access appropriate to roles and responsibilities?
3.	Authentication	a. Does MFA cover different authentication factors (e.g. something you know, something you have, something you are)? b. Does MFA involve a strong and secure authentication process?
4.	Key Management	a. How are authentication keys stored and managed? b. Are there procedures for managing lost or compromised keys?
5.	Security Event Reporting	a. Is there a mechanism for reporting MFA-related security events? b. Are there any defined actions to respond to security incidents involving MFA?

No.	Security Aspects	Evaluation
6.	Integration	a. Does MFA integrate with other systems and applications smoothly? b. Are there any integration obstacles that need to be overcome?
7.	Update	a. How are MFA security updates and improvements implemented? b. Is there a process to ensure MFA remains secure over time?

However, other research provides an overview of implementation challenges which are found to show the need for special preparation such as training. User training needs to be improved to ensure better understanding of usage, and integration with existing systems needs to be managed carefully to ensure operational effectiveness and efficiency.

Recommendations put forward by users and stakeholders are key to optimizing implementation. By paying attention to user feedback, educational institutions can improve system access security and better respond to user needs and expectations.

This article makes a concrete contribution to the understanding of the application in educational institutions and provides a basis for further research and continuous improvement in efforts to protect information and data in educational environments.

CONCLUSION

Based on the results and discussion, it can be concluded o Implementation of MFA significantly increases the level of system access security in educational institutions. Survey results show that most users report feeling more secure after using it, and analysis of access activity data supports this improvement with a significant reduction in unauthorized access attempts. Based on research findings, a number of recommendations have been proposed to increase the effectiveness of in educational institutions. This includes providing regular training, improving the user interface, and exploring more practical authentication methods. System integration demonstrates the importance of a holistic security approach. Further thinking about how it can be integrated with other security solutions to achieve more comprehensive protection is an important step.

REFERENCES

Badeges, W., & Fauzi, M. N. (2020). *Implementasi Multi Factor Authentication Pada Phpmyadmin*. 35–39.

Baldin, I., Chase, J., Crabtree, J., Nechyba, T., Christopherson, L., Stealey, M., Kneifel, C., Orlikowski, V., Carter, R., Scott, E., Sone, A., & Sizemore, D. (2022). ImPACT: A networked service architecture for safe sharing of restricted data. *Future Generation Computer Systems*, *129*, 269–285. https://doi.org/10.1016/j.future.2021.11.026

Bharadwaj, S., Amin, P., Ramya, D. J., & Parikh, S. (2024). Reliable human authentication using AI-based multibiometric image sensor fusion: Assessment of performance in information security. *Measurement: Sensors*, *33*(October 2023), 101140. https://doi.org/10.1016/j.measen.2024.101140

Buccafurri, F., De Angelis, V., Lazzaro, S., & Pugliese, A. (2024). Enforcing security policies on interacting authentication systems. *Computers and Security*, *140*(October 2023), 103771. https://doi.org/10.1016/j.cose.2024.103771

Cahyaningrum, Y. (2023a). Analisis Tata Kelola Arsitektur dan Perancangan Sistem Enterprise dalam Ekspedisi Barang Pada Perusahaan Logistik. *Jurnal Rekayasa Sistem Informasi Dan Teknologi (JRSIT)*, *1*(2), 118–122.

Cahyaningrum, Y. (2023b). Penerapan Artificial Intelligence Dalam Dunia Pendidikan. *Amplifier*, *13*(2), 62–68. https://stuvia.id/tips-belajar/artificial-intelligence-dalam-pendidikan/

Cahyaningrum, Y., Suryono, S., & Warsito, B. (2021). Fuzzy-Expert System for Indicator and Quality Evaluation of Teaching and Learning Processes Online Study Programs. *E3S Web of Conferences*, *317*, 05021. https://doi.org/10.1051/e3sconf/202131705021

Das, S., Wang, B., Tingle, Z., & Camp, L. J. (2019). *Evaluating User Perception of Multi-Factor Authentication: A Systematic Review*. http://arxiv.org/abs/1908.05901

Dermawan, I., Baidawi, A., Iksan, & Mellyana Dewi, S. (2023). Serangan Cyber dan Kesiapan Keamanan Cyber Terhadap Bank Indonesia. *Jurnal Informasi Dan Teknologi*, *5*(3), 20–25. https://doi.org/10.60083/jidt.v5i3.364

Fitrisia Munir, Irfan Nursetiawan, Yuniana Cahyaningrum, Hermi Oppier, S. S. (2023). Kebijakan Publik di Era Digital. In *CV. Karsa Cendekia*. http://www.nber.org/papers/w16019

Ibrahimy, M. M., Norta, A., & Normak, P. (2023). Blockchain-Based Governance Models Supporting Corruption-Transparency: A Systematic Literature Review. *Blockchain: Research and Applications*, 100186. https://doi.org/10.1016/j.bcra.2023.100186

Iftikhar, A., Qureshi, K. N., Shiraz, M., & Albahli, S. (2023). Security, trust and privacy risks, responses, and solutions for high-speed smart cities networks: A systematic literature review. *Journal of King Saud University - Computer and Information Sciences*, *35*(9), 101788. https://doi.org/10.1016/j.jksuci.2023.101788

Irawan, B., Sani, I., Febrian, W. D., Setiawan, Z., Abdullah, A., Aprizal, Wasil, M., Suseno, D. A. N., Rahayu, N., Soeharjoto, Umar, N., Chasanah, S., Bilgies, A. F., & Harinie, L. T. (2022). *Konsep Dasar E-Business*.

Kaiser, T., Siddiqua, R., Hasan, M., & Uddin, M. (2022). *A multi-layer security system for data access control, authentication, and authorization. May*.

Kokila, M., & Reddy K, S. (2024). Authentication, Access Control and Scalability models in Internet of Things Security - A Review. *Cyber Security and Applications*, *3*(March 2024), 100057. https://doi.org/10.1016/j.csa.2024.100057

Komalasari, R. (2018). KESADARAN AKAN KEAMANAN PENGGUNAAN USERNAME DAN PASSWORD. *TEMATIK - Jurnal Teknologi Informasi Dan Komunikasi*, *5*(2), 141–152.

Mishra, R. A., Kalla, A., Braeken, A., & Liyanage, M. (2021). Privacy Protected Blockchain Based Architecture and Implementation for Sharing of Students' Credentials. *Information Processing and Management*, *58*(3), 102512. https://doi.org/10.1016/j.ipm.2021.102512

Nanda, A., Jeong, J. J., Shah, S. W. A., Nosouhi, M., & Doss, R. (2024). Examining usable security features and user perceptions of Physical Authentication Devices. *Computers and Security*, *139*(December 2023), 103664. https://doi.org/10.1016/j.cose.2023.103664

Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., & Porras, J. (2023). Mitigation strategies against the phishing attacks: A systematic literature review. *Computers and Security*, *132*, 103387. https://doi.org/10.1016/j.cose.2023.103387

Ngurah, I. G., Derrick, D., & Satrio, N. (2023). *Analisa Tindak Pidana Cyber Crime Pada Bidang Perbankan Nasional Berupa Pencurian Data Kartu Kredit (Carding)*. 1–12.

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography*, *2*(1), 1–31. https://doi.org/10.3390/cryptography2010001

Phan, K. (2018). *Implementing Resiliency of Adaptive Multi-Factor Authentication Systems*. *65*, 1–96. https://repository.stcloudstate.edu/msia_etdshttps://repository.stcloudstate.edu/msia_etds/65

Ray, P. P. (2023). Web3: A comprehensive review on background, technologies, applications, zero-trust architectures, challenges and future directions. *Internet of Things and Cyber-Physical Systems*, *3*(May), 213–248. https://doi.org/10.1016/j.iotcps.2023.05.003

Tripathi, G., Ahad, M. A., & Casalino, G. (2023). A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges. *Decision Analytics Journal*, *9*(March), 100344. https://doi.org/10.1016/j.dajour.2023.100344

Tyagi, A. K., & Sreenath, N. (2021). Cyber Physical Systems: Analyses, challenges and possible solutions. *Internet of Things and Cyber-Physical Systems*, *1*(July), 22–33. https://doi.org/10.1016/j.iotcps.2021.12.002

Vekariya, V., Joshi, M., Dikshit, S., & Manju bargavi, S. K. (2024). Multi-biometric fusion for enhanced human authentication in information security. *Measurement: Sensors*, *31*(December 2023), 100973. https://doi.org/10.1016/j.measen.2023.100973

Yuniana Cahyaningrum, Yulifda Elin Yuspita, Diana, Asrul Sani, Yudo Devianto, Ragel Trisudarmo, I Kadek Arya Sugianta, Heru Budianto, Noni Rahmawati, Meidar Hadi Avizenna, Novi Aryani Fitri, Darmawan Aditama, Miftahul Jannah, Y. A. E. (2023). *Arsitektur dan Organisasi Komputer* (M. M. Artika Arsita, S.Kom. (ed.); 1st ed.). PT Penamuda Media.