JOURNAL OF EDUCATIONAL RESEARCH AND COMMUNITY SERVICE (JERCS)
VOLUME 01 SPECIAL ISSUE MEI 2025 | | ISSN 3089-5561

A CYBERSECURITY FRAMEWORK FOR ACADEMIC INFORMATION SYSTEMS IN HIGHER EDUCATION

Syawal Kurnia Putra[1*], Baso Marannu[2]
[1]Universitas Islam Negeri Alauddin Makassar, Indonesia
[2]Peneliti Badan Riset Inovasi Nasional, Indonesia

*Email korepondesi: syawalp1@gmail.com

Abstrak

Transformasi digital di perguruan tinggi menempatkan sistem informasi akademik sebagai komponen penting dalam pelaksanaan layanan pendidikan. Namun, meningkatnya ancaman siber terhadap data akademik mengungkapkan kelemahan serius dalam tata kelola keamanan informasi. Penelitian ini bertujuan untuk merancang kerangka kerja keamanan siber yang sesuai dengan karakteristik dan kebutuhan perguruan tinggi, berdasarkan pendekatan kualitatif. Data tersebut diperoleh melalui wawancara mendalam dengan manajer TI, dosen, dan pakar keamanan siber dari tiga universitas di Indonesia. Temuan menunjukkan bahwa ketidaksiapan kelembagaan dalam hal kebijakan, budaya keamanan, dan kontrol teknis adalah penyebab utama kerentanan yang tinggi. Hasil ini diperkuat oleh penelitian sebelumnya yang menunjukkan pentingnya integrasi antara aspek teknis dan non-teknis dalam keamanan informasi pendidikan. Penelitian ini menawarkan kerangka kerja keamanan siber berbasis konteks lokal yang relevan untuk diterapkan di perguruan tinggi.
Kata kunci: Keamanan siber, sistem informasi akademik, pendidikan tinggi, kerangka kerja

Abstract (bahasa inggris)

Digital transformation in higher education places academic information systems as a crucial component in the implementation of educational services. However, the increasing cyber threats to academic data reveal serious weaknesses in information security governance. This research aims to design a cybersecurity framework that is in accordance with the characteristics and needs of higher education institutions, based on a qualitative approach. The data was obtained through in-depth interviews with IT managers, lecturers, and cybersecurity experts from three universities in Indonesia. The findings show that institutional unpreparedness in terms of policies, security culture, and technical controls is the main cause of high vulnerability. These results are reinforced by previous studies that show the importance of integration between technical and non-technical aspects in educational information security. This research offers a relevant local context-based cybersecurity framework to be implemented in colleges.
Keyword: Cybersecurity, academic information systems, higher education, framework

Artikel Info:
Submit : Mei-2025
Revisi : Mei-2025
Terima : Mei-2025
Cite : Putra & Marannu. (2025). A CYBERSECURITY FRAMEWORK FOR ACADEMIC INFORMATION SYSTEMS IN HIGHER EDUCATION. *Journal of Educational Research and Community Service.* 1(Special Issue, Mei 2025). 210-217.

PENDAHULUAN

In the past decade, colleges have extensively implemented academic information systems to improve the efficiency of academic administration and services (Mohammed et al., 2024) (Salih et al., 2025) (Mehrolia et al., 2021). However, the use of this technology also opens a gap against cybersecurity threats, such as hacking, falsification of grades, and theft of students' personal data (Alhadidi et al., 2024).

Alsmadi & Zarour (2015) noted that more than 60% of universities in developing countries do not have adequate information security policies (Akpabio et al., 2025) (Chapagain et al., 2022) (Kavak, 2024). In Indonesia, the increase in data leak cases in the campus environment reflects the weak readiness of institutions to deal with digital risks, which includes technical (Deja et al., 2021), governance (Saadé et al., 2025), and cybersecurity literacy aspects (Mulahuwaish et al., 2025).

Based on these conditions, this study aims to formulate a cybersecurity framework through a qualitative approach that explores the empirical reality and specific context of academic information systems in Indonesian universities. This research aims to identify the main challenges faced by universities in maintaining the security of academic information systems in the digital era. With a qualitative approach, this study delves in depth into the actual conditions in several higher education institutions in Indonesia related to policies, technical infrastructure, user awareness, and cybersecurity governance. The goal is to understand the main causes of information system vulnerabilities that are often overlooked, especially in the context of institutions with limited resources and the absence of integrated security standards.

METODE

This study uses a qualitative-descriptive (Karimi-Ghartemani et al., 2022) approach with a case study method (Liu et al., 2025) to explore cybersecurity challenges in academic information systems in higher education. This approach allows researchers to dig deeply into the actual conditions that occur in the field, especially in the context of higher education institutions in Indonesia, as well as to look at the role of various factors such as policies, technical infrastructure, and organizational culture.

The data was collected through in-depth interviews (Rocha-Jiménez et al., 2025) with 9 informants consisting of IT managers, lecturers, and cybersecurity experts from three universities in Indonesia. In addition, security policy documentation, incident reports, and operational procedures are also obtained to provide a comprehensive overview of the implementation of security on campus. Limited observations were also carried out to monitor the implementation of security policies in the field.

Data analysis uses the Miles and Huberman model which includes data reduction, data presentation, and conclusion drawn (Emezue et al., 2021). The reduction stage is carried out by grouping relevant data to identify key themes related to cybersecurity. The filtered data is then presented systematically and analyzed to draw conclusions relevant to existing theories as well as previous research. With this method, the research aims to provide an in-depth overview of the challenges and solutions that can be applied to improve cybersecurity in academic information systems in universities.

HASIL DAN PEMBAHASAN

The study reveals that the primary factor contributing to weak academic information system security in Indonesian universities is the absence of a formal and integrated cybersecurity policy. Most higher education institutions lack comprehensive policy documents that clearly outline security standards, procedures, and data protection protocols. Existing policies tend to be fragmented and fail to adequately address both technical and non-technical aspects, such as user behavior guidelines, incident response procedures, and risk management frameworks. This lack of clarity leads to inconsistent implementation of data security measures, rendering systems highly vulnerable to breaches.

Another significant issue identified is the low level of cybersecurity awareness and understanding among lecturers and administrative staff. Many system users are unfamiliar with basic cybersecurity threats such as phishing attacks, malware infections, or the risks of weak password practices. This situation is exacerbated by the lack of regular training or awareness programs that emphasize safe digital practices. The absence of a strong digital security culture results in behavioral vulnerabilities that cybercriminals can easily exploit.

In addition to policy and awareness issues, the limited availability of technical resources poses a serious challenge to effective information security management. Many Indonesian universities, particularly smaller institutions, do not have sufficient budgets to invest in advanced security technologies such as next-generation firewalls, intrusion detection systems (IDS), or high-level encryption tools. Furthermore, the shortage of qualified cybersecurity professionals within these institutions limits their ability to proactively respond to threats and maintain secure systems. Consequently, academic information systems often operate with outdated or insufficient security mechanisms.

The fourth issue relates to the lack of robust monitoring and auditing systems. Without continuous monitoring mechanisms that enable early threat detection, institutions struggle to identify and respond to attacks in a timely manner. This increases the risk of data breaches and unauthorized access incidents that can go unnoticed until significant damage has occurred. Moreover, the absence of structured security audits prevents institutions from regularly evaluating and improving their existing security infrastructure, thereby hindering long-term resilience against cyber threats.

Lastly, many universities heavily depend on third-party vendors to manage their IT infrastructure without implementing adequate oversight mechanisms. This reliance is often driven by internal limitations in expertise and resources. However, without contracts that enforce strict cybersecurity standards or clear monitoring procedures, outsourcing can inadvertently increase security risks. External vendors often have access to critical institutional data and systems, making them potential entry points for external attacks, especially when their security practices are not closely monitored or regulated.

Based on the findings of this study, a Cybersecurity Framework for Higher Education (CFHE) is designed to provide comprehensive solutions to cybersecurity problems faced by universities (Parambil et al., 2024) (Ragab et al., 2025) (Hossain et al., 2025). The framework consists of five main components, namely policy and governance (Edelenbos et al., 2025), risk management (Yuan et al., 2025), technical controls (Dağlı et al., 2025), security culture and education (Ekren et al., 2025), and monitoring and auditing (Takaoka et al., 2022). These components are chosen to cover both technical and non-technical aspects, which are often overlooked in cybersecurity approaches in educational institutions. Through this approach, it is hoped that all elements that play a role in information security management can collaborate to build a more secure and integrated system.

The first component in this framework is policy and governance. Clear and structured policies are the main foundation to ensure that all aspects of cybersecurity can be carried out consistently and coordinated. Without a standardized policy, information security management tends to be unorganized and there is no clarity in the responsibilities and procedures that must be followed by system users. This is in line with research by Alotaibi et al., which emphasizes that the success of security policies in universities is highly dependent on the commitment of management and the involvement of all stakeholders, from leadership to academic staff (Alotaibi et al., 2025).

The second component, risk management, focuses on identifying, assessing, and managing risks that can threaten the sustainability of academic information systems. Universities must be able to evaluate potential cyber threats that can damage the integrity of their data and operations. This process involves an analysis of their vulnerabilities, an assessment of possible impacts, and the development of appropriate mitigation strategies. As stated by Alsmadi & Zarour, a systematic risk management approach will assist institutions in reducing exposure to cyber threats that can lead to financial and reputational losses (Moussa et al., 2025).

The third aspect is technical control, which includes various technological solutions to protect information systems from external as well as internal threats. This involves implementing firewall systems, data encryption, role-based access control, and incident detection and response. The right technology can strengthen the system's defenses, but only with the right policy and education support, will these technical controls be effective. Research by Ifinedo shows that good management of technical controls, such as setting a strong password use policy, is essential to prevent data leaks and unauthorized access (Atzori et al., 2024).

Fourth, security culture and education are equally important aspects in increasing awareness and active participation of all system users in maintaining information security. While technology and policies are indispensable, in the absence of a supportive organizational culture and high awareness among users, vulnerabilities remain high. As discovered by Nur Fauzana et al., implementation failures are often caused by user negligence or ignorance in following security procedures (Fouzi et al., 2024). Therefore, the integration between security policies and ongoing training programs can help create a strong safety culture at every college level.

Finally, monitoring and auditing are essential components to ensure that the system that has been built runs effectively and meets the set standards. A regular monitoring process and thorough audits can quickly detect and respond to security threats or breaches. With audits, universities can evaluate the performance of security systems and make necessary improvements. This is in line with the findings of Dennis Brown, who stated that continuous

monitoring and auditing is an important part of ensuring that the policies and controls that have been put in place can function as they should in reducing cyber risk in the organisational environment (Brown et al., 2024). Overall, the CFHE framework designed in this study reinforces the findings of previous studies, which suggest that the successful implementation of cybersecurity systems in universities depends not only on technology alone, but also on the presence of clear policies and a supportive organizational culture. As such, the framework suggests a comprehensive and collaboration-based approach between technical and non-technical aspects. Integrating policies, user education, and technical controls is key in creating an effective and sustainable cybersecurity system in college.

SIMPULAN

This study concludes that the vulnerability of academic information systems in Indonesian universities is structural, stemming from the lack of security policies, low user awareness, and inadequate technical infrastructure. The Cybersecurity Framework for Higher Education (CFHE) developed in this study offers a strategic solution tailored to local contexts, focusing on five key aspects: policy, risk management, technical controls, user education, and system monitoring. It is recommended that universities adopt this framework to enhance their digital resilience, with the understanding that it should be customized to fit the scale, resources, and governance structure of each institution.

DAFTAR PUSTAKA

Akpabio, E. S., Akeju, K. F., & Omotoso, K. O. (2025). E-agriculture and food security in developing countries: beaming the searchlight on Nigeria. *Smart Agricultural Technology*, *10*, 100689. https://doi.org/https://doi.org/10.1016/j.atech.2024.100689

Alhadidi, I., Nweiran, A., & Hilal, G. (2024). The influence of Cybercrime and legal awareness on the behavior of university of Jordan students. *Heliyon*, *10*(12), e32371. https://doi.org/https://doi.org/10.1016/j.heliyon.2024.e32371

Alotaibi, B. A., Abbas, A., Azeem, M. I., Shahbaz, P., ul Haq, S., & Nayak, R. K. (2025). Role of risk perception and climate change beliefs in adoption of climate-resilient agricultural practices in Saudi Arabia. *Climate Services*, *38*, 100552. https://doi.org/https://doi.org/10.1016/j.cliser.2025.100552

Alsmadi, I., & Zarour, M. (2015). Building an Islamic financial information system based on policy managements. *Journal of King Saud University - Computer and Information Sciences*, *27*(4), 364–375. https://doi.org/https://doi.org/10.1016/j.jksuci.2014.11.001

Atzori, M., Calò, E., Caruccio, L., Cirillo, S., Polese, G., & Solimando, G. (2024). Evaluating password strength based on information spread on social networks: A combined approach relying on data reconstruction and generative models. *Online Social Networks and Media*, *42*, 100278. https://doi.org/https://doi.org/10.1016/j.osnem.2024.100278

Brown, D., Batra, G., Zafar, H., & Saeed, K. (2024). Reducing fraud in organizations through information security policy compliance: An information security controls perspective. *Computers & Security*, *144*, 103958. https://doi.org/https://doi.org/10.1016/j.cose.2024.103958

Chapagain, K., Aboelnga, H. T., Babel, M. S., Ribbe, L., Shinde, V. R., Sharma, D., & Dang, N. M. (2022). Urban water security: A comparative assessment and policy analysis of five

cities in diverse developing countries of Asia. *Environmental Development*, *43*, 100713. https://doi.org/https://doi.org/10.1016/j.envdev.2022.100713

Dağlı, E., Reyhan, F. A., & Kırca, A. Ş. (2025). Effectiveness of training for student midwives with jigsaw technique on respectful maternity care: A randomized controlled experimental study. *Nurse Education in Practice*, *85*, 104381. https://doi.org/https://doi.org/10.1016/j.nepr.2025.104381

Deja, M., Rak, D., & Bell, B. (2021). Digital transformation readiness: perspectives on academia and library outcomes in information literacy. *The Journal of Academic Librarianship*, *47*(5), 102403. https://doi.org/https://doi.org/10.1016/j.acalib.2021.102403

Edelenbos, J., van Popering-Verkerk, J., Taanman, M., & Stouten, M. (2025). Multilevel governance in times of COVID-19 pandemic. Patterns of legitimacy and governance capacity. *Urban Governance*, *5*(1), 94–102. https://doi.org/https://doi.org/10.1016/j.ugj.2025.02.001

Ekren, E., Hall, R. E., Pierdolla, E., Barnes, V., Jarzombek-Torralva, A., Morrish, D., & Martinez-Prather, K. (2025). Crime prevention through environmental design in public school career and technical education facilities: Principals' perceptions of security enhancement. *Safety Science*, *185*, 106781. https://doi.org/https://doi.org/10.1016/j.ssci.2025.106781

Emezue, C. N., Enriquez, M., Dougherty, D. S., Bullock, L. F. C., & Bloom, T. L. (2021). Rural young males' acceptance & receptiveness to technology-based interventions for dating violence prevention: A qualitative descriptive study. *Journal of Adolescence*, *92*, 137–151. https://doi.org/https://doi.org/10.1016/j.adolescence.2021.08.012

Fouzi, N. F. R., Aziz, H. A., & Yaakub, N. (2024). Systematic review of chemical safety and chemical security risk management approach. *Process Safety and Environmental Protection*, *183*, 676–686. https://doi.org/https://doi.org/10.1016/j.psep.2024.01.035

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2025). Cybersecurity in local governments: A systematic review and framework of key challenges. *Urban Governance*, *5*(1), 1–19. https://doi.org/https://doi.org/10.1016/j.ugj.2024.12.010

Karimi-Ghartemani, S., Khani, N., & Nasr Isfahani, A. (2022). A qualitative analysis and a conceptual model for organizational stupidity. *Journal of Organizational Change Management*, *35*(3), 441–462. https://doi.org/https://doi.org/10.1108/JOCM-04-2021-0099

Kavak, A. (2024). Impact of information security awareness on information security compliance of academic library staff in Türkiye. *The Journal of Academic Librarianship*, *50*(5), 102937. https://doi.org/https://doi.org/10.1016/j.acalib.2024.102937

Liu, H., Guo, S., Liu, C., Du, F., Li, B., & Hong, J. (2025). Case study of natural convection topology optimization based on finite volume method. *Case Studies in Thermal Engineering*, *66*, 105697. https://doi.org/https://doi.org/10.1016/j.csite.2024.105697

Mehrolia, S., Alagarsamy, S., & Indhu Sabari, M. (2021). Moderating effects of academic involvement in web-based learning management system success: A multigroup analysis. *Heliyon*, *7*(5), e07000. https://doi.org/https://doi.org/10.1016/j.heliyon.2021.e07000

Mohammed, A. B., Maqableh, M., Qasim, D., & AlJawazneh, F. (2024). Exploring the factors influencing academic learning performance using online learning systems. *Heliyon*, *10*(11), e32584. https://doi.org/https://doi.org/10.1016/j.heliyon.2024.e32584

Moussa, L. G., Mohan, M., Pitumpe Arachchige, P. S., Rathnasekara, H., Abdullah, M., Jaffar, A., Montenegro, J. F., Kale, A., Heng, J., King, ShaliniA. L., Daneil, R., Al-Awadhi, T., El Kenawy, A., & Abulibdeh, A. (2025). Impact of water availability on food security in GCC: Systematic literature review-based policy recommendations for a sustainable future. *Environmental Development*, *54*, 101122. https://doi.org/https://doi.org/10.1016/j.envdev.2024.101122

Mulahuwaish, A., Qolomany, B., Gyorick, K., Abdo, J. B., Aledhari, M., Qadir, J., Carley, K., & Al-Fuqaha, A. (2025). A survey of social cybersecurity: Techniques for attack detection, evaluations, challenges, and future prospects. *Computers in Human Behavior Reports*, *18*, 100668. https://doi.org/https://doi.org/10.1016/j.chbr.2025.100668

Parambil, M. M. A., Rustamov, J., Ahmed, S. G., Rustamov, Z., Awad, A. I., Zaki, N., & Alnajjar, F. (2024). Integrating AI-based and conventional cybersecurity measures into online higher education settings: Challenges, opportunities, and prospects. *Computers and Education: Artificial Intelligence*, *7*, 100327. https://doi.org/https://doi.org/10.1016/j.caeai.2024.100327

Ragab, M., Alghamdi, B. M., Alakhtar, R., Alsobhi, H., Maghrabi, L. A., Alghamdi, G., Nooh, S., & AL-Ghamdi, A. A.-M. (2025). Enhancing cybersecurity in higher education institutions using optimal deep learning-based biometric verification. *Alexandria Engineering Journal*, *117*, 340–351. https://doi.org/https://doi.org/10.1016/j.aej.2025.01.012

Rocha-Jiménez, T., Torres, I., Cabieses, B., López-Cevallos, D. F., & Mercado-Órdenes, M. (2025). Intersectionality, racism, and mental health of migrants arriving at borders in Latin America: a qualitative study based on in-depth interviews with key informants of the cases of Ecuador and Chile. *The Lancet Regional Health - Americas*, *44*, 101040. https://doi.org/https://doi.org/10.1016/j.lana.2025.101040

Saadé, R. G., Hao, L., & Kuusiholma, T. (2025). Global governance & aerospace – The need for a management-integrated air and space education paradigm. *Journal of Space Safety Engineering*. https://doi.org/https://doi.org/10.1016/j.jsse.2025.04.003

Salih, S., Husain, O., Hamdan, M., Abdelsalam, S., Elshafie, H., & Motwakel, A. (2025). Transforming education with AI: A systematic review of ChatGPT's role in learning, academic practices, and institutional adoption. *Results in Engineering*, *25*, 103837. https://doi.org/https://doi.org/10.1016/j.rineng.2024.103837

Takaoka, A., Zytaruk, N., Davis, M., Matte, A., Johnstone, J., Lauzier, F., Marshall, J., Adhikari, N., Clarke, F. J., Rochwerg, B., Lamontagne, F., Hand, L., Watpool, I., Porteous, R. K., Masse, M.-H., D'Aragon, F., Niven, D., Heels-Ansdell, D., Duan, E., … Cook, D. J. (2022). Monitoring and auditing protocol adherence, data integrity and ethical conduct of a randomized clinical trial: A case study. *Journal of Critical Care*, *71*, 154094. https://doi.org/https://doi.org/10.1016/j.jcrc.2022.154094

Yuan, S., Reniers, G., & Yang, M. (2025). Dynamic and integrated safety and security barrier management: A new framework to manage major event risks in chemical plants. *Journal of Loss Prevention in the Process Industries*, *96*, 105632. https://doi.org/https://doi.org/10.1016/j.jlp.2025.105632