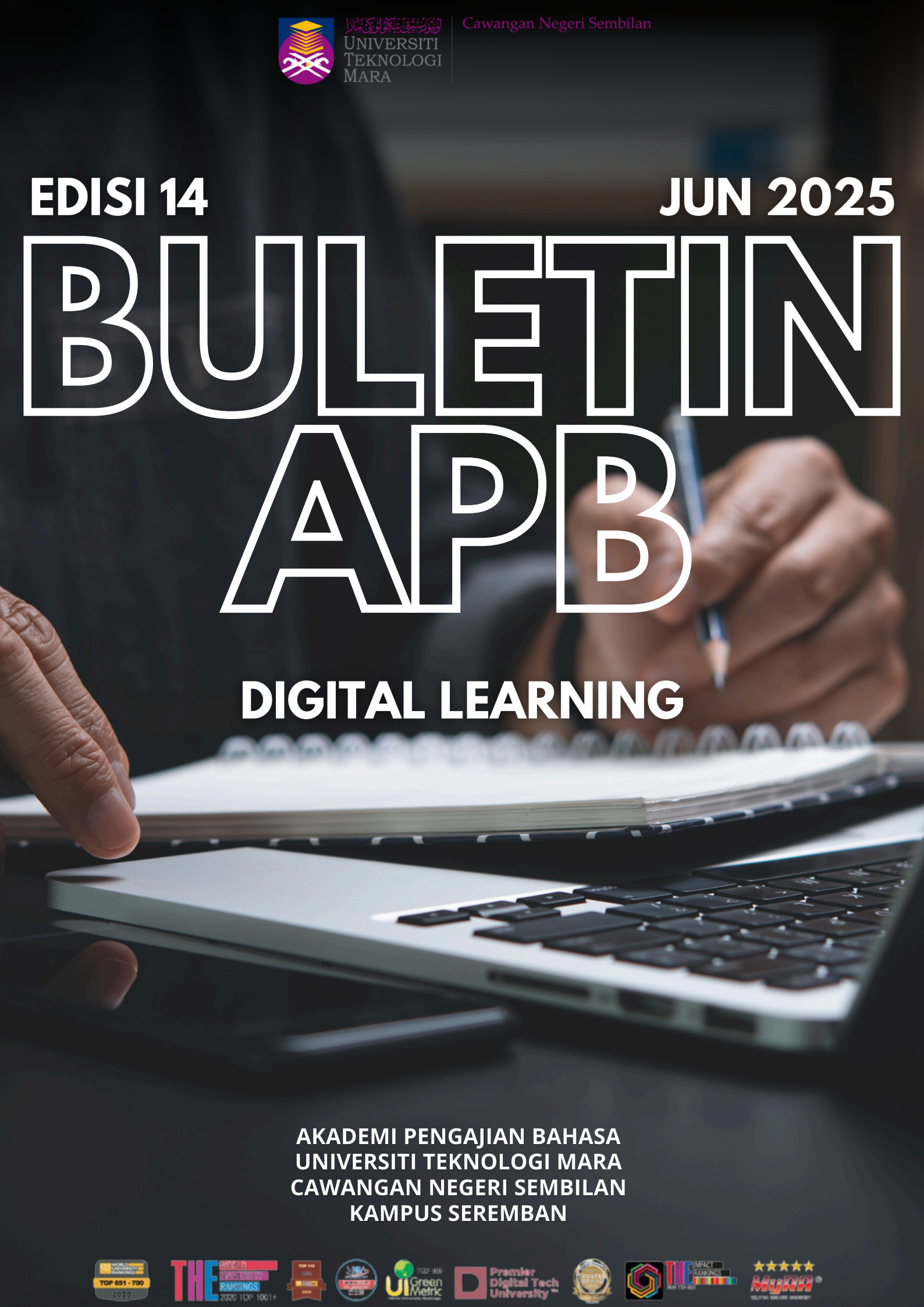
UNIVERSITI TEKNOLOGI MARA
Cawangan Negeri Sembilan

EDISI 14

JUN 2025

BULETIN APB

DIGITAL LEARNING



AKADEMI PENGAJIAN BAHASA
UNIVERSITI TEKNOLOGI MARA
CAWANGAN NEGERI SEMBILAN
KAMPUS SEREMBAN

Securing e-Learning: Challenges and Solutions for Cybersecurity in Higher Education

NORASHIKIN BINTI MOKHTAR, MOHD FAIZ ISMAIL, NIK MAHFUZAH NIK MAT & DR IRMA BINTI AHMAD
UiTM CAWANGAN NEGERI SEMBILAN KAMPUS SEREMBAN

The digital revolution has profoundly impacted education by enabling flexible, personalised, and convenient learning through e-learning platforms. However, this transformation has also led to a significant rise in cybersecurity threats, which higher education institutions must urgently address (Sadiqzade & Alisoy, 2025).

Advancements in technology have enabled learning materials to transition from physical classrooms to online spaces, opening access and facilitating collaborative engagement among universities. However, such a shift also carries substantial operational risks. While students and teachers begin to use more digital tools, they are also exposing themselves to threats, including hacking, phishing, ransomware, and unauthorised access.

The COVID-19 pandemic has led to significant growth in online education. The abrupt and unplanned transition to distance learning posed unique challenges for both educators and students, who had to quickly adapt to unfamiliar digital environments (Al-Hunaiyyan et al., 2021). However, this shift also exposed a widespread lack of preparedness across many universities and colleges. Poor digital infrastructure and limited technical competency among faculty and students contributed to inconsistent and unequal learning experiences. Furthermore, the expanded digital footprint resulting from widespread remote access to educational resources increased the vulnerability to cybersecurity threats, including data breaches (Yaseen, 2022).

Numerous factors contribute to the rise in cybersecurity threats within the e-learning sector. First, the immediate shift to virtual learning left many institutions racing to implement digital architectures with little time for comprehensive security planning. This rush to adopt often meant the use of insecure platforms, outdated software, and poorly configured systems that were vulnerable to exploitation. Second, the heavy reliance on personal devices to access learning content raises security concerns due to their inadequate protection and the common practice of sharing these devices among family members. Third, the increasing placement of sensitive data on cloud-based platforms introduces additional threats of cyber attack if access controls and encryption mechanisms are inadequate.

Lastly, cybercriminals are becoming increasingly sophisticated, employing a practical social engineering approach that utilises methods such as phishing and impersonation as they target an underinformed user base of students and staff. These dangers have been exacerbated by the absence of a comprehensive, integrated approach across an entire system of cybersecurity within institutions (Buja, 2021), resulting in increased challenges in responding to threats. These threats can only be addressed on multiple fronts. Organisations should consider investing in robust authentication systems, such as multi-factor authentication, to protect against unauthorised access. It is vital to achieve real-time monitoring with the help of IDS and IPS systems. The encryption of data during transmission and at rest can provide secure communication, and incident response plans can limit the damage caused by violations (Rjaibi et al., 2013). Similarly, the educational aspect of cybersecurity studies is also essential (Hasan et al., 2024).

To summarise, ongoing education for students, faculty, and staff on recognising phishing scams, managing credentials, and following protocols is vital. An informed academic community functions as one of the most effective safeguards against cyber threats. Thus, ensuring the security of e-learning environments is a collective concern. By leveraging technology, effective policy, and user education, institutions can create robust digital learning environments that are secure, inclusive, and future-ready.

References

Al-Hunaiyyan, A., Al-Sharhan, S., Alhajri, R., & Alhudaib, A. (2021). E-learning during the COVID-19 pandemic: Experiences and perceptions of Kuwait's higher education faculty. *Education and Information Technologies, 26*(6), 6995–7015. https://doi.org/10.1007/s10639-021-10530-0

Buja, A. G. (2021). Cyber security features for national e-learning policy. *Turkish Journal of Computer and Mathematics Education, 12*(5), 1729–1735. https://doi.org/10.17762/TURCOMAT.V12I5.2169

Hasan, S. A., AlJazeeri, F. H., Abdulla, H. H., AlMahafdha, Z. S., & AlAmmary, J. (2024). *A systematic literature review of models and factors influencing e-learning cybersecurity awareness among university students.* 2024 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), 405–412. https://doi.org/10.1109/3ict64318.2024.10824546

Rjaibi, N., Rabai, L. B. A., Aissa, A. B., & Mili, A. (2013). Mean failure cost as a measurable value and evidence of cybersecurity: E-learning case study. *International Journal of Secure Software Engineering, 4*(3), 64–81. https://doi.org/10.4018/jsse.2013070104

Sadiqzade, Z., & Alisoy, H. (2025). Cybersecurity and online education – risks and solutions. *Luminis Applied Science and Engineering*. https://doi.org/10.69760/lumin.20250001001

Yaseen, K. A. Y. (2022). Digital education: The cybersecurity challenges in the online classroom (2019–2020). *Asian Journal of Computer Science and Technology*. https://doi.org/10.51983/ajcst-2022.11.2.3450