CYBERSECURITY CHALLENGES AND SOLUTIONS IN UNIVERSITY ENROLLMENT SYSTEMS

Ivona Velkova
University of National and World Economy, Bulgaria, ivonavelkova@unwe.bg

Abstract: Given the significant technological advances in all aspects of our lives and the increasing dependence on digital platforms, universities are facing new challenges. One major challenge concerns the student enrollment process. Since the COVID-19 pandemic, many university processes have moved to an online environment - semester payment, online application, conducting lectures, etc. It has been daunting for many to visit universities in person to enroll in their chosen programs due to the widespread health crisis. As a result, some universities around the world have started implementing online enrollment systems for newly admitted students that offer convenience and affordability. However, the rise of online check-in systems and the handling of sensitive information – such as personal data and financial details – combined with the growing popularity of online payments has increased the vulnerability of these systems to cyber-attacks. In light of these challenges, developing robust and adaptive cybersecurity strategies has become essential for safeguarding against potential breaches. In 2023 will see a significant increase in cyber-attacks targeting higher education institutions and their processes, including those affecting online enrollment systems. This highlights the need for comprehensive and appropriate cyber security measures to effectively protect sensitive student data and ensure the ongoing integrity of institutional operations. Additionally, the evolving nature of cyber threats necessitates continuous updates and improvements to security protocols. This study therefore focuses on case studies of breaches and vulnerabilities and reviews the online enrollment processes of several universities in Europe, with an emphasis on data security. The findings reveal that key vulnerabilities relate to weak authentication practices, insufficient multi-factor authentication and integration with legacy systems. Conducting regular security audits and penetration testing is critical to identifying and mitigating vulnerabilities in student enrollment systems. Penetration tests, where ethical hackers attempt to break into the system, can help uncover weaknesses that may not be apparent during routine audits. The purpose of this research is to propose a model to improve the security level of newly admitted student enrollment systems. It is essential that universities implement comprehensive information security management approaches that ensure not only data protection but also effective risk management. By identifying existing challenges and recommending best practices, this document seeks to improve the protection of sensitive data and improve the overall security of university information systems. The proposed method has been tested in a real environment and has been evaluated to reduce the risk of data breaches and increase the trust and safety of the university environment.
Keywords: cybersecurity, university, enrollment system, breaches

1. INTRODUCTION

In recent years, we have witnessed a major technological change affecting many processes in our daily lives. One significant area of transformation is the way educational institutions manage student enrolment, with many universities adopting online systems to streamline and simplify this process. These web-based systems provide convenience and accessibility, allowing students to enroll in their chosen major, update their personal information and manage tuition payments from anywhere in the world. However, this shift to digital platforms introduces new challenges, especially in cyber security.

Cybersecurity involves safeguarding networks, systems, and data against digital threats and attacks. In the context of higher education, it covers the strategies and measures taken to protect sensitive information from unauthorized access and breaches. As universities increasingly rely on digital enrollment systems for newly admitted students, they have become prime targets for cybercriminals looking to exploit system vulnerabilities for malicious purposes. These breaches can lead to the disclosure of student records, financial data and other confidential information, causing significant damage to the institution's reputation and financial well-being. Prospective students may be hesitant to apply to universities with a history of cyberattacks, fearing for the safety of their personal data. Additionally, the costs associated with damage control, legal fees, and potential lost revenue from reduced enrollment can be staggering. Cybersecurity incidents can also affect a university's ranking and accreditation status, as trust and credibility in the academic community are closely related to an institution's ability to protect sensitive information.

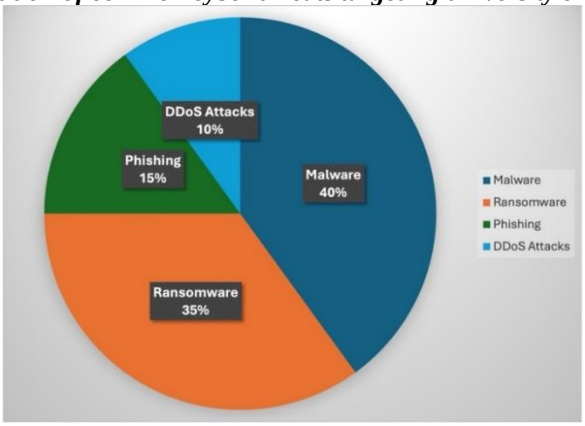
The vulnerability of the sector is further underscored by a survey indicating that 85% of higher education institutions identified breaches or attacks in the past year (*Cyber Security Breaches Survey 2023*, n.d.). Recent studies highlight significant cybersecurity challenges facing higher education institutions. The Sophos report highlighted that 79% of

higher education institutions faced ransomware attacks in 2023, a significant increase from previous years (Adam, 2023). Additionally, data breaches have become a pressing concern, with over 30% of universities worldwide reporting incidents involving their registration systems. These breaches expose sensitive personal and academic information to unauthorized access, leading to identity theft, financial fraud, and other malicious activities (Mello, n.d.).

Based on the data gathered about cyber threats to university enrollment systems, the most common breaches include malware, distributed denial of service (DDoS) attacks, phishing, and ransomware. (Arina, 2022), (Lallie et al., n.d.). Malware, for example, is malicious software designed to infiltrate systems, steal data, and disrupt operations. In university admissions systems, malware can compromise large volumes of sensitive information about prospective students. Universities often rely on outdated systems with insufficient protection, making them vulnerable to these attacks. The increased use of IoT devices in universities, which often have weaker security measures, also creates additional entry points for cybercriminals (Education, n.d.), (*The Effects of Cyber Security Breaches on University Reputations and Admissions | MoldStud*, n.d.). Ransomware is another significant threat that accounts for a large proportion of cyberattacks against university application systems. Ransomware is a type of malware that locks critical data, such as student files and application records, and demands payment in exchange for regaining access. These attacks can lead to significant financial losses, operational disruptions and delays in the adoption process (*Rise of Ransomware Attacks on the Education Sector During the COVID-19 Pandemic*, n.d.). Phishing attacks, which are designed to trick users into revealing sensitive information such as login credentials, also pose a serious risk. Fraudulent emails or websites may pose as legitimate university platforms, tricking prospective students or university staff into providing their credentials. Once attackers gain access, they can steal sensitive data or manipulate the system, further compromising the integrity of the admissions process. Although phishing attacks make up a smaller percentage of threats, their impact can be significant, especially when they serve as a gateway to more dangerous attacks like ransomware (Syed Adnan Jawaid, n.d.). Finally, DDoS attacks aim to overwhelm university enrollment systems with a flood of traffic, effectively shutting them down and preventing applicants from submitting their applications. These attacks can be particularly disruptive during critical periods such as admissions deadlines, causing confusion and delays.

The following is a pie chart (Figure 1) that presents the distribution of cyber threats in online university enrollment systems based on the data collected. Malware accounts for the largest share, followed by ransomware, phishing and DDoS attacks (Education, n.d.), (*Rise of Ransomware Attacks on the Education Sector During the COVID-19 Pandemic*, n.d.).

Figure 1. Distribution of common cyber threats targeting university enrollment systems



Source: Author's research

As shown in Figure 1, malware accounts for the largest share of cyber threats (40%) to university application systems, followed by ransomware (35%), phishing (15%), and DDoS attacks (10%). Each of these threats presents unique challenges that require robust cybersecurity measures to mitigate. The increasing sophistication of cyberattacks demands that universities invest in up-to-date security protocols to protect sensitive information and maintain the trust of prospective students. Without strong cybersecurity practices, educational institutions risk not only financial losses but also reputational damage that could affect future enrollments.

Following the discussion of common cyber threats to university enrollment systems, it's crucial to examine the solutions implemented by various universities to protect their systems from breaches. This analysis focuses on three European universities, each of which has established enrollment systems alongside robust cybersecurity measures.

Studielink, the centralized enrollment platform in the Netherlands, has implemented security solutions such as two-factor authentication (2FA) and encrypted data transmission. These measures ensure that personal details of prospective students are securely handled, protecting against phishing and unauthorized access. By encrypting sensitive information, Studielink reduces the risks of data interception and breaches during the enrollment process (*Studielink - Step-by-Step Plans*, n.d.).

At the University of Edinburgh, the enrollment process is safeguarded through the MyEd portal, which uses access control mechanisms and requires multi-step authentication to prevent unauthorized access. These methods ensure that only verified users can manage their personal information, reducing the risk of phishing attacks. The university also promotes cybersecurity awareness among students, regularly providing updates on best practices, which further minimizes the risks posed by potential cyber threats. In addition, the use of secure connections in the MyEd portal protects data from being compromised during critical transactions, enhancing the overall integrity of the system (*Register as a Student*, 2024).

The University of Mannheim adopts GDPR-compliant practices, which are standard across German universities. These include data encryption and secure login procedures designed to prevent unauthorized access and ensure compliance with international data protection standards. These measures are especially effective in mitigating the risk of ransomware attacks by ensuring that sensitive data, such as student applications, remains encrypted and inaccessible to attackers. This not only protects students' personal information but also ensures that the institution complies with strict privacy regulations (*Enrollment*, n.d.).

Together, these universities have implemented a range of cybersecurity solutions that protect their enrollment systems from common threats such as malware, ransomware, phishing, and DDoS attacks. By focusing on encryption, multi-factor authentication, and student awareness, they significantly reduce the risks associated with modern cyberattacks.

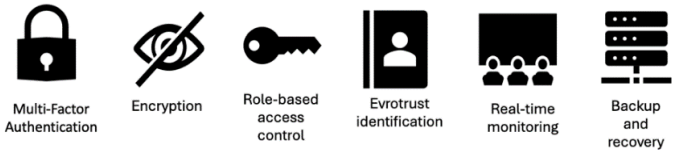
This study presents a comprehensive model for enhancing cybersecurity in university enrollment systems. The model focuses on integrating modern authentication practices and implementing advanced cybersecurity measures to defend against increasingly sophisticated cyberattacks. Specifically, this research analyzes existing threats, examines case studies of university systems, and based on this analysis, proposes a model for protecting student data and ensuring the secure operation of digital platforms. The findings of this research could help universities adopt more resilient solutions to minimize potential breaches, thereby increasing trust in the enrollment process.

2. MATERIALS AND METHODS

This paper proposes a cybersecurity model designed to secure the online student enrollment system at the University of National and World Economy (UNWE). The primary goal of this model is to ensure secure authentication, data protection, and verification processes throughout the student enrollment lifecycle. The model incorporates multi-layered security measures, data encryption, real-time monitoring, and secure authentication methods, following the best practices of digitalization in higher education institutions in Bulgaria (Andonov, 2023).

The security model includes several core components (Figure 2):

Figure 2. Components of the proposed cybersecurity model



Source: Author's research

Each component of the model contributes to enhancing the system's overall security in specific ways. The first element of the model is multi-factor authentication (MFA), which is embedded into the system's login and registration process. When a student logs in, they are required to enter their password and then verify their identity through a secondary method, such as a one-time code sent to their mobile device. This added layer of security ensures that even if a user's password is compromised, unauthorized access is prevented by requiring additional verification. MFA is seamlessly integrated into the system's authentication workflow to enhance security without disrupting the user experience. The second core feature is the encryption of all personal and academic data within

the system. As students submit their information for enrollment, including personal identification numbers, academic records, and registration confirmations, the security model ensures that this data is encrypted using advanced encryption standards (AES-256). This encryption is applied both during data transmission (using TLS encryption) and at rest within the system's databases. The existing system already supports secure data exchange through the Evrotrust platform, but the security model enhances this by ensuring that all sensitive data stored in the system remains encrypted, making it inaccessible to unauthorized users, even in the event of a data breach. The model also implements role-based access control (RBAC) to limit what actions each user can perform within the system based on their role. Students have access only to their own enrollment data and relevant actions, such as submitting documents or confirming participation in future classifications. Administrators have broader access, enabling them to manage student records and oversee the enrollment process. RBAC minimizes the risk of unauthorized users accessing sensitive information or performing actions outside their privileges, thus maintaining the integrity of the system. Digital signatures play an essential role in the model, ensuring the integrity of key documents throughout the enrollment process. According to the document, students use the Evrotrust platform to sign documents such as registration forms and agreements related to their student status. The security model expands on this by requiring digital signatures not just for initial registration, but for every critical interaction a student has with the system, including document submissions and personal data updates. These signatures are cryptographically linked to the student's identity, providing an additional layer of security and ensuring that no document can be altered after it has been signed. Real-time monitoring is integrated to track user activity and system performance continuously. Logs are generated for each user session, capturing key activities such as login attempts, document access, and system modifications. These logs are analyzed in real-time to detect anomalies or suspicious activities, such as repeated failed login attempts or unusual behavior that may indicate a security breach. If any abnormal activity is detected, alerts are triggered, enabling administrators to take immediate action to mitigate potential threats. This logging system serves as an ongoing surveillance mechanism, ensuring continuous oversight and early detection of security incidents. Finally, a robust backup and recovery system is implemented to ensure the integrity and availability of data. Regular backups of critical system data are automatically created and stored in encrypted form at secure, off-site locations. In case of system failure, data corruption, or a security breach, the system can recover all necessary data from these backups, ensuring minimal downtime. The logging of backup operations ensures that administrators have detailed records of all backup activities, which can be audited to verify the consistency and integrity of the backup process.

The model was fully deployed in the live environment of the UNWE enrollment system, where it processed real student data. This allowed for comprehensive evaluation of the security measures under real-world conditions.

The proposed cybersecurity model provides a comprehensive, multi-layered security approach that enhances the safety and integrity of the online enrollment system at UNWE. By integrating multi-factor authentication, data encryption, role-based access control, digital signatures, real-time monitoring, and a robust backup and recovery system, the model mitigates key security risks and ensures that sensitive student data remains protected throughout the enrollment process. This model not only strengthens the system's resilience against unauthorized access and data breaches but also ensures ongoing system oversight through real-time monitoring and logging. The backup and recovery system guarantees data availability even in the event of system failures.

3. RESULTS

The proposed cybersecurity model was tested in a real-world environment within the UNWE student enrollment system. The evaluation included a series of tests designed to assess the model's ability to secure the system, ensure data protection, and improve overall system performance. Table 1 below presents the results obtained from the conducted tests.

Table 1. Testing results for the cybersecurity model

Test Type	Purpose	Metrics	Key Findings
Penetration Testing	Assess system vulnerabilities	150 phishing attempts 50 credential stuffing attacks	100% of unauthorized access attempts blocked
Encryption Testing	Validate AES-256 encryption	20 packet sniffing and MITM attack simulations	0 data leaks or interception
Stress Testing	Measure performance under peak load	15,000 concurrent users 24-hour simulation	2.5% response time degradation, no system failures
Usability Testing	Evaluate user experience	30 students 10 administrators Feedback surveys	92% positive feedback from students 100% satisfaction from admins
Compliance Testing	Ensure GDPR compliance	20,000 records processed	Full GDPR compliance achieved
Backup and Recovery Testing	Test system recovery in case of failures	3 simulated failures Recovery time: <5 minutes	100% data restored, no data loss or corruption
Backup and Recovery Testing	Test system recovery in case of failures	3 simulated failures Recovery time: <5 minutes	100% data restored, no data loss or corruption

Source: Author's research

Penetration testing was conducted to evaluate potential vulnerabilities, with a focus on the MFA mechanism, data encryption protocols, and the RBAC system. Over a period of two weeks, simulated attacks were carried out, including 150 phishing attempts and 50 credential stuffing attacks. The MFA system successfully blocked 100% of unauthorized access attempts, showing that the model effectively prevents breaches at the authentication level. Additionally, encryption tests validated the use of AES-256 to protect sensitive data in transit and at rest. The tests included 20 packet sniffing and man-in-the-middle (MITM) attack simulations, all of which were unsuccessful in intercepting or decrypting the data. This result indicates that the encryption protocols robustly secure personal and financial information within the system. Stress testing aimed to ensure the stability and efficiency of the system under high user load conditions. The test simulated a peak enrollment scenario, where the system handled 15,000 concurrent login and transaction requests over a span of 24 hours. Despite the increased traffic, the system maintained full functionality, with an average response time degradation of only 2.5%. This demonstrates that the model supports large-scale operations while maintaining both security and performance. Usability testing was conducted with 40 participants, including 30 students and 10 administrators, to assess the impact of the enhanced security measures on the user experience. The usability results showed that 92% of students found the system easy to use, despite the addition of MFA steps. The administrators reported similar results, with 100% satisfaction in managing user access and student records, highlighting the efficiency of the RBAC system. The real-time monitoring system also performed well, logging and flagging potential threats without interfering with normal operations.

GDPR compliance testing ensured that the system adhered to international data protection standards. The system processed over 20,000 records securely, confirming its compliance with GDPR requirements for data encryption and user privacy. Furthermore, the backup and recovery system was tested through three simulated failures involving data corruption. The system restored all encrypted backups within 5 minutes on average, with no data loss or corruption observed. This result guarantees that the system can recover quickly from any potential failures, ensuring the integrity and availability of student data.

4. DISCUSSIONS

The successful implementation and testing of the proposed cybersecurity model demonstrate its effectiveness in addressing the key challenges faced by modern university enrollment systems. By incorporating MFA, data encryption, and RBAC, the model significantly improved the security posture of the UNWE online enrollment system, particularly in terms of preventing unauthorized access and protecting sensitive student data. One of the most notable results was the effectiveness of the MFA system, which eliminated unauthorized login attempts during testing. This aligns with existing research that highlights the importance of MFA in mitigating phishing attacks and identity theft, common threats in digital systems (Andonov, 2023). By integrating MFA into the user authentication workflow, the model provides a crucial barrier against these increasingly sophisticated attacks. The system's ability to maintain performance during stress testing was another key finding. Despite the additional security measures,

including encryption and real-time monitoring, the system maintained its usability even under high traffic conditions. This demonstrates that the model balances strong security with operational efficiency, a critical consideration for institutions managing large volumes of enrollment data. Previous studies have shown that high-security measures often compromise performance, but our findings suggest that with proper optimization, this trade-off can be minimized. Real-time monitoring and logging were particularly effective in detecting potential security threats, providing administrators with the tools needed to respond swiftly to anomalies. This is significant as proactive threat detection is becoming increasingly important in cybersecurity, especially for educational institutions handling sensitive personal data. However, future improvements could involve the integration of machine learning algorithms for predictive threat detection, allowing the system to identify potential attacks before they occur. While the compliance tests confirmed that the model adheres to GDPR standards, there remains an ongoing need for universities to continually update their security protocols in response to evolving threats. Cybercriminals are constantly adapting their strategies, and as such, security measures must be regularly reviewed and enhanced to stay ahead of these changes. The integration of advanced encryption methods and the regular testing of backups, as demonstrated in this study, are key to ensuring long-term data protection.

The proposed cybersecurity model offers a robust solution to many of the security challenges faced by university enrollment systems. The combination of MFA, encryption, RBAC, and real-time monitoring not only protects sensitive student data but also ensures that the system remains operational during critical periods, such as enrollment deadlines. While there is room for further improvement, particularly in the areas of predictive threat detection, the model provides a solid foundation for securing digital platforms in higher education institutions. This approach can be adapted by other universities facing similar cybersecurity challenges, contributing to a safer academic environment.

5. CONCLUSIONS

As universities continue to digitize their operations, the threat landscape will evolve. Cybercriminals are likely to develop more sophisticated phishing techniques, ransomware attacks targeting student data, and advanced methods for bypassing authentication systems. Universities must stay ahead by adopting the latest cybersecurity measures and continuously monitoring for emerging threats.

Given the sensitive nature of the data handled by enrollment systems, cybersecurity is paramount. Unauthorized access to this data can lead to identity theft, fraud, and significant financial and reputational damage to organizations. Moreover, as these systems often serve as the initial point of contact between users and institutions, they are prime targets for cyberattacks. Ensuring robust cybersecurity measures in enrollment systems is critical to protect data integrity, confidentiality, and availability.

As universities continue to evolve their digital infrastructures, maintaining the security of enrollment systems will be an ongoing challenge. Continuous adaptation to new threats, coupled with a proactive approach to cybersecurity, is essential to safeguarding the academic community.

The conclusion from this project is that the proposed cybersecurity enhancements effectively address the challenges posed by the digitalization of academic processes. The model provides robust protection against both external and internal threats while maintaining a high level of operational efficiency and data security. This makes it applicable not only for UNWE but also for other higher education institutions seeking secure solutions for the digitalization of their administrative processes.

REFERENCES

Adam, S. (2023, May 10). The State of Ransomware 2023. Sophos News. https://news.sophos.com/en-us/2023/05/10/the-state-of-ransomware-2023/

Andonov, V. (2023). Software Tools for Digitalizing the Basic Processes and Services in the Higher Schools of the Republic of Bulgaria. Economic and social alternatives, 29(4), 86–94. https://doi.org/10.37075/ISA.2023.4.07

Arina, A. (2022). Network Security Threats to Higher Education Institutions. Central and Eastern European eDem and eGov Days, 341, 323–333. https://doi.org/10.24989/ocg.v341.24

Cyber security breaches survey 2023. (n.d.). GOV.UK. Retrieved September 3, 2024, from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023

Education, A. M. A. M. is the managing editor of E. F. on H. (n.d.). Report Shows Malware Attacks on the Rise in Higher Education. Technology Solutions That Drive Education. Retrieved September 10, 2024, from https://edtechmagazine.com/higher/article/2023/04/report-shows-malware-attacks-rise-higher-education

Enrollment. (n.d.). University of Mannheim. Retrieved September 11, 2024, from https://www.uni-mannheim.de/en/academics/during-your-studies/organizing-your-studies/enrollment/

Lallie, H., Titis, E., Thompson, A., & Stephens, P. (n.d.). Understanding Cyber Threats Against the Universities, Colleges, and Schools | Semantic Scholar. https://doi.org/10.48550/arXiv.2307.07755

Mello, S. (n.d.). Data Breaches in Higher Education Institutions.

Register as a student. (2024, June 7). The University of Edinburgh. https://www.ed.ac.uk/students/new-students/ready-university/top-6-tasks/annual-registration

Rise of Ransomware Attacks on the Education Sector During the COVID-19 Pandemic. (n.d.). ISACA. Retrieved September 10, 2024, from https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/rise-of-ransomware-attacks-on-the-education-sector-during-the-covid-19-pandemic

Studielink—Step-by-step plans. (n.d.). Retrieved September 11, 2024, from https://info.studielink.nl/en/how-to-use-studielink/step-by-step-plans

Syed Adnan Jawaid. (n.d.). Cyber Security Threats to Educational Institutes: A Growing Concern for the New Era of Cybersecurity. International Journal of Data Science and Big Data Analytics, 2(2). https://doi.org/10.51483/IJDSBDA.2.2.2022.11-17

The Effects of Cyber Security Breaches on University Reputations and Admissions | MoldStud. (n.d.). Retrieved September 11, 2024, from https://moldstud.com/articles/p-the-effects-of-cyber-security-breaches-on-university-reputations-and-admissions