Scilight

Library, Information & Services
https://www.sciltp.com/journals/lis

Article

Exploring the Aids of Machine Learning and Artificial Intelligence for the Detection of Fraudulent Documents in University Admissions Databases: A Perspective from University Officers and IT Professionals

Jacky Tam, Apple H. C. Lam and Dickson K. W. Chiu *

Faculty of Education, The University of Hong Kong, Pokfulam, Hong Kong, China
* Correspondence: dicksonchiu@ieee.org

How To Cite: Tam, J; Lam, A.H.C; Chiu, D.K.W. Exploring the Aids of Machine Learning and Artificial Intelligence for the Detection of Fraudulent Documents in University Admissions Databases: A Perspective from University Officers and IT Professionals. *Library, Information & Services* **2025**, *1*(1), 2.

Received: 17 August 2025
Revised: 19 September 2025
Accepted: 30 October 2025
Published: 7 November 2025

Abstract: This research examines the vulnerabilities in current university admissions document verification processes and explores the potential application of machine learning (ML) and artificial intelligence (AI) in detecting fraudulent submissions. Drawing on ten semi-structured interviews with admissions staff from various Hong Kong higher education institutions, the study employed thematic analysis guided by the PEACE investigative interviewing framework and the Diffusion of Innovations theory. The findings reveal significant reliance on manual, inconsistent verification practices, frequent procedural loopholes, and a lack of standardized consequences for fraud. While AI adoption is currently minimal, participants demonstrated cautious optimism, viewing AI as a supportive tool for pattern recognition, efficiency enhancement, and fraud flagging—especially in high-volume document types such as language test results. Institutional challenges, such as limited technical infrastructure and staff resistance, were identified as barriers to implementation. This study proposes a phased strategy for AI integration and emphasizes the need for cross-institutional collaboration, standardized protocols, and proactive staff development. It offers original insights into how AI can complement existing work processes, address cultural and infrastructural barriers, and potentially lay a foundation for practical innovation in academic admissions fraud prevention.

Keywords: document fraud; university admissions; machine learning; artificial intelligence; verification practices; fraud detection; PEACE model; qualitative research; thematic analysis

1. Introduction

The integrity of university admissions processes hinges critically on robust document verification systems, which serve as the first line of defense against fraudulent submissions and ensure equitable access to educational opportunities. As globalization rapidly intensifies competition for the limited seats in higher education institutions on both national and global scales [1], the prevalence of fraudulent academic credentials that includes a combination of falsified transcripts, forged recommendation letters, and AI-generated application materials has surged alarmingly, with institutions in Hong Kong widely reporting a series of university students admitted to universities in Hong Kong found applying with fraudulent documents and qualification. A trend that began in the late 2010s has seen a significant increase in the 'staggering' network providing fake qualifications worldwide. For instance, in the UK, it has been reported that qualifications were sold to nurses and consultants [2]. This trend is

exacerbated by advancements in generative AI technologies, which enable sophisticated forgeries that bypass traditional verification methods, such as manually comparing physical documents or relying on subjective human scrutiny [3]. On the defensive side, machine learning (ML) and artificial intelligence (AI) have also emerged as transformative tools in fraud detection, offering scalable solutions to analyze document authenticity, detect anomalies in application patterns, and identify AI-generated text with increasing accuracy [3]. While some institutions have already adopted AI-powered verification tools, such as the S.A.F.E. platform and Amazon Fraud Detector, these systems often operate in isolation and lack integration with broader admissions workflows, making it challenging for them to adapt to evolving fraud methodologies.

Current practices remain heavily reliant on fragmented manual checks and outdated digital workflows, creating vulnerabilities that malicious actors exploit to submit fraudulent materials [4]. These gaps may persist due to several factors, including the lack of significant collaboration between institutions, limited adoption of adaptive AI models, and an overemphasis on reactive fraud mitigation rather than proactive prevention [5,6]. To some extent, it may also be a combination of all these factors.

Addressing these deficiencies, necessitated by the increasing prevalence of document forgery and misrepresentation in academic and professional credentials, requires a paradigm shift toward integrated, the development of a more advanced verification methodology that adopts more recent technology capable of analyzing multi-modal data (including text, images and metadata) while maintaining transparency and fairness in decision-making that is mobbing towards automation [3].

Thus, this research aims to explore the potential of such prerequisites. To correctly frame the research, two main research questions (RQs) are set up to guide the research:

RQ1: How do current document verification practices in university admissions create opportunities for fraudulent submissions?

RQ2: What are the perceptions of university staff regarding the potential of ML and AI technologies to enhance fraud detection in document databases?

They address two critical gaps: systemic vulnerabilities in manual verification processes and institutional readiness for the adoption of AI/ML. By understanding workflows across diverse university systems and staff perceptions of technological solutions, the study aims to establish a framework for modernizing fraud detection protocols while addressing implementation barriers at university admissions.

This investigation would make three pivotal contributions to document verification research and practice. Firstly, it identifies procedural weaknesses in current university admissions processes that enable fraudulent submissions, building on findings from digital transformation studies that highlight gaps in legacy systems and staff training. By examining verification workflows across institutions, the research aims to uncover how manual checks and fragmented digital tools create vulnerabilities in the rapidly growing high-volume admission cycles. Second, the study aims to investigate the potential impact of AI/ML integration on university admissions procedures. While these technological enhancements have strong potential for enhancing fraud detection, particularly in cases of forged transcripts and counterfeit recommendation letters, their implementation hinges on real-time validation against centralized databases [14]. It would be significant to gather insider perspectives from institutional staff to assess their readiness for this implementation. In addition, this study can also provide findings that carry significant policy implications for higher education governance. The research aims to provide evidence-based recommendations for interoperability standards. By aligning technological adoption with organizational culture and infrastructure capabilities, the results can inform sustainable implementation roadmaps for global universities.

Unlike existing research, which often focuses on technical ML capabilities, this study examines institutional readiness and procedural loopholes from the frontline staff's perspective. It focuses on diagnosing vulnerabilities in current verification practices through workflow analysis and fraud pattern identification, while assessing any possible human factors in technological adoption through semi-structured interviews. Through engaging admissions officers, IT specialists, and administrative staff, the research maps attitudes toward AI/ML tools and identifies their perspectives on the issue.

Specific objectives include:

- Assessment of document verification practices in university admissions
- Developing a taxonomy of document fraud techniques prevalent in academic admissions
- Conducting thematic analysis on admission staff and openness to AI adoption
- Proposing phased implementation strategies that address cultural resistance and infrastructure limitations

The scope of this research focuses on examining document verification processes within higher education institutions in Hong Kong. The study involves university staff who are explicitly selected, such as admissions officers and IT staff, who are involved in the admission process and face challenges related to fraudulent document submissions, as these individuals play critical roles in evaluating and verifying applicant documents. By focusing on these demographics, the research aims to gather insights from professionals directly involved in the admissions process, thereby enabling a comprehensive understanding of current practices and potential improvements. The geographical focus on Hong Kong is due to the limitation in available interviewees, which should allow the findings to be framed in a way that is relevant and applicable to the local context. This targeted approach will facilitate a more in-depth exploration of the implications of integrating machine learning and artificial intelligence technologies in the specific setting of Hong Kong's higher education landscape.

2. Literature Review

2.1. Artificial Intelligence and Machine Learning

The integration of data management techniques in university admissions processes has garnered significant attention in recent years. With the advent of generative AI tools like ChatGPT and, more recently, DeepSeek, there has been a notable trend toward transitioning from traditional data management approaches to the application of machine learning (ML) and artificial intelligence (AI) technologies.

Beyond Generative AI, extensive research on various new computer technologies has been conducted before their advent. For instance, Calvet Liñán and Juan Pérez [7] had explored the application of Education Data Mining (EDM) in Learning Analytics. Mengash [8] has also focused on the application of data management techniques and the adaptation of Artificial Neural Network methods to enhance admissions operations, demonstrating a foundational understanding of how data can influence decision-making in educational settings. As recently, Çela, et al. [9] also explored expanding the use of Machine Learning Internet of Things (IoT) adoption in education, highlighting key technological advancements and their data collection and analysis applications, while also points out the challenges, particularly in issues related to data privacy, upon integrating of IoT into education [9,10].

With the popularization of ML and generative AI tools, researchers have begun to explore their applications in higher education admissions administration. Alothman, et al. [11] presented a viable methodology to enhance university admission systems using machine learning techniques, namely deterministic algorithms, to improve efficiency and reliability in the application process. For instance, Van Busum and Fang [12] presented a case study to understand which variables are essential in Student Admissions; while in more technical aspects, Hollman and Krause [13] suggested the application of the Chi-Square Automatic Interaction Detection tool to analyze admissions data that admissions committees may use to analyze their admissions processes and outcomes. Zhao, Borelli, Martinez, Xue and Weiss [3] have also studied how far AI tools can be used to counter-detect AI-generated content.

2.2. Fraudulent Documents in University Admissions

Studies in fraudulent documents have been an ongoing topic of study; however, the academic field has lagged in its focus on this area, and it is evident that quality research on such a niche topic is limited.

A rare piece of academic writing showcases contributors from multiple countries, including scholars, professionals, and leaders, to address the topic of fake degrees and credential fraud [14]. The publication provides a comprehensive analysis of the prevalence and impact of credential fraud within academic institutions. Showcasing the Canadian Higher Education scene, it highlights the methods used by fraudsters to produce counterfeit degrees and the challenges universities face in detecting such forgeries using traditional verification practices. The authors emphasize the urgent need for adopting advanced technological solutions, such as digital authentication and AI-based verification systems, to safeguard academic integrity and maintain trust in higher education credentials.

One interesting point to note regarding this topic is that the mainstream media often sheds the spotlight on this problem by highlighting notable stories in the news at certain times. In contrast, the topic has been noticeably neglected by academic scholars, as evidenced by the lack of academic writings on this particular topic, as noted in the work by Eaton, Carmichael, and Pethrick [14]. As for Hong Kong, it is only after the surge of "fraudulent academic profile" found in The University of Hong Kong in mid-2024 that led to the subsequent media coverage and government attention locally [15–18].

2.3. Theoretical Frameworks

2.3.1. The PEACE Model

A strong focus on planning during interview training is empirically proven to enhance the quality of pre-interview planning [19]. As one of the modern interrogation model, PEACE, standing for Preparation and Planning, Engage and Explain, Account (subcategorized by Clarify and Challenge), Closure, and Evaluation, which was developed in England and Wales in 1992, represents a significant shift from traditional coercive interviewing techniques to a non-accusatory, information-gathering approach aimed at obtaining accurate, relevant, and complete accounts from interviewees, including suspects, witnesses, and victims [20,21]. This integration model encompasses the entire interview process, from before to during, and after the interaction.

Research shows that interviewers trained in the PEACE model use more open-ended questions, engage in greater rapport-building behaviors, and employ fewer coercive tactics compared to untrained interviewers, resulting in significantly more detailed and reliable information from interviewees [22,23]. The model integrates scientifically supported techniques, such as conversation management and "free recalling," tailored to different interview contexts, aiming to improve the quality of information elicited while minimizing risks like false confessions [23].

The PEACE interrogation model is widely recognized and adopted as the ideal practice in ethical interviewing, and is considered a successful alternative to accusatory interviewing; its use has since expanded to additional nations and organizations [24]. Continuous research and global adoption underscore its effectiveness and ethical superiority over traditional accusatory methods, promoting both improved investigative outcomes and respect for interviewee rights, particularly interviewers more likely to obtain comprehensive accounts or confessions from their interview subjects than denials or 'no comment' [22,25].

The PEACE model was initially developed for investigative interviewing but has been adapted in this study as both a methodological guide and a conceptual framework for fraud detection in admissions. Regarding the methodological guide, the PEACE model was directly utilized to structure interviews with admission officers. Its phases—Preparation and Planning, Engage and Explain, Account, Closure, and Evaluation—ensured systematic, transparent, and ethically sound data collection. This methodological alignment is why the model is prominently featured in the research design.

Beyond its methodological role, the structured approach of the PEACE model in handling uncertain or deceptive information parallels how AI could be integrated into admissions processes. Just as the model emphasizes careful preparation, systematic questioning, and critical evaluation in human-led investigations, it can also inform the design of structured, accountable, and transparent AI-assisted student verification processes in university admission offices. Specifically, the PEACE model was employed in this study to investigate how these offices can examine cases of students who may have falsified their educational qualifications with the aid of AI integration.

The model can be implemented in the AI-assisted verification process in the following ways. For example, the Preparation and Planning parallels the development of standardized AI-assisted protocols. The Account & Evaluation phase reflects a human-AI hybrid review process, where discrepancies flagged by the AI are critically assessed by staff. The Closure phase ensures clear documentation and communication of outcomes, which is crucial for supporting AI in maintaining consistency over time.

The PEACE model is deeply rooted in human interaction. This study attempted to extend the model as a structural and ethical analogue for AI deployment in admissions fraud detection. It enhances our understanding by highlighting that AI integration should not directly replace human judgment, but instead follow a structured, transparent, and reviewable process, similar to how investigators manage sensitive human interactions.

2.3.2. Diffusion of Innovations

Everett Rogers' Diffusion of Innovations Theory (DOI) is a foundational framework that explains how, why, and at what rate new ideas, technologies, or practices spread through social systems [26]. In his seminal work, particularly highlighted in his original 1962 publication "Diffusion of Innovations", Rogers defines an innovation as any object, idea, or practice perceived as new by individuals or groups, while diffusion refers to the process through which these innovations are communicated over time within a social system [26].

The theory posits that innovation adoption depends on five perceived attributes: relative advantage, compatibility, complexity, trialability, and observability [27]. Recent studies applying DOI to technological adoption in education and public administration reveal insights directly relevant to integrating ML/AI solutions for detecting fraudulent documents.

This theory has been widely applied across various disciplines, including public health, education, and knowledge management [29], as well as the adoption of technology, and remains a significant framework for

understanding the dynamics of innovation dissemination and the roles of communication networks and social change in facilitating this process. For instance, Handoko, et al. [28] apply Rogers' Diffusion of Innovation theory to auditor adoption of AI/ML, finding that relative advantage, compatibility, trialability, and observability significantly influence adoption, while complexity shows no significant effect, highlighting the role of perceived benefits and adaptability in professional technology uptake; while Abdalla, et al. [30] apply DOI to reveal that business and management students' ChatGPT adoption is driven by perceived relative advantage, compatibility, trialability, and observability, with positive attitudes mediating this relationship.

2.4. Challenges and Research Gap

Despite the increasing interest in applying machine learning (ML) and artificial intelligence (AI) technologies for detecting fraudulent documents in university admissions, several challenges and research gaps persist that warrant further investigation, which connect to the research questions of this study.

Existing verification methods are often fragmented and heavily reliant on manual checks, creating vulnerabilities that can be exploited for fraudulent submissions [14]. RQ1 seeks to explore how these traditional practices facilitate opportunities for fraud. However, there is a scarcity of empirical studies systematically analyzing specific weaknesses in verification workflows within higher education institutions. This gap limits the understanding of the mechanisms behind these practices, necessitating a thorough examination to identify critical failure points.

The literature reviewed for this topic indicates that institutions face significant challenges in adopting ML and AI technologies [3,11]. RQ2 aims to investigate university staff's perceptions of the potential of these technologies to enhance fraud detection. However, there is limited research on the human factors that influence technology acceptance, including staff training and institutional culture. Understanding these barriers is crucial for creating a supportive environment that fosters technological integration.

In addition, although literature exists on fraudulent documents in higher education, much remains anecdotal or case-based, with limited empirical research on the effectiveness of AI and ML in mitigating this issue [14], as well as the fact that many, if not most studies focus predominately on technical accuracy (e.g., AI model performance), while ignoring social or operational challenges like staff resistance and ethical transparency. This lack of rigorous analysis restricts insights into how these technologies can systematically enhance fraud detection. Further research is needed to evaluate the actual performance of ML and AI tools in real-world admissions scenarios.

It is also noteworthy that many existing works lack integration with structured investigative frameworks. Applying an ethical investigative framework, such as the PEACE model, as a two-way methodology—using the PEACE model in interviews and addressing its application in the research subject—would represent an innovative approach.

Addressing these challenges and research gaps is vital for understanding the complexities of document verification practices in university admissions and the potential of ML and AI technologies to enhance fraud detection. Thus, this study employs a qualitative thematic approach to understand staff perspectives, assess operational challenges, and explore phased, hybrid models for fraud detection. These insights should directly inform the development of a context-specific, scalable strategy, providing a critical foundation for the following methodology section.

3. Methodology

This study employs a qualitative research design to investigate the application of machine learning (ML) and artificial intelligence (AI) in detecting fraudulent documents in university admissions processes. The primary objective is to examine current document verification practices and assess staff perceptions on integrating ML and AI technologies to enhance fraud detection. Appendix A summarizes the interview questions and their objectives. The faculty-level ethics committee approved this research.

Participants were selected using purposive sampling, targeting university staff involved in the admissions process, such as admissions officers, as well as IT personnel with experience in handling document verifications (see Table 1). This approach ensures that individuals with relevant experience and expertise are included in the study, providing valuable insights into the admissions landscape.

Participants were chosen based on their professional experience in admissions, familiarity with document verification workflows, and potential exposure to discussions around the use of machine learning (ML) and artificial intelligence (AI) in fraud prevention.

The sample included a mix of admissions officers, administrative staff, and IT security analysts to ensure diverse perspectives on both operational and technical challenges. This approach seeks to gather participants' in-depth knowledge and context-rich insights that align with the research objectives.

Data were collected through voluntary semi-structured interviews, allowing for maximum flexibility in discussing topics while ensuring that key questions are systematically addressed. Each interview was conducted confidentially, either in person or via a secure online platform. No personally identifiable data was recorded or disclosed in this research. All data collected is used for research purposes only and can only be accessed by the researchers of this project. Any personal data collected is kept strictly confidential. Participants shall not be identified by name in any completed study report. These interviews will be transcribed, and the interview transcripts will be completely anonymous.

Table 1. Demographic Information of Interviewees.

	Role	Years of Experience	Institution Type	Work Location	Preference on How to Use ML and AI
P1	IT Lead at Administrative Office	3+ years	Public University	Hong Kong	AI for pattern recognition and cross-checking data inconsistencies
P2	Admissions Officer, with vast experience in different Public Universities	3+ years	Public University	Hong Kong	No direct preference stated, but openness to structured automation
P3	Admissions Officer, with experience in both Undergraduate and Postgraduate settings	5+ years	Public University	Hong Kong	Use AI to support repetitive checks and reduce human workload
P4	Executive Officer in an Academic Department	Not specified	Public University	Hong Kong	AI for fraud flagging and pre-screening applications
P5	Admissions Officer, with vast experience in different Public Universities	Not specified	Public University	Hong Kong	No preference mentioned explicitly
P6	Data Analyst/Consultant	Multi-projects	Private Sector	Hong Kong	Automation to handle volume; ensure speed without replacing staff judgment
P7	Admissions Officer, with vast experience in different Public Universities	Not specified	Public University	Hong Kong	No preference mentioned explicitly
P8	Admissions Officer	3+ years	Public University	Hong Kong	AI to improve early-stage detection; modular for document types like IELTS
P9	IT Auditor/Security Analyst	3+ years	Private Sector	Hong Kong	Flagging inconsistencies and support interview planning
P10	Admissions Officer	1.5 years	Public University	Hong Kong	AI to assist with heavy load and accuracy, not replace human analysis

Before the interviews, participants were well informed about the study's purpose, their rights, and the confidentiality of their responses. Informed consent was obtained from all participants before the interviews commenced. The Interview guide encompasses behavioral questions centered on the following themes, designed around a PEACE model approach in the interview to facilitate interviewees' engagement in the interview progressively [31]:

- Current practices in document verification
- Experience(s) related to handling fraudulent applications
- Perceptions of ML and AI technologies supporting fraud detection
- Concerns and barriers to the adoption of these technologies
- Success stories or challenges encountered in previous technology implementations

Following data collection, a thematic analysis was employed to identify patterns and themes within the interview data. This analytical approach can facilitate a deeper understanding of staff perceptions and practices related to document verification, as well as the potential role of ML and AI in enhancing fraud detection efforts. Having explored the methodological approach, the following section outlines the findings generated from the thematic analysis.

4. Research Findings

This section presents the findings of the study, organized by the two research questions. Themes and sub-themes emerged from in-depth interviews with ten admissions and compliance professionals in Hong Kong. Verbatim quotes are included to illustrate and support key points.

4.1. How do Current Document Verification Practices in University Admissions Create Opportunities for Fraudulent Submissions? (RQ1)

Table 2 summarizes the themes, sub-themes, and coding descriptions directly aligned with RQ1, which is detailed in this section.

Table 2. Thematic Table addressing RQ1.

Theme	Sub-Theme	Source Codes and Quotes	Coding Descriptions
Current Verification Practices	Verification Methods for Applicant Information	• "We try to find the website of that exam board and verify whether this school exists." (P3) • "We will contact the relevant secondary school or examination board to make sure that the student is studying…" (P2) • "Verify the documents via official websites… or by post…" (P5) • "We will read the transcript provided to see whether the personal particular data were in line with their information in the passport…" (P2) • "I pay attention to whether the official certificates can be provided…" (P5) • "We mainly check the documents from the applicants. We check their identity documents, their qualification certificates, and their transcripts." (P1) • "We focus on checking the transcript about the secondary level or post-secondary level…" (P1)	• Full Manual Verification methodology • Consult official platforms if available • Verify True Copies if no other resort • Institution and identity confirmation • Transcript authentication
	Transparent Engagement Strategy with Applicants	• "We don't want to create any unnecessary conflict... we adopt a more friendly and diplomatic tone..." (P1) • "We will explain very detail[ed]ly… what procedures that the applicants have to do…" (P3) • "List out the verification methods on the admission website." (P5) • "We verify… whether they're truly enrolled at the claimed institution." (P2) • "We will arrange an interview with them… to make sure the information they submit is correct." (P4) • "I would say the whole process is very confrontational." (P10)	• Applicant communication strategies; • Interviews and documentation clarifications • Use of friendly engagement, not hostile • Sometimes staff do have a confrontation process framing mindset
Challenges and Gaps in Existing Verification	Known Inconsistencies and Fraud Risk	• "They might claim to have taken an exam in a country, but records show the school does not exist." (P1) • "Sometimes… we find some fraudulent case[s] where the personal information does not match." (P2) • One suspicious case was a student taking the IELTS in Southeast Asian countries like Indonesia or Vietnam, despite being from Mainland China." (P3) • "Some students submit transcripts issued by agents, or through back channels that aren't officially certified." (P4) • "We found it very suspicious because there's no point for the students to go to America to take the test." (P2) • "I pay attention to whether the official certificates can be provided." (P5) • "There is a rising trend for applicants/agents to make use of the 'loophole' to cheat." (P6)	• Fraud risk indicators • Mismatched info • Fake institutions • Unusual testing locations • Unverifiable documents

Table 2. *Cont.*

Theme	Sub-Theme	Source Codes and Quotes	Coding Descriptions
	Institutional Constraints and Process Limitations	• "The problem is that it slows down the offer process." (P3) • "Changing such a model plays a tremendous human effort…" (P1) • "Colleagues' knowledge and experiences in case investigation are relatively limited." (P6) • "Our admissions work is highly time-sensitive…" (P4) • "No consequences or punishments are outlined in the model." (P2)	• Time/resource limitations • Incomplete fraud follow-up • Knowledge/training gaps in verification
Current Handling of Fraudulent Applications	Response and Documentation of Fraud Cases	• "We will send an email… the information he or she provided has a discrepancy." (P4) • "The applicants decided to withdraw their applications after they were questioned or asked to provide further documentation." (P3) • "We keep a record about potential fraudulent case[s]." (P2) • "We are building a database for departmental use only." (P4) • "Specific remarks would be made on the cases about the suspected fraudulent documents." (P8) • "We do have simple measures like Excel files… However, I do admit these records are not centralized and are scattered…" (P10)	• Internal reporting and documentation • Reliance on suspects' responses to Verification Checking Requests • Necessary follow-up actions • Offer rescission and applicant withdrawal

4.1.1. Manual and Inconsistent Verification Practices

A central finding from this study is the pervasive reliance on manual and inconsistent verification practices among Hong Kong university admissions staff. Participants described current workflows as heavily dependent on "eyeball checks," where staff visually examine applicant documents, including identity cards, academic transcripts, and standardized test certificates, without systematic technological support. As highlighted in the thematic table (Table 2) and echoed throughout interviews, this manual approach introduces substantial variability and vulnerability in fraud detection.

Multiple admissions officers interviewed emphasized that they are required to frequently cross-check details by referring to official examination boards or institutional websites when available. As one participant described this process, *"We try to find the website of that exam board and verify whether this school exists" (P3)*, highlighting the reliance on external verification instead of integrated internal systems. In situations where online verification is not feasible, staff resort to requesting true copies or third-party certified documents by post or email, as another participant noted, *"We verify with the certificate authorities* via *email or by post" (P5)*.

However, these processes are not entirely standardized among various institutions or even at times within departments of a single institution, leading to significant inconsistencies in verification rigor. The thoroughness of verification varies depending on staff experience, institutional policies, and the type of qualification submitted. Moreover, full manual verification often requires staff to rely on their personal judgment to evaluate document authenticity and detect discrepancies. This subjectivity was seen as both a strength and a major limitation; while experienced officers might detect subtle irregularities, it also opens opportunities for human error or bias. One participant summarized this succinctly: *"We mainly check the document from the applicants. We check their identity documents, their qualification certificates, and their transcripts" (P1)*, illustrating a process deeply rooted in manual scrutiny rather than technological assistance.

This fragmented approach contributes to procedural weaknesses that fraudulent applicants may exploit. For instance, mismatches in names, photos, or testing locations could be missed under time pressure or if less experienced staff are involved. The presentation content explicitly identifies such gaps as "common failure points" and points to the lack of proactive fraud detection mechanisms beyond reactionary document checking.

This aligns with findings by Eaton, Carmichael and Pethrick [14], which emphasize the importance of "creating awareness regarding the importance of checking education credentials to circumvent these services.", whilst also observing that "not all universities engage in a rigorous credential verification process as part of the admissions process."

That means such a heavy dependence on manual and inconsistent document verification practices not only strains resources but also exposes higher education institutions to an increased risk of fraud. These findings underscore the need for standardized, technology-supported verification protocols to reduce reliance on subjective human judgment and enhance overall procedural integrity.

4.1.2. Common Failure Points: Loopholes and Risk Triggers

A further theme identified relates to fraud risk triggers and procedural loopholes, which present a critical vulnerability within the current admissions verification mechanism. Participants shared a variety of specific indicators that raise suspicion during document checks, most of which rely heavily on individual staff judgment rather than systematic screening tools.

Common fraud triggers included mismatches in personal information, such as inconsistencies between applicant names, photos, or passport details and those provided in supporting documents. For instance, one participant noted, "*Sometimes… we find some fraudulent cases where the personal information does not match" (P2)*. Such discrepancies often serve as the initial signal prompting deeper investigation.

Another frequently cited red flag involves unexpected exam locations, especially when applicants take language proficiency or standardized tests in distant or unrelated countries. This was mentioned by multiple participants as a tactic potentially used to avoid strict local proctoring standards. As one participant described, *"One suspicious case was a student taking the IELTS in Southeast Asian countries like Indonesia or Vietnam, despite being from Mainland China" (P3).*

Beyond these individual triggers, participants highlighted systemic procedural loopholes that applicants could deliberately exploit. The lack of unified, centralized databases for cross-checking applicant records means that an individual rejected or flagged at one institution may reapply elsewhere without detection. As captured in various interviews with admissions staff, this issue is compounded by the absence of standardized policies for addressing fraud consequences, which allows applicants to withdraw their applications without penalty once challenged. This reactive rather than preventive approach not only delays fraud detection but potentially enables

serial fraudulent applications across different universities. This fragmentation echoes broader challenges described by Smith [32], who highlighted how uncoordinated reporting systems and siloed data limit the effectiveness of fraud prevention efforts and enable repeat offending.

Participants also shared concerns about applicants providing incomplete or selectively chosen supporting documents to divert attention from suspicious credentials. In some cases, staff described challenges in verifying documents from lesser-known or overseas institutions where verification channels are weak or nonexistent.

These triggers, whereas similarity are found in similar research in other disciplines [33,34], and loopholes demonstrates the ingenuity nature of applicants, be it on purpose or by accident and the urgent need for enhanced, systematic safeguards, and the fact that it creates an enormous volumes of unstructured data, frequently with natural ambiguity and errors as Al-Ghamdi and Alsubait [35] points out in their study. Strengthening these areas requires more than just extensive staff training and vigilance; it also involves developing shared fraud tracking systems and implementing more robust, standardized verification protocols.

4.1.3. Lack of Standardized Fraud Response: Gaps in Preventive Measures and Documentation Holdbacks

Another critical theme that emerged is the role of applicant engagement and process transparency in the document verification workflow. Participants generally agreed on the importance of maintaining a neutral, professional, and friendly tone when interacting with applicants, while at times also reflecting elements of the PEACE model, particularly during the engagement and account phases.

While some staff reported making conscious efforts to avoid an accusatory approach, this practice has not seen much standardization, and the level of transparency offered to applicants varies significantly across cases and institutions. Participants described engagement as being designed to encourage cooperation and honesty. For example, staff often clarify the purpose of additional document requests to avoid unnecessary conflict or misunderstanding.

One participant explained, *"We usually maintain a friendly and neutral tone so applicants feel comfortable clarifying doubts rather than becoming defensive" (P4).* This strategy is designed to foster a fair investigative environment and enable applicants to explain any inconsistencies that might otherwise be flagged as fraudulent.

However, interviews also revealed that transparency in process steps and outcomes is often lacking. Many institutions do not provide applicants with verdicts and instead inform them of the final decision (acceptance or rejection). This approach eliminates any opportunity for applicants to correct genuine errors or provide additional explanations, potentially undermining the fairness of the process. As one participant also highlighted, "*We do not communicate the findings to the applicant. We simply deliver the verdict…" (P10)*. Additionally, varying levels of communication detail between departments or individual staff members mean that applicants may receive inconsistent information about what is required and why, increasing the potential for confusion or inadvertent non-compliance.

Moreover, in situations where applicants decide to withdraw their applications after being challenged, there is virtually no follow-up to verify the reasons for withdrawal or to document it as a genuine attempt at fraud. This not only limits institutional learning but also allows applicants to reapply elsewhere without consequence. While many staff members strive to maintain friendly and fair interactions with applicants, the inconsistent application of transparent processes and limited formal communication of findings highlight significant gaps. Addressing these gaps is thus crucial in creating a robust and fair admissions verification system that supports both procedural integrity and applicant trust.

4.1.4. Institutional Constraints: Institution Variation and Documentation Holdbacks

A final theme under Research Question 1 involves institutional constraints, which significantly affect the effectiveness and thoroughness of document verification. Participants widely reported that severe time pressures and high application volumes force admissions teams to prioritize processing speed over deep, detailed checks. More than three participants have mentioned that, as one participant said, *"The main challenge is that our work is highly time sensitive"* (P3). The essence of fast decision-making reduces the opportunity to investigate potential fraud triggers thoroughly and increases reliance on surface-level checks.

There is also an apparent lack of standardized performance metrics, such as formal Key Performance Indicators (KPIs) for fraud detection efficiency or error rates. Participants acknowledged that while the ultimate goal is to prevent fraudulent admissions entirely, there is no established system to measure success or track false negatives and false positives. One participant particularly highlighted this by saying, "*We do not have any solid KPIs; our target is to make sure* zero *applicants with fraudulent documents can enroll in our university" (P10).*

Furthermore, some participants pointed out that applicants who withdraw after being challenged do not face formal consequences or follow-up investigations. This creates a loophole that undermines deterrence, and fraudulent individuals may reapply elsewhere undetected.

All these constraints—operational, procedural, and cultural—reinforce each other, creating an environment where document fraud can persist despite frontline staff vigilance. The lack of a structured, systematic support and formalized verification frameworks suggests a pressing need for comprehensive policy and technological reforms.

4.2. What are the Perceptions of University Staff Regarding the Potential of ML and AI Technologies to Enhance Fraud Detection in Document Databases? (RQ2)

Table 3 summarizes the themes, sub-themes, and coding descriptions directly aligned with RQ2, which is detailed in this section.

Table 3. Thematic Table addressing RQ2.

Theme	Sub-Theme	Source Codes and Quotes	Coding Descriptions
Perceptions: Benefits and Expectations of ML/AI	Anticipated Benefits of AI and Machine Learning	• "AI or machine learning tools would be very helpful instead of manual checking." (P5) • "I envision deploying ML for tasks like real-time anomaly detection, document verification, and risk scoring." (P7) • "AI can help us to verify the documentation." (P3) • "The professor in our department is trying to develop a machine learning system…" (P4) • "AI technologies might be used… random check and manual check would also be needed." (P8) • "We've modeled security risks using machine learning to anticipate potential access fraud." (P9)	• Efficiency • Anomaly detection • Speed • Human-AI integration hybird • Application of AI into handling standard tasks • ML applied to predict risk of future threats based on pattern training.
Challenges and Barriers to Implementation	Implementation Challenges and Institutional Readiness	• "It will be the resources related, because we receive a lot of different types of qualifications." (P3) • "Changing such a model plays a tremendous human effort…" (P1) • "The most difficult part of employing this model is the first part: Preparation and planning…" (P4) • "Challenges include scaling solutions for large datasets and ensuring privacy compliance." (P7) • "The error rate of the technologies in the verification processes." (P8) • "Bias and privacy concerns are serious, especially when you can't explain how the model arrived at its conclusion." (P9) • "Staff tend to have complacency over current workflows that there used to be." (P10)	• Lack of resources, trustworthy data, and preparation time • AI limitations • Concern about explainability of ML systems and biases in training data. • Privacy concerns • Some staff members prefer existing methods and are hesitant to change, as they are comfortable with the routine.

Table 3. *Cont.*

Theme	Sub-Theme	Source Codes and Quotes	Coding Descriptions
Conditions for Adoption	Current Status and Integration Strategies	• "AI technologies for document verification were not yet adopted by the University." (P8) • "I haven't taken formal AI/ML training, but I've actively applied machine learning in real-world projects." (P7) • "Whether the database is a trustworthy one because AI is continuing to learn…" (P4) • "Most institutions are still exploring or piloting AI/ML use." (Summary of various interviewees) • "Lack of performance KPIs in place to evaluate the verification process." (P4)	• Early-stage adoption • Pilot testing • Missing KPIs • Limited training • Trust issues and concerns

4.2.1. Cautious Optimism Toward AI Potential: Complementary Role of AI and Its Cautiousness

A major theme that emerged from Research Question 2 is the cautious optimism expressed by interviewees regarding the integration of AI and ML technologies into document verification workflows. While participants recognized the potential benefits of AI, they consistently emphasized the importance of maintaining a complementary balance between technological tools and human oversight.

Many participants described AI and ML as promising support tools for managing the growing volume of applications, automating repetitive screening tasks, and identifying subtle fraud patterns that may escape manual checks. One participant noted, *"AI technologies might be used… random check and manual check would also be needed." (P8)*, while another mentioned, *"AI can help us to verify the documentation." (P3)*

Another staff member highlighted AI's potential for early pattern recognition, which can help detect irregularities and inconsistencies at scale: *"I believe that AI is better at capturing patterns and thus enhancing accuracy in identifying fraudulent documents as well" (P10).* These perspectives underscore the perceived strengths of AI in processing large data sets quickly and systematically, providing an initial safety net for human evaluators, as well as a resource optimizer and supportive partner that allows admissions staff to focus on more nuanced and judgment-based tasks reflecting a hybrid vision of AI working alongside human experts, rather than replacing themselves outright.

In connection with the above point, notably, this optimism is tempered by significant caution. Many participants emphasized that AI tools should not be relied upon as final decision-makers due to concerns over accuracy, potential bias, and the complexity of certain application cases. Instead, they envisioned AI as a first-level filter, flagging potential risks to be examined in detail by experienced staff. This cautious stance underscores a profound awareness of the ethical and operational implications of fraud detection in higher education. Participants acknowledged the promise of AI while firmly advocating for a human-in-the-loop model to ensure fairness, accountability, and context-sensitive decision-making. Interestingly, such sentiment aligns with Guingrich and Graziano's [36] research, which concludes that people are willing to engage with AI but do not anthropomorphize or fully trust it, indicating measured optimism.

Overall, these findings present an apparent readiness for stakeholders to explore AI's capabilities—but only within a carefully controlled, complementary framework that preserves human judgment at the center of the admissions process.

4.2.2. Barriers to Adoption: Implementation Barriers and Primary Concerns

Despite expressing cautious optimism, participants also expressed several significant barriers that currently limit the adoption of AI and ML technologies in document fraud detection within admissions processes. These barriers span technical, operational, ethical, and cultural dimensions.

A central concern highlighted was skepticism about the reliability and accuracy of AI tools. Participants feared that algorithms might produce false positives, wrongly flagging genuine applications, or false negatives, allowing fraudulent documents to slip through undetected. As one participant noted, *"I personally feel uncertain whether the results generated from AI would be accurate enough to trust without human review" (P8)*. This skepticism underscores the staff's belief in the importance of maintaining a high level of human oversight, particularly in critical decisions that affect applicants' educational futures, and mirrors the skeptics on AI in various domains, including the finance sector [37].

Privacy and data security concerns were also commonly raised. Participants were wary of how sensitive applicant information would be processed and stored by AI systems. One participant shared, *"Bias and privacy concerns are serious, especially when you can't explain how the model arrived at its conclusion" (P9)*. This concern aligns with broader discussions around AI ethics and highlights the potential risk of damaging institutional trust if privacy safeguards are not clearly defined and communicated.

Operationally, many staff pointed to a lack of technical infrastructure as a major barrier, an exact mirroring of what Alothman, Alazmi, Ali, Alqallaf and Khan [11] identify. Existing data formats and diverse document types from various regions make it challenging to build standardized AI input pipelines. The complexity of global academic credential formats, such as the difference in verification methodology between English qualifications like TOEFL and IELTS, complicates integration and increases the risk of error.

Cultural resistance and staff complacency also play significant roles. Several participants noted that staff members are accustomed to traditional manual processes and may be resistant to learning or trusting new technological solutions. One participant even observed that they *"tend to have complacency over current workflows that they are used to" (P10)*. This entrenched comfort with familiar systems creates an invisible psychological and cultural barrier to adoption, even if technical solutions are made available.

It is also known for a general lack of formal policy frameworks and implementation guidelines to support AI adoption—a similar finding in the adoption of new technology in the public sector, such as immigration [38]. Without clear standard operating procedures and institution-wide training in the fraudulent document verification process, staff fear misinterpretation of AI results, and accountability issues may lead to errors in verdicts.

Combining all these concerns, these potential barriers highlight the challenge of integrating AI and ML into admissions fraud detection, alongside the necessity of multifaceted institutional transformation. Addressing these concerns requires comprehensive strategies that include technological investments, policy development, training programs, and cultural change initiatives to build trust and readiness across all levels of staff.

4.2.3. Readiness and Current Adoption Status

Addressing the concern that universities lack formal policy frameworks and implementation guidelines to support AI adoption, the final theme under Research Question 2 focuses on the readiness of universities and the current status of AI/ML adoption in university settings for document fraud detection. While participants expressed interest in exploring technological tools, their responses clearly indicated that actual implementation remains at an early conceptual stage.

Participants consistently noted a lack of technical infrastructure as a primary reason for the slow adoption of AI and ML. Many universities do not yet have integrated systems capable of supporting automated document verification. Data from applicants comes in diverse formats, often originating from different countries and credentialing authorities, which complicates standardization and hinders the development of reliable AI pipelines. As highlighted in the thematic table, the fragmented nature of document types makes it difficult to train and deploy AI models effectively.

As many interviewees pointed out, "Most institutions are still exploring or piloting AI/ML use." Most AI applications in university settings are limited to analytics or operational efficiency improvements, rather than direct fraud detection in admissions. One interview even points out that there is no valuable implementation in his experience. This illustrates that while universities may be open to AI solutions in general, fraud detection remains an unexplored application area due to perceived operational complexity and perceived risks.

Culturally, the complacent attitudes of the staff mentioned above also suggest an underlying hesitancy to change long-established workflows, as many are more comfortable relying on manual processes and individual judgment. Participants repeatedly stressed the importance of human oversight and the difficulty of trusting automated systems for such high-stakes decisions. This finding is consistent with a classic finding on resistance to technological innovations, which suggests that the level of satisfaction experienced with an existing behavior increases resistance to and reduces the likelihood of adopting an alternative [39].

Finally, the lack of formal institutional policies and strategic roadmaps was mentioned as a significant barrier to readiness. Throughout the research interviews, very few mentions were made of such roadmaps within the institution, suggesting a possible lack of initiative on the part of the institution itself. These barriers are consistent with the observations of Rogers [26] that complexity and lack of compatibility hinder adoption. Without clear guidance, there is uncertainty around accountability, data governance, and operational procedures, making staff reluctant to experiment with or champion AI initiatives.

Overall, while there are cautious interests and recognition of potential benefits, current organizational and technical conditions suggest that universities may not yet be ready for large-scale AI-driven fraud detection

systems. Consistent with findings from Zhao, Borelli, Martinez, Xue and Weiss [3] and Handoko et al. [28], who highlight that most universities remain in early exploration phases, hindered by unclear strategic frameworks, infrastructure gaps, and cultural hesitancy. Future efforts will need to address infrastructure, staff training, cultural mindset shifts, and policy frameworks to move from conceptual interest to practical implementation.

Finally and notably, the themes discussed in RQ2 are summarized in the thematic table provided at the end of this section. This table clearly presents the themes, sub-themes, and coding descriptions, which are aligned specifically with the research question, providing a comprehensive overview of participants' perceptions regarding the adoption of AI and ML in admissions fraud detection.

4.3. Additional Findings: Reflections on PEACE Model

Table 4 summarizes the themes, subthemes, and coding descriptions related to the PEACE model reflections, providing additional context for these supporting findings.

Table 4. Thematic Table addressing additional findings of the PEACE model.

Theme	Sub-Theme	Source Codes and Quotes	Coding Descriptions
Application of the PEACE Model in Document Verification and Fraud Investigation	Digital-Enabled PEACE Model Integration	• "We didn't use PEACE per se, but we did follow a framework involving digital data validation and structured report-back." (P9)	• Suggests enhancing PEACE steps with automation and structured reporting walkthroughs.
	Structured Preparation and Communication	• "The PEACE model is effective in finding fraudulent documents and improving communication with the applicants." (P5) • "It's far better than rushing through admissions without it… only to later discover that over half of the admitted students submitted fraudulent credentials." (P1) • "Engage applicant/representative to provide opportunities for necessary clarification." (P6)	• The PEACE model facilitates planning, engagement, and documentation, supporting clear, neutral, and systematic interactions with applicants.
	Challenges and Institutional Gaps	• "The most difficult part of employing this model will be the first part: Preparation and planning…" (P4) • "No consequences or punishments are outlined in the model." (P2) • "Collective action in sharing and recording potential/confirmed fraudulent cases." (P6)	• Admissions officers face implementation issues, including time pressure, a lack of training, and the absence of formal protocols for responding to fraud.

While not a core research question, insights related to the PEACE model emerged as a resourceful additional finding, providing further context to the study. The PEACE model was incorporated into this research in two complementary ways: it directly informed some interview questions and also guided the overall design of the interview instrument to ensure ethical, neutral, and structured discussions with participants.

Participants generally recognize the benefits of the PEACE model in promoting fairness and structured engagement during document verification. Many appreciated its emphasis on a neutral tone approach and providing applicants an opportunity to explain inconsistencies, aligning with the "Engage" and "Account" phases of the model. One participant described it as offering "a solid foundational structure" that helps admissions staff avoid confrontational approaches and maintain professionalism.

However, operational constraints of the PEACE model itself may limit its application. Time pressures and resource demands, such as admission exercises, mean that the later phases, particularly "Closure" and "Evaluation," are often abbreviated or omitted altogether. For example, investigation outcomes are not typically communicated in detail to applicants, and systematic post-case evaluations are rarely conducted.

A few participants also suggested that formal integration of PEACE principles into standard operating procedures could strengthen process consistency and improve staff confidence in handling complex cases.

Overall, these reflections underscore the importance of integrating ethical and structured frameworks, such as PEACE, alongside any technological or procedural changes. They suggest that while AI and ML can support efficiency and detection, human-centered frameworks remain critical to maintaining fairness and transparency in admissions investigations.

4.4. Summary of Findings

In summary, this study revealed significant vulnerabilities in current university document verification practices. A heavy reliance on manual and inconsistent checks, combined with operational constraints such as time pressure and a lack of standardized metrics, creates procedural gaps that fraudulent applicants can exploit. The absence of centralized fraud tracking and the informal handling of suspicious cases further weaken institutional safeguards. At the same time, staff efforts to maintain professional and neutral engagement with applicants, though positive, are undermined by inconsistent transparency and limited formal communication of investigation outcomes. Together, these findings highlight a system that is highly dependent on individual staff judgment and institutional culture, rather than guided by unified, robust frameworks or technological support.

Regarding the potential adoption of AI and ML, participants expressed cautious optimism, emphasizing their potential to enhance efficiency and detect subtle patterns of fraud. However, this optimism was tempered by significant barriers, including concerns about reliability, privacy, data governance, and cultural resistance to change. Institutional readiness remains low, with limited technical infrastructure, insufficient staff training, and a lack of formal policy frameworks to guide implementation. Additional reflections on the PEACE model reinforced the value of structured and fair investigative approaches, but also revealed practical limitations in fully integrating such frameworks. Overall, these findings suggest that while AI and structured models, such as PEACE, offer promise, successful fraud prevention in admissions will require a thoughtful, hybrid approach that strengthens existing human judgment with technological and procedural innovations [42]

5. Suggestions and Implications: The Way to Move Forward

The findings of this study highlight critical vulnerabilities in manual verification processes and a cautious yet optimistic attitude toward AI among university staff. To address these challenges and prepare for future readiness, this section proposes practical suggestions grounded in Rogers' Diffusion of Innovation (DOI) theory. According to Rogers, successful adoption of innovation depends on factors such as relative advantage, compatibility, complexity, trialability, and observability. The proposed actions below are strategically designed with these elements in mind to facilitate smoother institutional transitions [26].

5.1. Develop Standardized Verification Protocols

Establishing comprehensive, standardized verification protocols is an urgent priority. By creating a thematic framework for AI-assisted document verification that integrates AI/ML technologies, universities can improve fraud detection while maintaining clear human oversight. This approach emphasizes relative advantage (superior to fragmented manual checks) and compatibility with existing values around fairness and procedural integrity. Standardization also improves observability, allowing other institutions to see tangible benefits, as Zhao, Borelli, Martinez, Xue and Weiss [3] suggest in relation to the effectiveness of domain-specific AI detection tools in academic admissions, supporting the call for standardized AI-assisted protocols that both strengthen document authenticity checks and reduce manual burden.

5.2. Foster Institutional Collaboration

Strengthening cross-institutional collaboration will enable universities to share best practices, identify fraud patterns, and develop effective verification strategies. Creating a shared knowledge base enhances observability and reinforces collective learning. This not only builds trust among institutions but also encourages the faster diffusion of effective verification innovations throughout the sector through enhanced consistency and enabling proactive fraud detection [33].

5.3. The Framework to Move Forward

By implementing these suggestions in accordance with the key principles of Diffusion of Innovation theory, universities can transition from fragmented, manual processes towards a more integrated, hybrid verification system that blends human expertise with technological advancements. The successful implementation of such a

framework can not only strengthen institutional integrity and resilience to fraud but also promote a culture of shared learning and continuous improvement.

5.3.1. Pilot AI Implementation

A key first step involves piloting AI modules on specific, high-volume document types, such as IELTS test result sheets or standardized academic transcripts. As Bansal, et al. [40] suggest, adopting AI incrementally and combining it with human oversight enhances trust, allowing organizations to address behavioral variables during early adoption phases. By starting with documents that have relatively uniform formats and well-established verification channels, universities can safely test AI functionalities without risking widespread errors or compromising complex cases. This controlled trial environment aligns with the trialability factor emphasized in Rogers' Diffusion of Innovation theory, allowing staff and administrators to experiment with AI capabilities in a manageable scope. Piloting also supports iterative learning, as feedback can be collected to fine-tune AI models and develop best practices before scaling. It fosters a safe space for staff to build familiarity and trust with the technology, addressing fears around accuracy and reliability. Over time, these smaller-scale successes can be shared across institutions, strengthening observability and building momentum for broader adoption [26]. This gradual approach reduces resistance while laying a strong foundation for future system-wide transformation.

5.3.2. Human-AI Hybrid Review Process

Rather than replacing human judgment, the proposed framework emphasizes a hybrid human-AI review process, positioning AI as a supportive tool for initial screening rather than a final decision-maker. This design directly addresses concerns around complexity and compatibility, two central elements in Rogers' theory [26]. Many staff members interviewed value the niche and contextual understanding they bring to document evaluation —a perspective that AI systems currently cannot replicate. In a hybrid model, AI would rapidly flag potentially fraudulent or high-risk applications based on anomaly detection and pattern recognition, while final assessments—something described as the "kill switch"- remain with experienced admissions officers. Eaton, Carmichael and Pethrick [14] provide a similar caution: while technological tools like AI are promising, they must complement, rather than replace, human judgment to ensure ethical and accurate verification processes. This balance would not only preserve the human-centric values embedded in admissions processes but also improve operational efficiency by reducing manual workload at the initial review stage. This also aligns with Eaton et al. [14] suggestions to enable multiple verification points in the admissions workflow and to audit it regularly. Additionally, it supports Hollman and Krause's research on incremental adoption and testing of AI modules in educational admissions, although the application is scoped in alternative settings.

By framing AI as a complementary partner, institutions can minimize staff skepticism, reduce errors from human fatigue, and maintain fairness and accountability in decision-making. This dual-layer approach can also enhance public trust by demonstrating responsible and transparent use of AI.

5.3.3. Structured Approach (PEACE Model)

Incorporating the PEACE model as a formal component of verification processes provides a clear and structured approach to handling potentially fraudulent cases. The PEACE model's five key phases—Planning and Preparation, Engage and Explain, Account, Closure, and Evaluation—align naturally with the procedural needs of admissions fraud investigation [25]. Its emphasis on fairness and non-confrontational engagement reflects compatibility with existing institutional values while providing a relative advantage in standardizing staff practices. Additionally, when integrated into routine workflows, the PEACE model enables admissions staff to maintain a high level of consistency in their communication with applicants, the gathering of supporting information, and the evaluation of outcomes. A structured approach aligns with the suggestion provided by Koenig and Devlin [41] to take a proactive, methodical, and consistent approach to document review.

Making the best use of this model also encourages ethical practice, fostering a culture of transparency and reducing the risk of subjective or biased judgments. Furthermore, by establishing clear, documented steps, the PEACE model helps alleviate ambiguity in decision-making processes and reinforces institutional credibility. As universities introduce AI, the PEACE model can serve as a human-centric role model framework to counterbalance the "cold-blooded" mechanical precision of algorithms with empathetic, fair treatment of applicants.

5.3.4. Promote Knowledge Sharing Culture

Promoting a cross-institutional knowledge-sharing culture is essential to strengthening sector-wide fraud prevention. Establishing a shared fraud knowledge base would allow universities to exchange verified cases, detection patterns, and best practices, improving overall system resilience. This approach supports observability in Rogers' Diffusion of Innovation theory, as successful strategies become visible and credible to other institutions [26].

By collaborating in the practice, universities can collectively reduce vulnerabilities to serial fraud attempts and learn from each other's experiences without duplicating efforts. Over time, fostering such a culture not only improves individual institutional safeguards but also builds trust and integrity across the entire higher education landscape.

5.3.5. Proactive Staff Development

Last but not least, investing in proactive staff development is critical to overcoming resistance and ensuring smooth AI integration. Institutions should initiate comprehensive training on AI ethics, technological literacy, and fraud detection, which empowers staff with the confidence and skills needed to adapt to hybrid verification processes, rather than estranging themselves from unfamiliar new methodologies. The success in doing so directly addresses the complexity and enhances trialability, two important adoption factors in Rogers' framework. Focused development reassures staff that technology serves as a supportive tool, not a replacement, reinforcing their professional value. Well-prepared staff can more effectively collaborate, interpret AI outputs, and uphold fairness, ultimately supporting a responsible and transparent admissions environment, aligning with the findings from Bansal, Paliwal and Singh [40]

6. Conclusion & Limitations

This research has attempt to capture the essence of how current document verification practices in university admissions create opportunities for fraudulent submissions, at the same time seek the perceptions of university staff regarding the potential of ML and AI technologies to enhance fraud detection through qualitative research guided by the PEACE as both an investigative and structural tool, the study conducted a thematic analysis to capture a grounded understanding of the issues at hand.

The findings revealed several recurring problems in existing practices, including the continued dependence on manual verification methods, inconsistencies between departments, procedural loopholes that applicants may exploit, and the lack of a standardized fraud response mechanism. Although current implementation of AI tools remains minimal, participants expressed cautious optimism about AI's potential benefits, particularly in tasks involving pattern recognition and workload redistribution. However, concerns were also raised regarding privacy, explainability, and system reliability.

To address these challenges, the study proposes a set of forward-looking suggestions grounded in both empirical findings and the Diffusion of Innovation framework. These include establishing standardized verification protocols, encouraging inter-institutional collaboration, piloting AI tools on selected document types, and fostering staff training and knowledge sharing. Overall, the research offers timely insights into both the structural constraints and the emerging opportunities for AI-enhanced document verification in higher education admissions.

Despite the insights gained, this research remains a subject of limitations. First, the participant sample was limited to admissions officers, IT staff, and consultants with experience in Hong Kong's higher education sector, as the university admissions sector is relatively smaller compared to other industries, such as marketing or services, in Hong Kong. Besides, the data from these interviewees were collected through semi-structured interviews that relied on self-reported experiences and perspectives. This approach may introduce bias, as participants might consciously or unconsciously underreport challenges or overemphasize procedural strengths due to the nature of the qualitative interviews [42]. Notably, the ever-evolving development of AI and ML technologies presents the opportunity for increasingly sophisticated document fraud techniques, meaning that the findings may potentially represent only a snapshot in time.

Despite the limitations mentioned above, as the AI-integrated fraud detection processes for university admissions have not yet been widely explored, particularly in the context of Hong Kong, this study could contribute to the literature by delving into the AI integration and assistance in fraud detection for university admissions. This qualitative study's findings may shed light on how to integrate AI in assisting the admissions process, particularly in detecting fraud, for academic researchers and practitioners in the context of Hong Kong, an international city with several globally renowned comprehensive universities.

To generalize this study's findings, future research could quantitatively survey the effectiveness of AI-integrated fraud detection processes and performances in different contexts, such as different regions or types of institutions, from the perspectives of admissions officers and IT professionals. Mixed-methods research could also

be conducted to further ensure the reliability and validity of the research data through triangulation. Furthermore, future research should continually re-evaluate these practices as technologies and fraud patterns evolve.

Looking forward, this study provides a foundational exploration of the challenges and opportunities associated with integrating AI and ML into fraud detection processes in higher education admissions.

Author Contributions

Conceptualization, Methodology, Investigation: all authors; Validation, Supervision, D.C. and A.L.; Formal analysis, J.T.; Data curation, J.T. and D.C; Writing—original draft, J.T.; Writing—review & editing, D.C. and A.L.; Project administration, D.C. All authors have read and agreed to the published version of the manuscript.

Funding

This research received no external funding.

Institutional Review Board Statement

The study was conducted according to the guidelines of the Declaration of Helsinki, and approved by the Ethics Committee of Faculty of Education, The University of Hong Kong (30 April 2025.)

Informed Consent Statement

Informed consent was obtained from all subjects involved in the study.

Data Availability Statement

Data are available on reasonable request to the corresponding author.

Conflicts of Interest

The authors declare no conflict of interest.

Use of AI and AI-assisted Technologies

Grammarly was used for the language polishing for this article.

Appendix A. Interview Instrument

Table A1. Brief Description of Interview Instrument.

Interview Questions	Research Objective Alignment
0. Demographics and Backgrounds	
Age, Gender, Education (level, major, minor) Any formal/informal training related to AI/ML?	
What is your current position or role within the institution?	To understand the background and context of the interviewee's responses regarding fraud detection practices.
How many years have you worked in your current role or in the admissions process?	To establish the interviewee's experience level, which may influence their perspectives on document verification and fraud detection.
What type of institution do you work for? (e.g., public university, private university, community college)	To categorize responses based on institutional type, which may affect verification practices and fraud detection approaches.
1. Preparation and Planning	
Preparation Practices	
How does your office plan to avoid false applicant information? How do you prepare for that?	To assess current practices in document verification and identify gaps or weaknesses in existing strategies.
Particularly, which information do you pay the most attention to? How and why?	To understand critical areas of focus in the verification process and inform potential improvements or technology applications.

Table A1. *Cont.*

Interview Questions	Research Objective Alignment
2. Engage and Explain	
Engagement Techniques	
When engaging with applicants or their representatives, what strategies do you use to build rapport and explain the verification process?	To explore how staff interact with applicants, which may impact the effectiveness of fraud detection efforts.
3. Account	
Gathering Accounts	
Can you describe a situation where you had to investigate a potentially fraudulent application? How did you approach gathering information from the applicant?	To gain insights into real-life experiences of fraud investigations and to identify effective practices.
Evaluating Responses	
How do you assess the credibility of applicants' information during the verification process? What specific indicators do you look for? Why?	To identify criteria used in assessing information credibility, which may inform the development of AI/ML tools for fraud detection.
Utilization of ML/AI	
Have you considered using machine learning or artificial intelligence tools in your investigations? If so, how do you envision these technologies being deployed into your current processes?	To explore perceptions of ML and AI technologies and their potential integration in fraud detection practices.
Concerns and Barriers	
What concerns do you have regarding the adoption of ML and AI technologies for fraud detection? What barriers (e.g., technical, ethical, or resource-related) do you anticipate to be addressed?	To identify potential obstacles to implementing new technologies in fraud detection, which can guide future research or recommendations.
Success/Failure Stories (if any)	
Have you encountered successful/unsuccessful technology implementations, such as ML or AI, in fraud detection within your institution or elsewhere? If so, can you share what made them effective?	To gather examples of successful practices that could serve as models for future technology adoption in fraud detection.
4. Closure	
Concluding Investigations	
Once an investigation is complete, how do you communicate your findings to the applicant? What steps do you take to ensure clarity and transparency in your closure?	To understand communication practices and transparency in fraud investigations, which can inform best practices for improving applicant relations and trust.
Follow-up Actions	
After concluding an investigation, what follow-up actions do you take to ensure similar issues are addressed in the future?	To identify strategies for preventing future fraud and improving document verification practices.
5. Evaluate	
Effectiveness of the Process	
Overall, how effective is your current process? Which parts have their merits or problems? Any metrics or KPIs employed?	
Reflection on the Process	
In your experience, how effective is the PEACE model in guiding your investigations of problematic applicants? What aspects do you find most beneficial, and what challenges do you face?	To assess the effectiveness of the PEACE model in practice and identify areas for improvement in the admissions process.
Suggestions for Improvement	
How do you think the application of the PEACE model could be improved within your institution's admissions process?	To gather recommendations for enhancing the PEACE model application, which can inform future training and development for staff involved in fraud detection.

References

1. Altbach, P.G.; Reisberg, L.; Rumbley, L.E. Globalization and Internationalization. In *Trends in Global Higher Education: Tracking an Academic Revolution*; Brill: Leiden, The Netherlands, 2019; Volume 22, pp. 23–36.
2. Clifton, H.; Chapman, M.; Cox, S. 'Staggering' trade in fake degrees revealed. *BBC News*, 2018 January 16.
3. Zhao, Y.; Borelli, A.; Martinez, F.; et al. Admissions in the age of AI: Detecting AI-generated application materials in higher education. *Sci. Rep.* **2024**, *14*, 26411. https://doi.org/10.1038/s41598-024-77847-z.
4. Ayub Khan, A.; Laghari, A.A.; Shaikh, A.A.; et al. Educational Blockchain: A Secure Degree Attestation and Verification Traceability Architecture for Higher Education Commission. *Appl. Sci.* **2021**, *11*, 10917.
5. Awaji, B.; Solaiman, E.; Albshri, A. Blockchain-Based Applications in Higher Education: A Systematic Mapping Study. In Proceedings of the 5th International Conference on Information and Education Innovations, New York, NY, USA, 26–28 July 2020; pp. 96–104.
6. de Castro, R.Q. Blockchain Applications for Diploma Verification in Higher Education Institutions in Portugal—A Mixed Methods Study. Master's Thesis, Universidade do Porto (Portugal), Porto, Portugal, 2021.
7. Calvet Liñán, L.; Juan Pérez, Á.A. Educational Data Mining and Learning Analytics: Differences, similarities, and time evolution. *Int. J. Educ. Technol. High. Educ.* **2015**, *12*, 98–112. https://doi.org/10.7238/rusc.v12i3.2515.
8. Mengash, H.A. Using Data Mining Techniques to Predict Student Performance to Support Decision Making in University Admission Systems. *IEEE Access* **2020**, *8*, 55462–55470. https://doi.org/10.1109/ACCESS.2020.2981905.
9. Çela, E.; Potluri, R.M.; Vajjhala, N.R. A Comprehensive Meta-Analysis of IoT Integration for Data-Driven Decision Making in Education. *Des. Sustain. Internet Things Solut. Smart Ind.* **2025**, 27–50. https://doi.org/10.4018/979-8-3693-5498-8.ch002.
10. Kassab, M.; DeFranco, J.; Laplante, P.A. Systematic literature review on Internet of things in education: Benefits and challenges. *J. Comput. Assist. Learn.* **2020**, *36*, 115–127.
11. Alothman, B.; Alazmi, H.; Ali, M.B.; et al. Accelerating University Admission System using Machine Learning Techniques. In Proceedings of the 2022 Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN), Barcelona, Spain, 5–8 July 2022; pp. 439–443.
12. Van Busum, K.; Fang, S. Analysis of AI models for student admissions: A case study. In Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing, New York, NY, USA, 27–31 March 2023; pp. 17–22.
13. Hollman, J.H.; Krause, D.A. Machine Learning in Admissions? Use of Chi-Square Automatic Interaction Detection (CHAID) to Predict Matriculants to Physical Therapy School. *J. Allied Health* **2023**, *52*, 93–98.
14. Eaton, S.E.; Carmichael, J.J.; Pethrick, H. *Fake Degrees and Fraudulent Credentials in Higher Education*; Springer: Cham, Switzerland, 2023.
15. Yiu, W. Hong Kong warns students over using fake credentials to enter universities. *South China Morning Post*, 18 October 2024.
16. Yiu, W. University of Hong Kong students urged to report suspicions on fake qualifications after 'small number' of cases uncovered at business school. *South China Morning Post*, 21 May 2024.
17. Lee, C.Y. Fake university degree scandal: Uncovering the loophole in Hong Kong universities' admissions behind the sky-high "guaranteed admission"of Chinese students. *BBC News*, 20 September 2024.
18. Lee, W.L. Hong Kong intermediary headquarters exposed, claiming to have bribed international examination centers to enter Hong Kong University for 2 million. *HK01*, 14 October 2024.
19. Chin, J.; Rebecca, M.; and Bull, R. Fuelling an investigative mindset: The importance of pre-interview planning in police interviews with suspects. *Psychol. Crime Law* **2024**, *30*, 1016–1040. https://doi.org/10.1080/1068316X.2022.2139829.
20. Clarke, C.; Milne, R. *A National Evaluation of the PEACE Investigative Interviewing Course*; Home Office: London, UK, 2001.
21. College of Policing. Investigative Interviewing. Available online: https://www.college.police.uk/app/investigation/investigative-interviewing/investigative-interviewing (accessed on 26 March 2025).
22. Barron, W.T. The Peace Model of Investigative Interviewing: A Comparison of Trained and Untrained Suspect Interviewers. Ph.D. Thesis, Memorial University of Newfoundland, 2017.
23. Akca, D.; Lariviere, C.D.; Eastwood, J. Assessing the efficacy of investigative interviewing training courses: A systematic review. *Int. J. Police Sci. Manag.* **2021**, *23*, 73–84.
24. Cleary, H.M.; Warner, T.C. Police training in interviewing and interrogation methods: A comparison of techniques used with adult and juvenile suspects. *Law Hum. Behav.* **2016**, *40*, 270–284. https://doi.org/10.1037/lhb0000175.
25. Clarke, C.; Milne, R.; Bull, R. Interviewing Suspects of Crime: The Impact of PEACE Training, Supervision and the Presence of a Legal Advisor. *J. Investig. Psychol. Offender Profiling* **2011**, *8*, 149–162. https://doi.org/10.1002/jip.144.
26. Rogers, E.M. *Diffusion of Innovations*, 5th ed.; Free Press: New York, NY, USA, 2003.
27. Dearing, J.W. 611Diffusion of Innovations. In *The Oxford Handbook of Organizational Change and Innovation*; Poole, M.S., Van de Ven, A.H., Eds.; Oxford University Press: Oxford, UK, 2021.

28. Handoko, B.L.; Angelus, M.; Mulyawan, A.N. Diffusion of innovation on auditor adoption of artificial intelligence and machine learning. In Proceedings of the 2023 7th International Conference on Software and e-Business, Osaka, Japan, 21–23 December 2023; pp. 20–26.
29. Mohammad Khaleel, O.; Chin Wei, C.; Fadi Abdel Muniem Abdel, F. Knowledge management systems usage: application of diffusion of innovation theory. *Glob. Knowl. Mem. Commun.* **2021**, *70*, 756–776. https://doi.org/https://doi.org/10.1108/GKMC-08-2020-0117.
30. Abdalla, A.A.; Bhat, M.A.; Tiwari, C.K.; et al. Exploring ChatGPT adoption among business and management students through the lens of diffusion of Innovation Theory. *Comput. Educ. Artif. Intell.* **2024**, *7*, 100257. https://doi.org/10.1016/j.caeai.2024.100257.
31. Shawyer, A.; Walsh, D. Fraud and Peace: Investigative Interviewing and Fraud Investigation. *Crime Prev. Community Saf.* **2007**, *9*, 102–117. https://doi.org/10.1057/palgrave.cpcs.8150035.
32. Smith, R.G. Coordinating individual and organisational responses to fraud. *Crime, Law and Social Change.* **2008**, *49*, 379–396. https://doi.org/10.1007/s10611-008-9112-x.
33. Al-Ameri, M.A.A.; Mahmood, B.; Ciylan, B.; et al. Unsupervised Forgery Detection of Documents: A Network-Inspired Approach. *Electronics* **2023**, *12*, 1682. https://doi.org/10.3390/electronics12071682
34. Al-Ameri, M.A.A.; Mahmood, B.; Ciylan, B.; et al. Computational Methods for Forgery Detection in Printed Official Documents. In Proceedings of the 2022 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS), Manama, Bahrain, 22–23 June 2022; pp. 307–313.
35. Al-Ghamdi, N.; Alsubait, T. Digital Forensics and Machine Learning to Fraudulent Email Prediction. In Proceedings of the 2022 Fifth National Conference of Saudi Computers Colleges (NCCC), Makkah, Saudi Arabia, 17–18 December 2022; pp. 99–106.
36. Guingrich, R.E.; Graziano, M.S.A. P(doom) Versus AI Optimism: Attitudes Toward Artificial Intelligence and the Factors That Shape Them. *J. Technol. Behav. Sci.* **2025**, in press. https://doi.org/10.1007/s41347-025-00512-3.
37. Aniceto, M.C.; Barboza, F.L.d.M.; Kimura, H. Machine learning predictivity applied to consumer creditworthiness. *Future Bus. J.* **2020**, *6*, 37. https://doi.org/10.1186/s43093-020-00041-w.
38. Badhan, I.A.; Hasnain, M.D.N.; Rahman, M.D.H.; et al. Strategic Deployment of Advance Surveillance Ecosystems: An Analytical Study on Mitigating Unauthorized U.S. Border Entry. *Inverge J. Soc. Sci.* **2024**, *3*, 82–94. https://doi.org/10.63544/ijss.v3i4.105.
39. Ellen, P.S.; Bearden, W.O.; Sharma, S. Resistance to technological innovations: An examination of the role of self-efficacy and performance satisfaction. *J. Acad. Mark. Sci.* **1991**, *19*, 297–307. https://doi.org/10.1007/BF02726504.
40. Bansal, K.; Paliwal, A.C.; Singh, A.K. Analysis of the benefits of artificial intelligence and human personality study on online fraud detection. *Int. J. Law Manag.* **2025**, *67*, 191–209. https://doi.org/10.1108/IJLMA-08-2023-0198.
41. Koenig, A.M.; Devlin, E. Fighting Domestic and International FRAUD in the Admissions and Registrar's Offices. *Coll. Univ.* **2012**, *88*, 18–33.
42. Cheron, C.; Salvagni, J.; Colomby, R.K. The Qualitative Approach Interview in Administration: A Guide for Researchers. *Rev. De Adm. Contemp.* **2022**, *26*, e210011. https://doi.org/10.1590/1982-7849rac2022210011.en.