Volume 5, Issue 2
e-ISSN: 2716-666X

The Asian Journal of Professional and Business Studies

Please cite this article as: 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), 73–85. https://doi.org/10.61688/ajpbs.v6i2.422

ENHANCING SECURITY AND PRIVACY IN CREDIT TRANSFER APPLICATION SYSTEMS: A PROPOSED FRAMEWORK

Farah Farzana Abdul Aziz[1]*, Raznida Isa[2], Noraliza Azizan[3], Noornajwa Md Amin[4], Noorshamshillah Kamarzaman[5], & Siti Fajar Jalal[6]

[1,2,3,4,5&6]Faculty of Computing & Multimedia, Universiti Poly-Tech Malaysia, Malaysia

Corresponding author: farah_aziz@uptm.edu.my
Received 20 June 2025, Accepted 1 November 2025, Available online 30 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 current security vulnerabilities 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 expected to strengthen system access control, improve user accountability, enhance data privacy, and facilitate alignment with Malaysia's Personal Data Protection Act (PDPA). This study presents a practical and scalable security solution that can guide future system enhancements and deployment, providing a strong foundation for safeguarding academic data and supporting potential cross-institutional credit transfer initiatives. Additionally, the framework contributes to improving institutional credibility, ensuring data protection best practices and promoting digital transformation in academic processes in higher education.

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

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 transfer from one program, institution and university to another in supporting undertakings like 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 the utilisation of technology to accelerate the process, minimise errors and maintain consistency. Utilisation of automation without security controls, however, leaves institutions with huge vulnerabilities (Al-Slais & Ali, 2023). Breach of students' academic records, alteration of credit transfer decisions and unauthorised disclosure of student confidential data can drastically compromise the integrity of the system as well as erode stakeholders' confidence (Ashwani Goyal, 2024).

In Universiti Poly-Tech Malaysia (UPTM), the prototype of CTAS was developed as part of the digitalisation process in the institution towards the automation of credit assessment procedures. While the system effectively corrects for the majority of inefficiencies in operations, it has yet to incorporate key security features such as user authentication mechanisms, role-based access control, secure communication protocols and encrypted data storage. Loopholes such as these are structural weaknesses that expose the system to hostile intrusion, data corruption and possible breaches with catastrophic results.

Their absence not only jeopardises institutional data but also institutional compliance with Malaysia's Personal Data Protection Act (PDPA), which mandates high-level protection when processing personal data. In the case of credit transfer, where student identity, academic history and detailed syllabi are being processed, system insecurity can invite legal, image and operational sanctions against the institution (Ramim & Levy, 2006).

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 login of users, role-based access, secured communication channels and database security measures. The aim is the development of a robust system, not only addressing the current vulnerabilities but also with future scalability, inter-system integration and possible cross-institutional integration.

By integrating security as the core element, this study shall deliver an empowered solution, such as best practices in educational technology and e-governance (Singh, Kumar, & Das, 2013). The suggested framework will promote institutional readiness, develop users' confidence and provide 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 in an existing prior academic programme to a new one within the same institution or to a different university, frequently across borders. Cross-national systems like the European Credit Transfer and Accumulation System (ECTS) and the ASEAN Credit Transfer System (ACTS) are used far and wide for credit assessment and standardisation of recognition (Impola, 2024). Digital technologies in credit transfer systems are being popularly used, as they promise to minimise the burden of manual work and enhance processing time.

Nonetheless, even in the wake of increased automation, institutions still use fragmented or half-automated systems subject to errors, human judgment and inaccuracies. Research by Chandrasekaran and Mago (2022) indicates that credit transfer decisions are not transparent, especially where there is manual comparison of syllabi and learning outcomes. This has necessitated the need for high-quality, standardised and secure systems that may be capable of handling the increased number of academic mobility as well as protecting student data.

Although the fundamental emphasis of credit transfer systems has consistently remained on accumulating academic equivalency judgments, research highlights that security issues have often been left behind. According to Pollard, Hadjivassiliou and Swift (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 valuable sensitive data, such as student identities, personal data, academic records, financial information and proprietary research. Trofymenko, Loginova, Serhii and Dubovoil (2022) carried out an extensive survey on security concerns in academic setups and demonstrated that the majority of university systems had no integrated security controls, exposing them to data theft, phishing, and system compromise.

Within the context of credit transfer system applications, a lack of security features such as encrypted communications, authenticated and role-based access, substantially elevates the exposure of the system 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 have a tendency to store full course syllabi, student transcripts and histories of approvals, which are extremely sensitive in nature (Jones & VanScoy, 2019).

With no well-organised security system, not only do institutions suffer data breaches, but they also lose academic integrity, whereby unauthorised parties can alter credit decisions. As cyberattacks evolve, education systems that lack cutting-edge security measures become more vulnerable to being manipulated.

2.3 Authentication and Authorisation in Web Applications

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

Role-Based Access Control (RBAC) has been well propagandised in the literature as a strong method for handling user authorisation in educational systems. RBAC, as Destini and Tony (2024) have argued, makes access management easier through the allocation of well-defined roles like administrator, coordinator and student with predefined rights to access. The study reduces the chances of privilege abuse and allocates sensitive system processes to only competent individuals.

In addition, Multi-Factor Authentication (MFA) is more and more advised to aid security, especially for systems handling high-risk information. MFA compels users to enter two or more proofs of identity, for example, passwords and one-time passcodes or biometric verification. Research has time and again demonstrated that MFA diminishes the brute-force attack success rate and unauthorised access considerably (Singh, Kumar, & Das, 2013). In the event of a request for credit transfer, both RBAC and MFA being integrated would enhance the defence system in the system with layered security, countering present-day cybersecurity risks.

2.4 Data Protection Regulations in Higher Education

It is not only an option but a statutory requirement that local and overseas educational institutions must comply with local and overseas data protection legislation. In Malaysia, personal data is regulated by the Personal Data Protection Act (PDPA) 2010 and this regulates the processing, collection and storage of personal data, making sure data users, including universities, are accountable for protecting the information they use (Hamin, Saslina Kamaruddin, Noh, Othman, &

Mohamad, 2025). Institutions that do not respect these provisions can face severe legal sanctions, heavy fines, and reputational damage, potentially leading to the loss of public confidence and institutional legitimacy.

At the broadest level, the strongest and best-known data protection statute in the world is the General Data Protection Regulation (GDPR). Having been applied throughout the whole European Union (EU) in May 2018, the GDPR seeks to safeguard people's private data as well as their privacy by imposing stringent regulations on how companies handle, utilize, store and transfer personal data (Tarchila, 2021). GDPR requires organisations to get the consent of individuals in a clear way before processing their personal information, in order to implement data minimisation and exercise the right of individuals to see, correct, or erase their information.

Although GDPR is a regional regulation, it has global impacts in the sense that most of the non-European institutions, such as Asian educational institutions, are required to adhere to its standards when dealing with the personal information of EU citizens or when they are dealing with EU-based entities. This has prompted increasingly more education systems globally to embrace GDPR principles to enhance international partnerships and schemes for student mobility (Halawi & Makwana, 2023).

In applications for per se credit transfer, PDPA compliance is paramount. It means that all students' personal data are collected lawfully, held securely and transmitted in a secure manner. Infringement of institutional policy by unauthorized access, loss of data or corruption of data not only violates institutional policy but also trespasses directly over the PDPA and subjects the institution to legal punishment (Ismail, 2024).

In order 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 workflow and architecture, not as an added feature after it's developed. 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 to protect sensitive student data, uphold institutional accountability, and create user trust in the system (Dr. Pradeep Kumar Tiwari, 2025). Credit transfer applications that incorporate these privacy and security controls are not just effective in their operations, but they are also a reflection of regulatory accountability and conformity with ethical data handling practices. With such high levels of security, it assists in the protection of the integrity of academic qualifications, facilitates student mobility and renders institutions reliable partners 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. Alaattin Burak Bekmezci, Cigdem Eris and Pinar Sarisaray Boluk (2018) suggest a multi-layered security model that includes the secure authentication of users, the storage of data through encryption and encrypted communication channels via Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. These protocols help ensure that data exchanged over the internet is safe from eavesdropping and tampering.

Also included in a secure architecture are 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 contribute to security through instant detection and response to threats.

Confidential database management is equally important. Encryption of sensitive information while in storage guarantees that even when storage media are compromised, the information is still unusable without the relevant decryption keys (Neeli,

2025). Backup procedures, disaster recovery and regular vulnerability scanning need to be integrated into the system's security lifecycle as well.

In conclusion, literature heavily favors the integration of elaborate 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 system sustainability in the long term.

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, which are Requirement Analysis, Framework Design and Planning for Validation. The phases have been thoroughly discussed to ensure that the recommended security architecture eliminates the system's weaknesses identified, complies with data protection needs and allows for future system extension without compromise in usability.

3.1 Requirement Analysis

The initial part of the methodology is identifying the security weaknesses of the existing prototype of the CTAS. The design of the system, working procedure and security weaknesses were comprehensively analyzed. At the top of its issues were poor verification of the user, protection against access, secure transmission of data and safeguarding data storage.

There was a need for the system to be defined on how it would enforce user authentication processes that would grant access only to authorised users. Without user authentication, the system would be open to unauthorised use. Additionally, without the use of RBAC, users would be able to view functions outside of their area of work, and this would expose sensitive academic information to the general public (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 necessity of protecting sensitive academic data such as student records and transcripts by encrypting the latter during storage in the database to avoid being victims of 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 in order to permit traceability and auditing of the system in the future. Malaysian policy and Malaysia's Personal Data Protection Act (PDPA) were long quoted to ensure that the framework being constructed was completely in line with national data protection procedure and law (Muhammad Adil Inam et al., 2023).

The security requirements of this phase are as follows, which to use encrypted user authentication with MFA as a capability, for instances, role-based access control to manage user permissions, securing communications via HTTPS with SSL/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 rigorously designed to blend with the current CTAS workflow without compromising system usability or performance. The suggested security architecture adds a user authentication module that mandates secure login processes. The passwords of users 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.

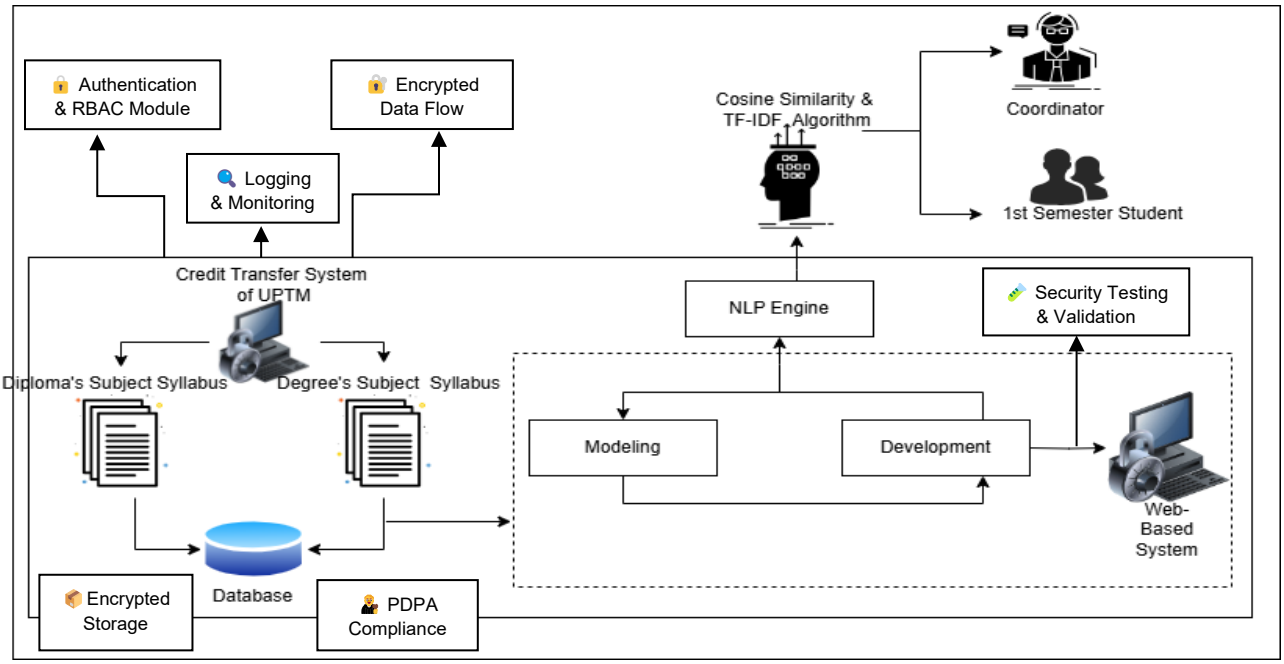
The design includes RBAC to provide for system access based on roles. Administrators will have unlimited access to operate users and view audit trails. Program coordinators will have limited access to credit evaluation and approval functionality and students will have access only to enter and monitor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

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

Design also comprises an extensive audit trail and logging subsystem for tracking all important user activity, like 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 thoughtfully designed to harmoniously adapt 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 suggests a security framework for the CTAS, a plan for validation 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, Amador-Donado, & Marceles-Villalba, 2022).

The validation plan described herein is designed to make sure that all the key aspects of security will be rigorously tested by simulation, penetration attempts, performance testing, compliance testing, and user acceptance testing. All of these elements are developed with great care to make susre that the proposed system not only enhances system security but also

preserves user satisfaction and complies with institutional policy and national law. 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 the development and proposal of a secure framework for the CTAS at UPTM. The findings of this research are derived from the system requirement analysis and framework design, supported by a well-structured validation plan for future testing. As the proposed framework has not yet been implemented in the live system, the findings presented here are conceptual, focusing on the expected benefits and improvements once the framework is deployed.

4.1 Identified Security Gaps

The analysis requirement on the current prototype of the CTAS at UPTM revealed some crucial security weaknesses that would seriously jeopardise the confidentiality, integrity and availability of academic information. The most critical flaw is the absence of user authentication. In the absence of authentication, users can never be certain of their identity when accessing the system. This implies that unauthorised users would be granted unrestricted access to the system and this would be a serious security risk by allowing malicious users to modify, erase or steal confidential information.

Other than this, the existing CTAS does not use RBAC. With no RBAC, everyone will have equal levels of access irrespective of their role or duty within the system. This uncontrolled access greatly enhances the danger of data exposure as accredited users who are given access to simple functions, like students, can intentionally or unintentionally read, modify, or erase confidential data, such as 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. At present, information being exchanged between the system server and the user's browser is not encrypted and hence can be easily intercepted by hackers. This creates a platform for man-in-the-middle (MITM) attacks, where a hacker intercepts and also tampers with sensitive data such as usernames, passwords, student transcripts and application information while in transit (Almakdi & Alshehri, 2023). Interception of such data can seriously disrupt the integrity and privacy of student data.

In addition, academic material within the database of the system is not encrypted. Keeping sensitive information such as students' personal data, course syllabi and academic records in plaintext significantly increases the risk of data theft in case of a system breach. With no encryption, if an unauthorised user accesses the database, it would be an easy extraction and exploitation of the information contained, 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. Lacking accountability to users, it is not known with certainty who performed specific actions within the system and this erodes the institution's ability to enforce security policies and respond to potential violations effectively.

In totality, all these security vulnerabilities cumulatively make the CTAS vulnerable to high threats of data leakage, system abuse and non-compliance with data protection laws like Malaysia's PDPA. Any remedy to such weaknesses is paramount to protecting students' data, ensuring system integrity, and upholding institutional reputation.

4.2 Proposed Security Enhancements

For the efficient addressing of the main security vulnerabilities presented in the existing prototype of the CTAS, 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 ensuring system usability and regulatory compliance.

The user authentication module is the centre of the proposed changes, protecting the system from unauthorised use by approved users. This module implements industry-standard password hashing algorithms, such as bcrypt, to securely store the user passwords. The algorithms convert the plain-text passwords into irreversible one-way hash values and make it computationally costly for the attackers to obtain the original passwords even if the database is compromised. To provide user authentication with an added layer of strength, MFA steps in. MFA mandates users to enter a second level of authentication, like one-time password (OTP) or biometric information, following the entry of 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, any user will be accorded 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 halfway access to functions involving credit assessment and approval, whereas students will receive access to apply for credit transfers and see their application status only. By isolating the privileges of user access based on their role, RBAC greatly reduces the possibility of unauthorized data alteration and guards critical system operations against the wrong user groups' access (Mehra, 2024).

The architecture also includes secure communication protocols for encrypting data in transit between users and the system server. All system communication is mandated using the HTTPS protocol, protected by SSL/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 the data transfer, especially when dealing with sensitive data like records of students and login passwords (Chordiya, Majumder, & Javaid, 2018).

Aside from protecting sensitive data in transit, the system also protects sensitive data at rest by encrypting databases. All sensitive academic information, such as students' personal information, transcripts, course syllabi and credit transfer information, will be encrypted when stored in the database. This data-at-rest encryption renders the data stored unusable and unreadable even if unauthorised groups access the database.

In addition, the suggested framework contains a detailed logging and audit trail capability. 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 raises user responsibility by offering 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 will enable system administrators to recognise malicious activity and correct it instantly.

The architecture of the proposed security framework enables such security features to be integrated into the current CTAS process without impacting usability or performance of the system. The advancements are designed to impart strong protection while allowing a user-friendly environment and greater adoption of the system. With improved authentication, access control, secure communication, stored data encryption and traceability, the security framework designed forms 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 design of the framework has been done carefully in a way that there would be no disruption to system performance. Deployment and integration of controls like MFA, RBAC, encrypted media communication, encrypted storage of data and fine-grained audit logging have been designed with the greater goal of making sure that there would be a balance between system security and efficiency.

From a performance point of view, the implementation of industry-accepted password hashing algorithms, such as bcrypt, and the use of SSL/TLS encryption protocols are seen to offer good security at the cost of losing as little system response time as possible when fine-tuned. Equally so, MFA will only add a minimal 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 will be implemented so as to run in the background unobtrusively with minimal overhead processing in order to keep the system's responsiveness within acceptable limits.

User acceptance is also a primary factor in determining the success of any security improvement. The outlined security measure assumes that the users of the system, who are administrators, program coordinators and students, will appreciate the additional security features and not be as intrusive. Based on prior research in comparable systems, it is expected that users will accept the additional logon 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 scheduled user testing will evaluate the effect on the routine workflow of different user groups from the added security features, namely MFA and access controls. Feedback will be gathered to establish whether or not the system remains easy to use and whether or not the added security is seen as improving, as opposed to 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 confidentiality of data 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 ensure severe rigor scrutiny of system functionality, security robustness, performance efficiency, regulatory compliance and end-user satisfaction. These activities will be essential to ensuring that the intended framework achieves its desired security requirements while remaining pragmatic for institutional adoption.

The initial phase is System Simulation Testing, during which it will confirm the users' authentication and role-based access control. Different scenarios will be simulated so that every user role (program administrator, program coordinator, student) may use only the system functions applicable to their assigned privilege. Any unauthorized attempt must always be refused and system modules should be protected based on user role assignments.

The second procedure is Penetration Testing, which will mimic cyber-attack situations, such as brute-force password cracking attacks, unauthorized login attacks and MITM attacks on data transfer pipes. The system must be secure against these typical threats by rejecting password cracking, continually rejecting login attempts of unauthorized entry, and encapsulating data transfers in secure SSL/TLS-encrypted HTTPS tunnels.

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 to verify that the system is conforming to Malaysia's PDPA and institutional security policy will be carried out. An exhaustive checklist will be employed to verify that the system conforms to all regulatory aspects, such as data protection, user responsibility, access control, and privacy measures. The assessment will ensure that the security controls of the system enhance institutional and national compliance requirements.

The last testing and validation is User Acceptance Testing (UAT) via a TAM-based formal survey questionnaire. The questionnaire will be used by system administrators, program coordinators, and students in order to obtain feedback on the usability of the system, satisfaction with security features, and perceived trade-off between security and usability. The UAT would be an extremely significant component in establishing if the proposed security framework is in tune 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 only access system features based on their assigned roles. Unauthorised access is denied.
2	Penetration Testing	To ensure the system can resist brute-force attacks, unauthorized access, and data interception.	Simulate brute-force attacks, unauthorized 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.
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 like 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 security features are implemented.	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 guarantees that the suggested security system is effectively tested for technical validity, performance efficiency, legislative compliance and user acceptance before being deployed live.

5.0 CONCLUSION

This research has suggested a full security framework to counter the vital vulnerabilities that exist in the existing prototype of CTAS. Although the system is operationally viable in streamlining credit transfers, it currently lacks essential security features. These vulnerabilities make the system vulnerable to serious attacks such as intrusion, unauthorised access and data interception, and possible intrusions of sensitive academic information.

To seal these security loopholes, the new architecture introduces multi-level security controls aimed at improving 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. System simulation, penetration testing, performance testing, compliance with regulatory requirements, and user acceptance testing are part of the validation plan to ensure that the framework satisfies security, usability, and regulatory specifications.

The architecture detailed is a high-strength and high-extensibility security solution that will be capable of propelling future development within the CTAS and other education systems. It provides a firm foundation for the protection of academic data and allows for the future possibility of secure cross-institutional credit transfer processes. The future development will include the implementation of the architecture, field-testing validation work, and the inclusion of 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 data collection, analysis, and validation of the results.
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 research was conducted in accordance with the ethical standards of Universiti Poly-Tech Malaysia, and adhered to the principles outlined in the Declaration of Helsinki. Ethical approval was obtained from the [**Institutional Ethics Committee/Review Board**] under reference number [**Approval Number, if applicable**]. All participants were informed about the purpose of the study and provided written informed consent prior to participation. Participants' privacy and confidentiality were strictly maintained, and data collected were used solely for academic purposes.

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

Alaattin Burak Bekmezci, Cigdem Eris, & Pinar Sarisaray Boluk. (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

Ashwani Goyal. (2024). 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

Dr. Pradeep Kumar Tiwari. (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., Saslina Kamaruddin, Noh, M., 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*, *IX*(IV), 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, & A. Rengarajan. (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/ijircce.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/ijsra.2024.13.1.1733

Muhammad Adil Inam, Chen, Y., Goyal, A., Liu, J., Mink, J., Michael, N., … Wajih Ul Hassan. (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. *INTERANTIONAL JOURNAL of SCIENTIFIC RESEARCH in ENGINEERING and MANAGEMENT*, *09*(01), 1–6. https://doi.org/10.55041/ijsrem16443

Pollard, E., Hadjivassiliou, K., & Swift, S. (2017). *Credit Transfer in Higher Education A review of the literature Green - Institute for Employment Studies Acknowledgements*. Retrieved from 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. (2024). 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., & Dubovoil, 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