Modeling and Constructing a Network Security System for Colleges and Universities in the Context of Digital Transformation

Zhong Huang

[1] Shanghai Publishing and Printing College

[a] huangzhong1109@163.com

Abstract. In recent years, with the rapid development of a new generation of digital technology, especially in the context of digital transformation faced by colleges and universities, cloud computing, big data, the Internet of Things mobile Internet and other technologies effectively promote the development of higher education to the development of intelligent education, and the digital campus of colleges and universities is facing the digital transformation and upgrading. New technologies bring many benefits to the construction of digital campuses in colleges and universities, but also bring new network security risks. Colleges and universities are faced with network openness without borders, zero trust in security authentication, asymmetric attack and defence confrontation, and ever-changing network information security problems. In the context of digital transformation, how colleges and universities can cope with the network security problems brought by new technologies and how to effectively construct network security defences is the work that colleges and universities must pay attention to and move forward. This paper first discusses the background and significance of the digital transformation of colleges and universities, the network security challenges and real needs faced in the transformation process, and finally puts forward the network security system construction ideas for the existing problems, aiming to improve the level of network security protection in the process of constructing smart campuses in colleges and universities.

Keywords: digital transformation; network security; information system; security system.

1. Introduction

In an era marked by the rapid advancement of technology, the landscape of higher education is undergoing a transformative change. Colleges and universities around the globe are increasingly incorporating emerging technologies such as cloud computing, big data, Internet of Things (IoT), and mobile Internet in the construction of a more integrated and efficient digital campus. These technologies are not merely add-ons to the educational experience; they are becoming fundamental components that redefine the way education is delivered and received. These technologies have brought unprecedented convenience to both teachers and students[1]. Cloud computing enables seamless access to educational resources and collaborative tools, freeing both faculty and students from the constraints of physical location and traditional class schedules. Big data analytics are providing insights into student learning behaviors and institutional operations, empowering educators to tailor teaching strategies to individual student needs and administrators to make data-driven decisions. IoT technologies are making campuses smarter and more sustainable through energy management and security surveillance systems. These innovations not only contribute to a safer and more efficient environment but also promote sustainability by allowing institutions to monitor and reduce their energy usage effectively. Mobile Internet is empowering learning without geographic boundaries, turning the world into a potential classroom. This evolution allows for the development of flexible and diverse learning pathways, where students can engage in synchronous or asynchronous learning modes, participate in virtual global exchanges, and access a wealth of knowledge beyond traditional textbooks.Moreover, these technological advancements are challenging the traditional roles and skills required of educators. Faculty now must become proficient not just in their subject matter, but also in the technology tools they employ. This involves learning to navigate new software platforms, understanding data privacy issues, and adapting pedagogical strategies to effectively engage students in a digital environment. Yet, while these developments are largely positive, they also introduce significant security and privacy concerns. With increased data collection comes the risk of breaches and unauthorized use of sensitive information. The integration of various technologies across campus operations makes universities more susceptible to cyber-attacks, requiring robust and continually updated security protocols.

As higher education institutions continue to deeply integrate emerging technologies into their core operations and educational delivery methods, they are both enhancing and complicating the academic landscape. These technologies, including cloud computing, big data, IoT, and mobile Internet, are revolutionizing the educational experience, providing unprecedented flexibility, personalization, and global reach. However, with these benefits come significant challenges, most notably in terms of cybersecurity and data privacy. As such, it is imperative for colleges and universities to approach this digital transformation with a balanced and thoughtful strategy, embracing the opportunities for enhanced learning and efficiency while vigilantly safeguarding the security and privacy of their digital ecosystems[2].

However, alongside these remarkable benefits come significant and evolving security risks. Cybersecurity incidents, including hacking, webpage tampering, and phishing emails, have surged in recent years, posing a threat to the integrity and confidentiality of sensitive information and intellectual property stored in university networks. These incidents, which are becoming increasingly sophisticated and frequent, threaten not only the quality but also the very process of digital transformation, and may undermine trust in digital platforms among students, faculty, and staff. In acknowledgment of the centrality of digital transformation in modern education, various authoritative bodies, such as the Ministry of Education in many countries, have enacted plans and action strategies. These policies are designed to provide a roadmap for the digital transformation of higher education institutions and emphasize the necessity of robust cybersecurity measures as a core component of this transformation. These directives highlight the importance of developing targeted, adaptable security strategies that are capable of addressing an ever-changing landscape of cyber threats. In response, colleges and universities must cultivate a culture of security awareness among staff and students alike, regularly updating training programs and conducting security drills to reinforce best practices. This extends to allocating resources effectively, fostering expertise in cybersecurity within the institution, and perhaps even collaborating with external security agencies and experts for timely advice and intervention.

The digital transformation of higher education institutions is not merely a reaction to technological progress. It represents a fundamental paradigm shift, a need to adapt to the realities of the digital era. It is not only a path towards enhanced efficiency and modernization of educational practices but is increasingly seen as a critical step towards the broader modernization and development of the higher education system at large. The digital transformation of higher education is a double-edged sword[3]. While it offers immense opportunities for enriching the educational experience, fostering global collaboration, and streamlining administrative procedures, it also exposes institutions to a complex web of cybersecurity risks. It demands a proactive, continuously evolving strategy—one that integrates cutting-edge educational technology with comprehensive, resilient cybersecurity measures. As institutions navigate this dynamic landscape, the balance between innovation and security becomes not just a technical challenge, but a defining aspect of educational leadership in the digital age.

This paper aims to explore in detail the complexities of this transformation, examining the technologies that are driving change, analyzing the security risks that they introduce, and investigating the strategies that can be developed to mitigate these risks while maximizing the benefits of a digitally integrated educational environment. We delve into the policies that govern this transformation, critique their effectiveness, and propose a comprehensive framework for the secure, efficient, and educationally enriching digital transformation of higher education institutions.

2. Network security challenges of digital transformation of universities

In the current regulatory landscape, there is an increasing emphasis on stringent cybersecurity laws and regulations. Universities, as network operators, are required to adhere to a wide array of local, national, and international cybersecurity standards. Non-compliance not only risks exposure to cyber threats but also potential severe administrative penalties, including hefty fines and reputational damage.These compliance requirements are not static; they evolve in response to emerging cyber threats, thus demanding continual updates to institutional policies and practices. Educational institutions must, therefore, engage in continuous monitoring of the regulatory landscape and invest in resources for frequent policy updates and staff training. This ensures that universities remain ahead of potential legal issues while adapting to new cybersecurity best practices[4].

As digital campuses become more sophisticated, their information systems are deeply integrated with core educational and administrative functions. The development of myriad applications, designed to enhance learning and operations, has inadvertently increased the risk of system vulnerabilities. These vulnerabilities, paired with potential management deficiencies, expose universities to a plethora of security threats, from data breaches to unauthorized system access. To mitigate these risks, there is a growing need for universities to employ comprehensive, multi-layered security protocols, which involve regular system audits, penetration testing, and the adoption of advanced threat detection and response tools.The speed at which new technologies are adopted and business processes change in universities poses its own set of network security challenges. Frequent system updates and overhauls, necessary for maintaining cutting-edge educational environments, may inadvertently introduce security gaps. These transitional periods, if not managed with rigorous security oversight, can be prime opportunities for malicious actors to exploit system weaknesses. As such, a robust change management process, which incorporates stringent security checks and balances, is imperative. Universities must develop strategies to securely manage the lifecycle of their systems, ensuring that security is a foundational component of system design, development, deployment, and decommissioning[5].

Emerging technologies, such as artificial intelligence, IoT, and cloud platforms, while offering substantial benefits, introduce novel security concerns. For example, IoT devices often lack built-in security features, making them potential entry points for cyberattacks. Similarly, the use of artificial intelligence can be a double-edged sword; while it can help to identify and counteract threats more efficiently, it may also be used by adversaries to launch more sophisticated attacks.While most universities have established traditional cybersecurity systems, many of these systems are reactive rather than proactive. They may be adept at responding to known threats but are often ill-equipped to actively discover new vulnerabilities or to defend against novel attack strategies. This is exacerbated by a frequent lack of investment in up-to-date security technologies and an over-reliance on outdated security protocols.Addressing these cybersecurity challenges is not solely a matter of technology; it is also a human issue. There is a pressing need for colleges and universities to invest in extensive personnel training. This includes not only training IT staff in the latest security practices but also educating faculty, staff, and students about the risks of cyber threats and the importance of adhering to security protocols. Furthermore, there is a necessity to continually optimize the security systems in place. This involves regular reviews and updates to ensure that the security measures are commensurate with the current threat landscape and are integrated seamlessly with the evolving digital campus infrastructure[6].

3. Exploration of network security requirements for digital transformation in universities and colleges

In the digital transformation process, the cybersecurity risks (R) that universities face can be related to multiple factors, such as technical vulnerabilities (V), malicious attacks (A), compliance (G), and staff training (T). Simultaneously, universities' defense capabilities (D) are related to various factors, such as technical protection (P), organizational management (M), and teachers and students' cybersecurity literacy (E). We can create the following linear models to describe these relationships:

$$R = \alpha \cdot V + \beta \cdot A + \gamma \cdot G - \delta \cdot T$$

$$D = \theta \cdot P + \iota \cdot M + \kappa \cdot E$$

Here, $\alpha, \beta, \gamma, \delta, \theta, \iota$ are weight coefficients, representing each factor's relative impact on risks and defense abilities.

To calculate the overall risk and defense capabilities of cybersecurity, we can create a function between risk and defense, represented as:

$$S = R - D$$

Where S represents the overall situation of cybersecurity. The lower the value of S, the higher the overall security of the university's network.

Now, we can choose specific values to simulate this model. Assuming the values for technical vulnerabilities, malicious attacks, compliance, and staff training are: V=5, A=7, G=3, T=4. The values for technical protection, organizational management, and teachers and students' cybersecurity literacy are: P=6, M=4, E=5.

Selecting appropriate weights, such as:

$$\alpha = 0.5, \beta = 0.6, \gamma = 0.4, \delta = 0.3, \theta = 0.7, \iota = 0.5, \kappa = 0.6$$

We can calculate:

$$R = 0.5 \cdot 5 + 0.6 \cdot 7 + 0.4 \cdot 3 - 0.3 \cdot 4 = 9.4$$

$$D = 0.7 \cdot 6 + 0.5 \cdot 4 + 0.6 \cdot 5 = 9.7$$

$$\text{S=9.4-9.7=-0.3}$$

The negative value of S indicates that the university's network defense capability exceeds the risks, and the overall situation of network security is positive.

4. Construction of Network Security System for Digital Transformation of Higher Education Institutions

To bolster network security, educational institutions must first establish a dedicated leadership group for cybersecurity. This team is charged with defining roles, formulating strategic plans, and crafting actionable, comprehensive network security policies[. Furthermore, the group is tasked with recruiting a professional network security team, which might include both internal experts and third-party service providers. This blend of in-house and external expertise can provide a broad and deep pool of knowledge and skills. The professional development of existing staff is equally paramount. Continuous training programs must be established to ensure that internal teams are kept abreast of the latest threats and best practices. Regular security audits, vulnerability assessments, and penetration testing should be scheduled to identify potential weak points before they can be exploited by malicious actors. Enhancing the network security literacy of teachers and students is an essential component of a comprehensive strategy. Universities must deploy ongoing educational campaigns that inform and update the community on security best practices, emerging threats, and responsible use of digital resources. These efforts can be supplemented with regular drills that simulate various types of cyber threats, preparing the community for potential real-world incidents.

On the technical side, institutions should consider building an integrated network security protection system. This system would comprise a perception center, which continuously monitors network behavior; an intelligence center, responsible for analyzing data and detecting anomalies; and a management center that oversees response strategies when threats are detected. This robust framework should be designed to evolve in response to the swiftly changing landscape of cyber threats. With respect to the support and guarantee system, selecting forward-looking, iterative network security products, technologies, and services that align with digital business needs is vital. These products must be scalable to accommodate the growing digital infrastructure of the institution and flexible enough to adapt to new types of cyber threats.Investment is also key. Ensuring adequate funding for network security initiatives, from staff training to infrastructure improvements, is crucial. This may involve reallocating existing budgets or seeking additional funding through government grants, partnerships, or other external sources.

The security literacy of teachers and students is paramount. Regular training programs, public awareness campaigns, and practical drills should be part of a university's strategy to educate its community on the importance of network security and how to respond to potential threats. These initiatives aim to foster a campus culture where security is everyone's responsibility and where individuals are equipped to act proactively to mitigate risks. To ensure robust technical protection, colleges and universities need to develop a layered and responsive network security architecture. This might involve the establishment of a perception centre to monitor and detect network anomalies, an intelligence centre to analyze these anomalies and predict potential threats, and a management centre to coordinate timely and effective responses. The system should be designed to evolve, incorporating new technologies and strategies as the security landscape changes. A solid network security foundation requires a compatible selection of products, technologies, and services tailored to an institution's unique digital business needs. Beyond choosing appropriate tools and services, universities need to ensure that their selections are adaptable and future-proof, ready to meet the challenges of an ever-evolving cyber threat landscap.

Moreover, ensuring the implementation of these systems also involves the allocation of budget and resources. Universities must prioritize funding to maintain and enhance network security infrastructure and staffing continuously. This involves regular reviews and updates to the budget, reflecting the dynamic nature of digital security needs and threats.

We can use graph theory to describe the network security structure of universities. A directed graph $G=(V, E)$ is defined, where V is the set of network nodes, representing various devices, systems, and platforms, and E is the set of edges, representing network connections. Connectivity is an essential parameter to measure network robustness. In the presence of disconnections in the network, the number of connected components can be calculated using the following formula:

$$C = |V| - |E| + k$$

The network's security level can be defined as a variable S within the range [0,1], with 0 being completely insecure and 1 being completely secure. The security level can be calculated through:

$$S = \frac{\sum_{i=1}^{n} s_i}{n}$$

Assuming our network has 100 nodes and 150 edges, with 5 connected components. The security levels for each node are randomly distributed between 0.6 and 0.9. Thus:

Number of connected components:

$$C = 100 - 150 + 5 = -45$$

Average security level:

$$S \approx 0.75$$

5. Conclusion

With the continuous deepening of social digital transformation, the cybersecurity ecological environment is more complex and changeable. New network architectures, new security challenges, and new application scenarios have given rise to a new generation of cybersecurity solutions. In the process of university digital transformation, cybersecurity construction is an important part, and cybersecurity engineering is a long-term and systematic project. Universities need to strengthen top-level design planning, comprehensively implement cybersecurity responsibility systems, pay attention to teachers and students' cybersecurity training and publicity work, strengthen cybersecurity team building, and build a scientific and effective cybersecurity system in the face of open and borderless networks, zero trust in security authentication, and asymmetric attack and defense in the background of digital transformation, to ensure the digital transformation of universities.

Reference

[1] Brunetti F, Matt D T, Bonfanti A, et al. Digital transformation challenges: strategies emerging from a multi-stakeholder approach[J]. The TQM Journal, 2020, 32(4): 697-724.

[2] Benavides L M C, Tamayo Arias J A, Arango Serna M D, et al. Digital transformation in higher education institutions: A systematic literature review[J]. Sensors, 2020, 20(11): 3291.

[3] Garzoni A, De Turi I, Secundo G, et al. Fostering digital transformation of SMEs: a four levels approach[J]. Management Decision, 2020, 58(8): 1543-1562.

[4] Garzoni A, De Turi I, Secundo G, et al. Fostering digital transformation of SMEs: a four levels approach[J]. Management Decision, 2020, 58(8): 1543-1562.

[5] Jelonek D, Tien N H, Dao M T H, et al. Comparative analysis of business strategy of Vietnamese real estate developers: the use of Hoffer matrix[J]. International journal of multidisciplinary research and growth evaluation, 2022, 3(1): 197-204.

[6] Okunlaya R O, Syed Abdullah N, Alias R A. Artificial intelligence (AI) library services innovative conceptual framework for the digital transformation of university education[J]. Library Hi Tech, 2022, 40(6): 1869-1892.