

Enhancing Security and Privacy in Credit Transfer Application Systems: A Proposed Framework

Farah Farzana Abdul Aziz^{1}, Raznida Isa², Noraliza Azizan³, Noornajwa Md Amin⁴,
Noorshamshillah Kamarzaman⁵, & Siti Fajar Jalal⁶*

^{1,2,3,4,5,6} Faculty of Computing & Multimedia, Universiti Poly-Tech Malaysia, 56100 Kuala Lumpur, Malaysia

Corresponding author: Farah Farzana Abdul Aziz

Email: farah_aziz@uptm.edu.my

DOI: <https://doi.org/10.61688/ajpbs.v6i2.422>

Article History

Received	Revised	Accepted	Published
5 July 2025	20 November 2025	30 November 2025	31 December 2025

ABSTRACT

Automated credit transfer systems in higher education offer substantial efficiency improvements but also introduce critical data security and confidentiality challenges. This paper addresses the reported security gaps in the Universiti Poly-Tech Malaysia (UPTM) prototype of the Credit Transfer Application System (CTAS), which lacks essential security features such as user authentication, role-based authorization, and encrypted data protection. To address these issues, this study proposes a secure academic data management framework incorporating secure user authentication, role-based access control, encrypted database storage, and secure HTTPS communication protocols. The research methodology includes comprehensive security requirement analysis, detailed system architecture design, and the development of a validation plan comprising system simulation, penetration testing, performance evaluation, and compliance assessment to be conducted in future work. The proposed framework is intended to strengthen system access control, improve user accountability, enhance data privacy, and support alignment with Malaysia's Personal Data Protection Act (PDPA). This study presents a proposed security architecture to guide future system enhancements and deployments, providing a strong foundation for safeguarding academic data and supporting potential cross-institutional credit transfer initiatives. If implemented and validated, the framework may support institutional credibility, data protection practices, and digital transformation in academic processes in higher education.

Keywords: Data Security, Credit Transfer, Authentication, Privacy, Educational Technology

How to Cite

Abdul Aziz, F. F., Isa, R., Azizan, N., Md Amin, N., Kamarzaman, N., & Jalal, S. F. (2025). Enhancing Security and Privacy in Credit Transfer Application Systems: A Proposed Framework. The Asian Journal of Professional & Business Studies, 6(2), 74–86. <https://doi.org/10.61688/ajpbs.v6i2.422>

Copyright © 2025 The Author(s)

Published by Universiti Poly-Tech Malaysia. This is an open access article distributed under the Creative Commons Attribution (CC BY 4.0) license. <http://creativecommons.org/licenses/by/4.0/legalcode>

1.0 INTRODUCTION

The transition from paper to computer-based credit transfer systems for higher education has brought efficiency benefits but also introduced challenges, particularly related to data security and confidentiality. Credit transfer operations play a critical role in facilitating student mobility, academic achievement and institutional cooperation within and between nations (Strack et al., 2022). These processes facilitate seamless student transfers from one program, institution, or university to another, supporting initiatives such as the Credit Transfer Application System (CTAS) and other mobility programs for students abroad. Credit transfer was formerly initiated manually, involving extensive document review and discretionary human judgment, leading to inefficiency, delays and higher administrative expenditure.

Utilisation of automated credit transfer systems is intended to simplify such transactions by utilising technology to accelerate the process, minimise errors, and maintain consistency. However, utilising automation without security controls leaves institutions with significant vulnerabilities (Al-Slais & Ali, 2023). Breaches of students' academic records, alterations to credit transfer decisions, and unauthorised disclosure of students' confidential data can drastically compromise the integrity of the system and erode stakeholders' confidence (Goyal & Verma, 2025).

At Universiti Poly-Tech Malaysia (UPTM), the CTAS prototype was developed as part of the institution's digitalisation process to automate credit assessment procedures. While the system is intended to address operational inefficiencies, it has yet to incorporate key security features, including user authentication, role-based access control, secure communication protocols, and encrypted data storage. Loopholes such as these are structural weaknesses that may expose the system to intrusion, data corruption and possible breaches (Ramim & Levy, 2006).

Their absence may jeopardise institutional data and compliance with Malaysia's Personal Data Protection Act (PDPA), which sets requirements for processing personal data where applicable. In the case of credit transfer, where student identity, academic history and detailed syllabi are being processed, system insecurity may lead to legal, reputational and operational consequences for the institution (Ismail, 2024).

For these essential needs, this paper suggests that an enhanced secure environment, particularly for the CTAS, be put in place. The proposed model takes into consideration multilayer security features such as secure user logins, role-based access, secure communication channels, and database security measures. The aim is to develop a robust system that not only addresses current vulnerabilities but also supports future scalability, inter-system integration, and possible cross-institutional integration.

By integrating security as the core element, this study proposes an approach informed by practices in educational technology and e-governance (Singh et al., 2013). The suggested framework may support institutional readiness and user confidence, and inform the development of a secure platform for managing educational information in the newer schooling environment.

2.0 LITERATURE REVIEW

2.1 Credit Transfer Systems in Higher Education

Credit transfer systems play a crucial role in facilitating student mobility and study continuity among and between institutions of learning. The systems allow students to transfer earned credits from an existing academic programme to a new one within the same institution or to a different university, often across borders. Cross-national systems such as the European Credit Transfer and Accumulation System (ECTS) and the ASEAN Credit Transfer System (ACTS) are widely used for credit assessment and the standardisation of recognition (Impola, 2024). Digital technologies in credit transfer systems are widely used, as they promise to minimise manual workload and reduce processing time.

Nonetheless, even in the wake of increased automation, institutions still use fragmented or half-automated systems that are subject to errors, human judgment, and inaccuracies. Research by Chandrasekaran and Mago (2022) indicates that credit

transfer decisions are not transparent, especially when syllabi and learning outcomes are compared manually. This has necessitated the need for high-quality, standardised, and secure systems capable of handling increased academic mobility and protecting student data.

Although the fundamental emphasis of credit transfer systems has consistently been on accumulating academic equivalency judgments, research highlights that security issues have often been overlooked. According to Pollard et al. (2017), institutions are interested in system performance, but not necessarily with the urgency of maintaining sensitive information and blocking unauthorised access, which may jeopardise institutional trust and compliance with the law.

2.2 Security Vulnerabilities in Educational Systems

As higher education institutions increase their online presence, they also open themselves up to cyber threats. Educational institutions are attractive to cyber attackers because they handle sensitive data, including student identities, personal information, academic records, financial information, and proprietary research. Trofymenko et al. (2022) discuss cybersecurity threats in higher education, including risks of data theft, phishing, and system compromise.

In credit transfer system applications, a lack of security features such as encrypted communications and authenticated, role-based access substantially increases the system's exposure to internal and external threats (Gharpure & Rai, 2022). Inadequate system hardening and weak access control policies can result in tampering with students' records, approval of falsified credits, and unauthorised disclosure of student information. This is particularly important since credit transfer applications tend to store full course syllabi, student transcripts, and histories of approvals, which are extremely sensitive in nature (Jones & VanScoy, 2019).

Without a well-organised security system, institutions not only suffer data breaches but also lose academic integrity, whereby unauthorised parties can alter credit decisions. As cyberattacks evolve, education systems that lack cutting-edge security measures become increasingly vulnerable to manipulation.

2.3 Authentication and Authorisation in Web Applications

Authentication and authorisation are the pillars of system security, especially for web-based learning systems (Krishnarajan & Rengarajan, 2024). Authentication verifies that users requesting access to the system are who they claim to be, ensuring that only valid users gain access. Authorisation, conversely, specifies the extent of activities that each authenticated user can undertake in accordance with their role in the system.

Role-Based Access Control (RBAC) has been widely discussed in the literature as a robust approach to user authorisation in educational systems. RBAC, as Destini and Tony (2024) have argued, simplifies access management by allocating well-defined roles such as administrator, coordinator, and student, each with predefined access rights. This approach may reduce the risk of privilege abuse and ensure that sensitive system processes are assigned only to competent individuals.

In addition, Multi-Factor Authentication (MFA) is increasingly advised to aid security, especially for systems handling high-risk information. MFA requires users to provide two or more proofs of identity, such as passwords, one-time passcodes, or biometric verification. MFA can add a layer of protection against credential-based unauthorised access (Simha.R et al., 2025). In the event of a request for credit transfer, integrating both RBAC and MFA would enhance the system's defence with layered security, countering present-day cybersecurity risks.

2.4 Data Protection Regulations in Higher Education

Educational institutions should assess the data protection laws applicable to their processing activities. In Malaysia, personal data is regulated by the Personal Data Protection Act (PDPA) 2010, which governs the collection, processing, and storage of personal data, ensuring that data users, including universities, are accountable for protecting the information they use (Hamin et al., 2025). Non-compliance where the Act applies may result in legal and reputational consequences.

The European Union's General Data Protection Regulation (GDPR) provides a further reference point for data protection. Having been applied throughout the European Union (EU) in May 2018, the GDPR seeks to safeguard people's private data and privacy by imposing stringent regulations on how companies handle, use, store, and transfer personal data (Tarchila, 2021). The GDPR provides for lawful bases for processing, data minimisation, and rights of access, rectification, and erasure.

Although GDPR is a regional regulation, it has global impact, as non-European institutions may fall within its scope when the conditions for territorial application are met. Its principles may also inform privacy practices in international academic partnerships and student mobility schemes (Halawi & Makwana, 2023).

In applications for per se credit transfer, PDPA compliance is paramount. This means that all students' personal data are collected lawfully, held securely, and transmitted securely. Unauthorised access, data loss, or data corruption may violate institutional policy and, depending on the circumstances, applicable PDPA requirements (Ismail, 2024).

To ensure continuous compliance, privacy-by-design principles need to be integrated from the initial stages of system development. By doing so, data protection methods are embedded directly into the credit transfer system's workflow and architecture, rather than added as an afterthought after development. Active design with privacy mitigates breach risks and facilitates simpler compliance with PDPA and international standards like GDPR.

Additionally, data protection policies need to address certain data retention practices, logging, and incident response. These are essential cornerstones for protecting sensitive student data, upholding institutional accountability, and building user trust in the system (Tiwari, 2025). Credit transfer applications that incorporate these privacy and security controls may support operational effectiveness, regulatory accountability and conformity with ethical data-handling practices. These controls may help protect the integrity of academic qualifications, facilitate student mobility, and support institutional partnerships in local and foreign academic collaborations.

2.5 Secure System Architecture for Educational Applications

Creating secure education apps needs an integrated security approach at all system design levels. Bekmezci et al. (2018) propose a multi-layered security model that includes secure user authentication, encrypted data storage, and encrypted communication channels via Transport Layer Security (TLS). This protocol helps ensure that data exchanged over the internet is safe from eavesdropping and tampering.

A secure architecture also includes real-time activity monitoring and audit trails. Audit trails allow administrators to monitor all user activity within the system, maintaining a forensic record that can be examined in case of suspicious activity or security breaches (Kebande, Karie, & Ikuesan, 2020). Real-time monitoring tools further enhance security by enabling instant detection and response to threats.

Confidential database management is equally important. Encrypting sensitive information at rest ensures that, even if storage media are compromised, the information remains unusable without the corresponding decryption keys (Neeli, 2025). Backup procedures, disaster recovery, and regular vulnerability scanning also need to be integrated into the system's security lifecycle.

In conclusion, the literature strongly favors the integration of robust security architectures in education technology products, particularly those that handle delicate academic processes like credit transfer. Modern research stresses that security cannot be an afterthought but a fundamental design consideration to guarantee trust, compliance, and long-term system sustainability.

3.0 METHODOLOGY

This research employs a systematic method to recommend a secure architecture for Universiti Poly-Tech Malaysia's (UPTM) Credit Transfer Application System (CTAS). The method has been broken down into three phases: Requirements Analysis, Framework Design, and Validation Planning. The phases have been thoroughly discussed to explain how the proposed architecture is intended to address identified weaknesses, data protection needs and future system extension while considering usability.

3.1 Requirement Analysis

The initial part of the methodology involves identifying the security weaknesses in the existing CTAS prototype. The system design, working procedures, and security weaknesses were reviewed as described in this paper. The top issues were poor user verification, protection against unauthorised access, secure data transmission, and safeguarding data storage.

The system needed to be defined in terms of how it would enforce user authentication processes that grant access only to authorised users. Without user authentication, the system would be open to unauthorised use. Additionally, without RBAC, users could view functions outside their area of work, potentially exposing sensitive academic information to unauthorised users (Neeli, 2025).

Aside from that, secure communication protocols were determined to be needed in protecting information in transit from the system server to the user's browser. If the information is not encrypted, traveling information can be accessed or intercepted. Storage facilities for data also demanded focus; that is, the need to protect sensitive academic data, such as student records and transcripts, by encrypting them during storage in the database to prevent unauthorised recovery and manipulation (Shah & Panchal, 2022).

User accountability and tracing of user activity were also identified as major security issues. The system needs to include a full history of user actions to enable future traceability and auditing. The proposed audit trail can also support the investigation of system activity (Inam et al., 2023), while applicable PDPA requirements should be assessed during implementation (Hamin et al., 2025).

The security requirements of this phase are as follows: to use secure user authentication with MFA as a capability; for instance, role-based access control to manage user permissions, securing communications via HTTPS with TLS encryption, encrypting data at rest and having a complete logging and audit trail system to manage user accountability and traceability.

3.2 Framework Design

The second phase is designing the aforementioned security framework to remedy the found vulnerabilities. The security architecture is designed to integrate with the current CTAS workflow, subject to later usability and performance testing. The suggested security architecture adds a user authentication module that mandates secure login processes. User passwords will be stored securely using bcrypt, a strong hashing algorithm that includes salting and computational difficulty to resist brute-force attacks. MFA should also be suggested to add a further verification step, especially for administrative users and approvers of credit transfers.

The design includes RBAC to provide for system access based on roles. Administrators would have role-specific access to manage users and view audit trails. Program coordinators will have limited access to credit evaluation and approval functionality, and students will have access only to enter and monitor their own credit transfer requests. Role segregation is required to minimise the risk of unauthorised access to sensitive system parts.

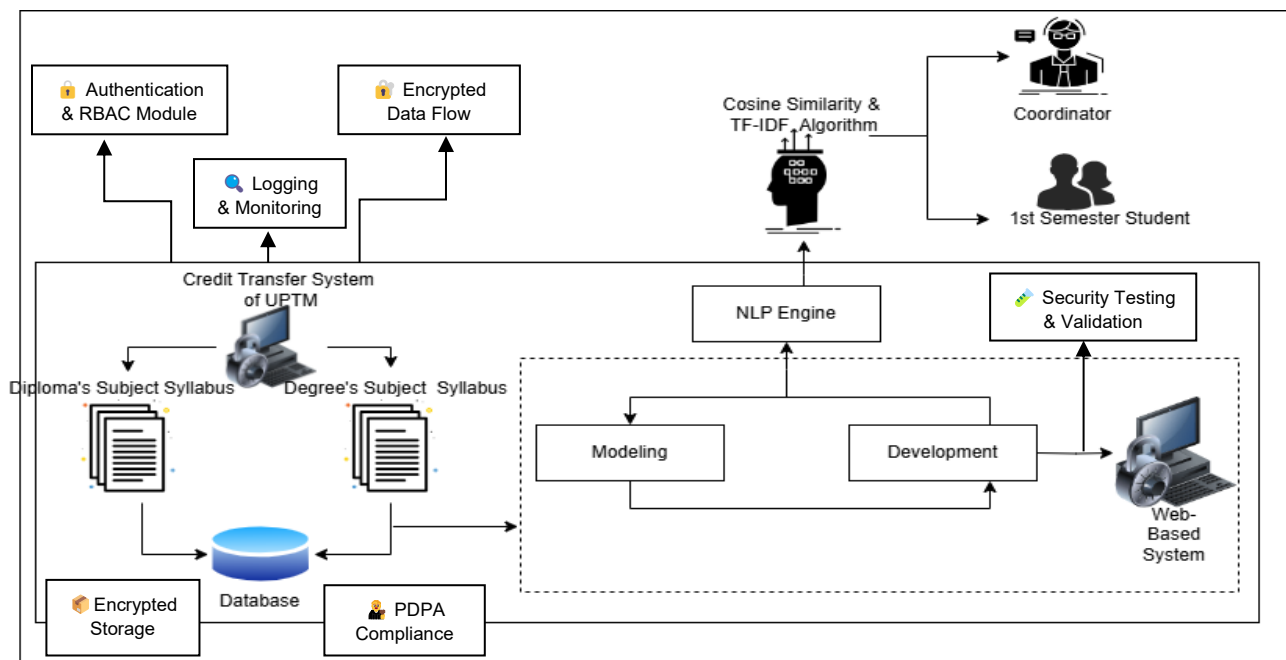
For secure transmission of data, the system must insist on safe HTTPS communication protocols under the cover of TLS encryption (Shah & Correia, 2021). In addition, all sensitive academic records and student information must be encrypted at rest to prevent unauthorized access, even in the case of a database compromise.

The design also comprises an extensive audit trail and logging subsystem for tracking key user activity, such as login attempts, data access, and credit transfer approvals. The logs will facilitate system monitoring, traceability, as well as accommodate institutional audits.

The security framework is designed to integrate to the existing CTAS process, encompassing both system protection and user usability. This framework is also adaptable to future scalability, system upgrades and potential cross-institutional credit transfer initiatives. The proposed security framework is visually illustrated in Figure 1 below to show the multi-layered security components integrated within the CTAS.

Figure 1

Proposed Security Framework for Credit Transfer Application System (CTAS)



3.3 Proposed Validation Plan

As this research proposes a security framework for the CTAS, a validation plan has been proposed for future implementation. Validation aims to comprehensively verify system security, performance, regulatory compliance, and user acceptance after the framework is designed and implemented in the system (Llanten-Lucio et al., 2022).

The validation plan described herein outlines how key aspects of security can be tested through simulation, penetration testing, performance testing, compliance testing, and user acceptance testing. All of these elements are developed with great care to assess whether the proposed system enhances security while preserving user satisfaction and meeting applicable policy and legal requirements. The validation steps in detail and the test plan are elaborated upon in Section 4.4 of this report.

4.0 FINDINGS AND DISCUSSION

This study focuses on developing and proposing a secure framework for the CTAS at UPTM. The discussion draws on the stated system requirements and the proposed framework design, and is supported by a validation plan for future testing. As the proposed framework has not yet been implemented in the live system, the discussion here is conceptual, focusing on the expected benefits and improvements once the framework is deployed.

4.1 Identified Security Gaps

The analysis of the current CTAS prototype at UPTM identified reported security gaps that could jeopardise the confidentiality, integrity, and availability of academic information. The most critical flaw is the absence of user authentication. Without authentication, users cannot be certain of their identity when accessing the system. This implies that unauthorised users could gain access to the system, posing a serious security risk by allowing them to modify, erase, or steal confidential information.

In addition, the existing CTAS does not use RBAC. Without RBAC, user permissions may not be adequately separated by role. This uncontrolled access greatly increases the risk of data exposure, as accredited users with access to simple functions, such as students, could read, modify, or erase confidential data, including credit transfer approvals, student records, or institution reports that must be viewed by administrators.

There is also a serious shortcoming in the absence of secure communication protocols within the system. As described for the prototype, communications lack the proposed TLS protection, creating a potential risk of interception. This creates a platform for man-in-the-middle (MITM) attacks, in which a hacker intercepts and tampers with sensitive data such as usernames, passwords, student transcripts, and application information in transit (Almakdi & Alshehri, 2023). Interception of such data can seriously disrupt the integrity and privacy of student data.

In addition, the prototype is described as lacking encryption for academic material in its database. Storing sensitive information, such as students' personal data, course syllabi, and academic records, in plaintext significantly increases the risk of data theft in the event of a system breach. Without encryption, if an unauthorised user accesses the database, it would be easy to extract and exploit the information it contains, with no technical hindrance (Tyshyk, 2024).

Lastly, no user activity is properly tracked and no audit trail exists in the system. This implies that activities done within the system, for instance, login attempts, data access, and credit transfer authorizations, are not traceable and logged. Since there is no logging capability, it is challenging to determine intruders, monitor user activity, or audit security incidents. Because it lacks accountability to users, it is not known with certainty who performed specific actions within the system, which erodes the institution's ability to enforce security policies and respond effectively to potential violations.

Taken together, these security vulnerabilities could increase the CTAS's exposure to risks of data leakage, system abuse, and non-compliance with data protection laws such as Malaysia's PDPA. Any remedy for such weaknesses is paramount to protecting students' data, ensuring system integrity, and upholding the institution's reputation.

4.2 Proposed Security Enhancements

To efficiently address the main security vulnerabilities in the existing CTAS prototype, an overall security architecture has been meticulously designed. The proposed scheme combines several layers of security to offer high-level protection for scholarly information, while usability and regulatory compliance are to be assessed during validation.

The user authentication module is the centre of the proposed changes, protecting the system from unauthorised use by approved users. The proposed module would use password-hashing algorithms, such as bcrypt, to securely store user passwords. The algorithms convert plaintext passwords into irreversible one-way hash values, making it computationally expensive for attackers to recover the original passwords even if the database is compromised. To provide user authentication with an added layer of strength, MFA steps in. MFA requires users to enter a second level of authentication, like a one-time password (OTP) or biometric information, after entering their username and password. The added security level greatly lessens the risk of malicious access, even if the user credentials are stolen or compromised.

RBAC is the other prominent element of the framework. Under RBAC, each user is granted system access strictly according to the role assigned to them in the institution. Administrators, for instance, will receive complete system access, right down to managing user accounts and audit trails. Program coordinators will receive partial access to functions involving credit assessment and approval, whereas students will receive access to apply for credit transfers and see only their application

status. By isolating user privileges based on role, RBAC greatly reduces the possibility of unauthorized data alteration and guards critical system operations against access by the wrong user groups (Mehra, 2024).

The architecture also includes secure communication protocols for encrypting data in transit between users and the system server. All system communication is required to use the HTTPS protocol, protected by TLS encryption. This encrypts the data as it is transferred across the network and safeguards it from interception, eavesdropping, and MITM attacks. It significantly contributes to the confidentiality and integrity of data transfer, especially when dealing with sensitive data like student records and login passwords (Chordiya et al., 2018).

In addition to protecting sensitive data in transit, the framework proposes to protect sensitive data at rest by encrypting database records. All sensitive academic information, such as students' personal information, transcripts, course syllabi, and credit transfer information, would be encrypted when stored in the database. This data-at-rest encryption is intended to reduce the exposure of readable data if unauthorized parties access the database.

In addition, the suggested framework includes detailed logging and audit-trail capabilities. The facility is to track and log all user operations on the CTAS, for example, login attempts, data query operations, credit transfer approvals and requests to change system records. High-detail logging increases user accountability by providing an exact trace of system interactions, which is critical for security monitoring, forensic analysis, and compliance audits. In the event of a security breach, the audit trail may help administrators investigate suspicious activity and respond.

The architecture of the proposed security framework enables such security features to be integrated into the current CTAS process, subject to usability and performance testing. The proposed controls aim to strengthen protection while supporting the system's usability and adoption. With improved authentication, access control, secure communication, data storage encryption, and traceability, the designed security framework provides a strong foundation for a secure, scalable, and compliant academic credit transfer system.

4.3 Anticipated System Performance and User Acceptance

Although the suggested security framework has not yet been implemented in the working CTAS, the framework aims to limit disruption to system performance. Deployment and integration of controls such as MFA, RBAC, encrypted media communication, encrypted data storage, and fine-grained audit logging have been designed with the broader goal of ensuring a balance between system security and efficiency.

From a performance point of view, implementing industry-accepted password hashing algorithms, such as bcrypt, and using TLS encryption protocols may offer security with an acceptable effect on response time, subject to testing. Similarly, MFA may add an extra step to login procedures without otherwise hampering user access to core system functionality. The logging mechanism to record all significant user actions within the system is proposed to run in the background; its processing overhead and responsiveness will need to be measured.

User acceptance is also a primary factor in determining the success of any security improvement. The outlined security measure considers whether administrators, program coordinators, and students would find the additional security features acceptable. Based on prior research in comparable systems, users may accept the additional login process for the added assurance of the security, confidentiality, and integrity of the academic records.

Future user acceptance testing will be necessary to verify this hypothesis. The proposed user testing will evaluate the effect of the added security features, namely MFA and access controls, on the routine workflow of different user groups. Feedback will be gathered to establish whether the system remains easy to use and whether the added security is seen as improving, rather than discouraging, the user experience. It is hoped that the added security features offered by the system will be valued by users, particularly in an academic setting where data confidentiality and the institution's reputation matter most.

4.4 Validation Plan for Future Work

A comprehensive validation plan has been constructed to systematically examine the intended security framework when live-installed in the CTAS. The five pillars of the validation plan are intended to enable rigorous scrutiny of system functionality, security robustness, performance efficiency, regulatory compliance and end-user satisfaction. These activities will help assess whether the intended framework meets its desired security requirements while remaining pragmatic for institutional adoption.

The initial phase is System Simulation Testing, which would examine whether the users' authentication and role-based access control. Different scenarios will be simulated so that each user role (program administrator, program coordinator, student) can use only the system functions appropriate to their assigned privilege. Any unauthorised attempt must always be refused, and system modules should be protected based on user role assignments.

The second procedure is Penetration Testing, which will simulate cyber-attack scenarios, such as brute-force password cracking, unauthorised login, and MITM attacks on data transfer pipes. Testing would assess resistance to password attacks and unauthorised access attempts and verify that data are transmitted over HTTPS using TLS.

The third phase is focused on Performance Testing to determine whether the addition of security features, such as MFA and real-time logging, has a significant effect on system responsiveness or transaction processing speed. Performance requirements will be defined to ensure that the system can process normal user loads without causing unacceptably long delays or degrading the user experience.

Fourthly, Compliance Testing will be carried out to verify that the system complies with Malaysia's PDPA and the institution's security policy. An exhaustive checklist will be used to verify that the system complies with all regulatory requirements, including data protection, user responsibility, access control, and privacy measures. The assessment would identify whether the proposed controls meet applicable institutional and legal requirements.

The last testing and validation is User Acceptance Testing (UAT) via a TAM-based formal survey questionnaire. The questionnaire would be administered to system administrators, program coordinators, and students to gather feedback on system usability, satisfaction with security features, and the perceived trade-off between security and usability. The UAT would be an extremely significant component in determining whether the proposed security framework aligns with user expectations and provides a user-friendly interface.

The structured validation plan is summarised in Table 1 below:

Table 1				
Test Plan for Credit Transfer Application System (CTAS) Security Framework Validation				
No.	Test Category	Test Objective	Test Method	Expected Outcome
1	System Simulation Testing	To verify that user authentication and role-based access control work correctly for all user types.	Simulate login and system access for administrators, program coordinators, and students in a test environment.	Users can access only the system features assigned to their roles. Unauthorised access is denied.
2	Penetration Testing	To ensure the system can resist brute-force attacks, unauthorised access, and data interception.	Simulate brute-force attacks, unauthorised access attempts, and man-in-the-middle attacks in a controlled environment.	Password security withstands brute-force attempts. Unauthorised access is blocked. Data transmission is secure.

No.	Test Category	Test Objective	Test Method	Expected Outcome
3	Performance Testing	To confirm that security features do not significantly degrade system response time or user experience.	Measure system response time and transaction speed with security features enabled.	System performance remains acceptable. Additional security steps, such as MFA, are acceptable to users.
4	Compliance Assessment	Verify compliance with PDPA and institutional security policies	Conduct a compliance review using a detailed security checklist	The system fulfils all data protection, privacy, and accountability requirements
5	User Acceptance Testing	To assess user satisfaction and usability after implementing security features.	Distribute a Technology Acceptance Model (TAM)-based survey to administrators, coordinators, and students.	Users report satisfaction with system usability and security features. No significant usability concerns are reported.

This structured testing methodology outlines how the proposed security system could be tested for technical validity, performance efficiency, legislative compliance, and user acceptance before being deployed live.

5.0 CONCLUSION

This research proposes a security framework to address the reported gaps in the CTAS prototype. Although the system is operationally viable in streamlining credit transfers, it currently lacks essential security features. These gaps could expose the system to attacks such as intrusion attempts, unauthorised access, and data interception, including the potential disclosure of sensitive academic information.

To seal these security loopholes, the proposed architecture specifies multilevel security controls to improve system resilience and data security. The architecture incorporates secure user authentication and MFA, RBAC, HTTPS-encrypted communication, encrypted database storage, and secure audit trails for increased user accountability and system traceability.

While the framework has not yet been deployed in the production CTAS environment, a structured validation plan has been established to direct follow-on testing and deployment. The validation plan includes system simulation, penetration testing, performance testing, compliance testing against regulatory requirements, and user acceptance testing to assess whether the framework meets security, usability, and applicable regulatory specifications.

The proposed architecture may guide future development within the CTAS and other education systems. It offers a starting point for protecting academic data and enables future secure cross-institutional credit transfer processes. Future development will include implementing the architecture, field-testing and validation, and incorporating next-generation features such as biometric authentication and blockchain-based credit verification to further enhance system integrity.

6.0 ACKNOWLEDGEMENT

This research was funded by the Research Management Centre (RMC) of Universiti Poly-Tech Malaysia under the University Research Grant (URG), Grant Number: UPTM.DVCRI.RMC.15 (03). The authors would like to express their sincere appreciation to RMC for the financial support and continuous encouragement throughout the project.

7.0 CONFLICT OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in the paper.

8.0 AUTHOR CONTRIBUTION STATEMENT

Author 1 contributed to the conceptualization, research design, and writing of the original draft.

Author 2 was responsible for framework analysis and development of the proposed validation plan.

Author 3 provided supervision, critical review, and editing of the final manuscript.

All authors have read and approved the final version of the manuscript.

9.0 ETHICS STATEMENT

This paper proposes a conceptual security framework and a plan for future validation. It does not report participant recruitment or the collection of personal data for this study; ethics approval and participant consent are therefore not reported here. Any future user acceptance testing should follow applicable institutional ethics and data protection requirements.

REFERENCES

- Al-Slais, Y., & Ali, M. (2023, January 1). Robotic Process Automation and Intelligent Automation Security Challenges: A Review. <https://doi.org/10.1109/CyMaEn57228.2023.10050996>
- Bekmezci, A. B., Eris, C., & Boluk, P. S. (2018). *A multi-layered approach to securing enterprise applications by using TLS, two-factor authentication and single sign-on*. <https://doi.org/10.1109/siu.2018.8404773>
- Almakdi, S., & Alshehri, M. S. (2023). Developing an Attack Model for compromising Privacy over Secure Connection Protocols. *2023 IEEE 6th International Conference on Computer and Communication Engineering Technology (CCET)*, 43–47. <https://doi.org/10.1109/ccet59170.2023.10335137>
- Goyal, A., & Verma, P. K. (2025). Blockchain for Academic Integrity Preventing Fraud and Enhancing Transparency in Education. *Advances in Nonlinear Variational Inequalities*, 28(3s), 109–124. <https://doi.org/10.52783/anvi.v28.2853>
- Chandrasekaran, D., & Mago, V. (2022). Automating Transfer Credit Assessment-A Natural Language Processing-Based Approach. *Computers, Materials & Continua*, 73(2), 2257–2274. <https://doi.org/10.32604/cmc.2022.027236>
- Chordiya, A. R., Majumder, S., & Javaid, A. Y. (2018). Man-in-the-Middle (MITM) Attack Based Hijacking of HTTP Traffic Using Open Source Tools. *2018 IEEE International Conference on Electro/Information Technology (EIT)*. <https://doi.org/10.1109/eit.2018.8500144>
- Destini, J. S., & Tony, T. (2024). Implementing Hierarchical Role-Based Access Control for Document Administration in Student Organizations. *Internet of Things and Artificial Intelligence Journal*, 4(4), 785–802. <https://doi.org/10.31763/iota.v4i4.832>
- Tiwari, P. K. (2025). Digital Trust in Education: Investigating the Relationship between Cyber security Practices and Student Confidence in Online Learning. *International Journal of Advanced Research in Science, Communication and Technology*, 245–252. <https://doi.org/10.48175/ijarsct-26432>
- Gharpure, N., & Rai, A. (2022). *Vulnerabilities and Threat Management in Relational Database Management Systems*. <https://doi.org/10.1109/icast55766.2022.10039599>
- Halawi, L., & Makwana, A. (2023). THE GDPR AND UK GDPR AND ITS IMPACT ON US ACADEMIC INSTITUTIONS. *Issues in Information Systems*, 24(2). https://doi.org/10.48009/2_iis_2023_120
- Hamin, Z., Kamaruddin, S., Md Noh, H. N., Othman, M. B., & Mohamad, A. M. (2025). Recent Reforms to the Personal Data Protection Act 2010 and Its Implications for Business Organisations in Malaysia. *International Journal of Research and Innovation in Social Science*, 9(4), 410–422. <https://doi.org/10.47772/IJRISS.2025.90400033>

- Impola, J. (2024). European credit transfer and accumulation system as a time-based predictor of student workload. *Higher Education Research & Development*, 44(2), 417–430. <https://doi.org/10.1080/07294360.2024.2406490>
- Ismail, S. (2024). PERSONAL DATA PROTECTION POLICY: ENSURING EFFECTIVE IMPLEMENTATION OF DATA PRIVACY POLICIES IN PRIVATE HIGHER INSTITUTIONS. *International Journal of Law, Government and Communication*, 9(35), 45–55. <https://doi.org/10.35631/ijlgc.935005>
- Jones, K. M. L., & VanScoy, A. (2019). The syllabus as a student privacy document in an age of learning analytics. *Journal of Documentation*, 75(6), 1333–1355. <https://doi.org/10.1108/jd-12-2018-0202>
- Kebande, V. R., Karie, N. M., & Ikuesan, R. A. (2020). Real-time monitoring as a supplementary security component of vigilantism in modern network environments. *International Journal of Information Technology*, 13(1), 5–17. Retrieved from <https://link.springer.com/article/10.1007/s41870-020-00585-8>
- Krishnarajan, S., & Rengarajan, A. (2024). Surveying Authentication and Authorization Mechanisms in Today's Web Technology Landscape. *International Journal of Innovative Research in Computer and Communication Engineering*, 12(05), 6337–6340. <https://doi.org/10.15680/ijirccc.2024.1205198>
- Llanten-Lucio, Y.-I., Amador-Donado, S., & Marceles-Villalba, K. (2022). Validation of Cybersecurity Framework for Threat Mitigation. *Revista Facultad de Ingeniería*, 31(62), e14840. <https://doi.org/10.19053/01211129.v31.n62.2022.14840>
- Mehra, T. (2024). The Critical Role of Role-Based Access Control (RBAC) in securing backup, recovery, and storage systems. *International Journal of Science and Research Archive*, 13(1), 1192–1194. <https://doi.org/10.30574/ijrsra.2024.13.1.1733>
- Inam, M. A., Chen, Y., Goyal, A., Liu, J., Mink, J., Michael, N., Gaur, S., Bates, A., & Hassan, W. U. (2023). *SoK: History is a Vast Early Warning System: Auditing the Provenance of System Intrusions*. <https://doi.org/10.1109/sp46215.2023.10179405>
- Neeli, S. S. S. (2025). A Hands-On Guide to Data Integrity and Privacy for Database Administrators. *International Journal of Scientific Research in Engineering and Management*, 9(1), 1–6. <https://doi.org/10.55041/ijrsrem16443>
- Pollard, E., Hadjivassiliou, K., Swift, S., & Green, M. (2017). *Credit transfer in higher education: A review of the literature*. Department for Education. https://dera.ioe.ac.uk/id/eprint/28446/1/Credit_transfer_in_Higher_Education.pdf
- Ramim, M., & Levy, Y. (2006). Securing E-Learning Systems. *Journal of Cases on Information Technology*, 8(4), 24–34. <https://doi.org/10.4018/jcit.2006100103>
- Shah, M. H., & Panchal, M. (2022, May 1). Theoretical Evaluation of Securing Modules for Educational Chatbot. <https://doi.org/10.1109/ICICCS53718.2022.9788120>
- Shah, R., & Correia, S. (2021). Encryption of Data over HTTP (Hypertext Transfer Protocol)/HTTPS (Hypertext Transfer Protocol Secure) Requests for Secure Data transfers over the Internet. *2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT)*. <https://doi.org/10.1109/rteict52294.2021.9573978>
- Simha, R. K., H K, R., Prabhu, A., & Joshi, P. (2025). Beyond passwords: A multi-factor authentication approach for robust digital security. *Internet Technology Letters*, 8(2). <https://doi.org/10.1002/itl2.555>
- Singh, S., Kumar, M., & Das, S. (2013). An Efficient Model for Securing Identity Access in Scalable System. *International Journal of Computer Applications*, 70(5), 26–30. <https://doi.org/10.5120/11959-7793>

- Strack, H., Gollnick, M., Karius, S., Lips, M., Wefel, S., Altschaffel, R., ... Arn Waßmann. (2022). Digitization of (Higher) Education Processes: Innovations, Security and Standards. *EPiC Series in Computing*, 86, 22–29. <https://doi.org/10.29007/rrg4>
- Tarchila, P. (2021). PROTECTION OF PERSONAL DATA FOR INDIVIDUALS ON THE TERRITORY OF THE UNION OF EUROPE. *International Journal of Legal and Social Order*, 1(1). <https://doi.org/10.55516/ijlso.v1i1.41>
- Trofymenko, O., Loginova, N., Serhii, M., & Dubovoi, Y. (2022). CYBERTHREATS IN HIGHER EDUCATION. *Cybersecurity: Education, Science, Technique*, 4(16), 76–84. <https://doi.org/10.28925/2663-4023.2022.16.7684>
- Tyshyk, I. (2024). IMPLEMENTATION OF DATABASE SECURITY BASED ON ORACLE AUDIT VAULT AND DATABASE FIREWALL. *Cybersecurity: Education, Science, Technique*, 2(26), 56–70. <https://doi.org/10.28925/2663-4023.2024.26.666>