“© 2026 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.”

Academic Certificate Behavioral Fraud Detection: A Proof of Concept

1st Ibrahim Khormi
Jazan University, Saudi Arabia
University of Technology Sydney
Jazan, Saudi Arabia
ikhormi@jazanu.edu.sa

2nd Priyadarsi Nanda
University of Technology Sydney
Sydny, Australia
priyadarsi.nanda@uts.edu.au

3rd Manoranjan Mohanty
Carnegie Mellon University
Doha, Qatar
mmohanty@cmu.edu

***Abstract*— Academic certificate fraud has become problematic in this digital age. Insider threat in addition to the sophisticated nature of the today's evolving fraud, underscore the need for advance fraud detection system. This paper proposes a novel approach to academic certificate fraud detection problem by leveraging access logs. The analysis of access logs behavioral features facilitates the identification of fraudulent behavior in the certification process. A machine learning based behavioral fraud detection model has been developed, with the assumption that access logs produce unique behavioral patterns. As a proof-of-concept, a simple yet robust machine learning algorithm – logistic regression was employed to develop the model. The results demonstrate the efficacy of the proposed approach. It can accurately distinguish between legitimate and fraudulent certificates with a detection rate above 85%. This approach promises improved security against institutional certificate fraud. It also provisioned a model that can serve as a pre-registration fraud detection and prevention scheme to blockchain-enabled certificate system.**

Keywords—access logs, academic certificate, fraud, machine learning, logistic regression

I. INTRODUCTION

Educational institutions play an important role in human capital development and economic advancement. Individuals enroll into institutions of learning with expectations of acquiring certificate at the end of their studies. Certificate is an important document that serves as a proof to certify that an individual has received specific training and acquired relevant skills and qualification. Certificate uniquely define one's competence, qualification and identity. They are issued by recognized authorities such as government agencies or universities. Academic certificate is the first and most important document anyone can present as claim for validation of their academic achievement [1]. They are used to advance one's educational endeavor, obtain jobs or other privileges. Due to the increasing importance of certificate, individuals have become desperate to acquire certificates. This desperation birthed the certificate fraud regime, where individuals or organizations intentionally manipulate the certificate process to obtain or issue fake and fraudulent certificates. A recent survey shows that more than half of curricula vitae (CV) and job application claims turn out to be false and about 78% of these documents show misleading information [2].

Certificate fraud has grown into a big business all over the world and has become a significant problem in the education sector. It affects the credibility and reputation of educational institutions aside the economic damage it may cause. This menace is perpetrated by individuals or organized group of fraudsters. Technological advancement with internet access has also aided certificate fraud. Today, with digital certification, certificate can be easily forged to look exactly like an original one issued by a legitimately accredited institution. Fraudsters are continuously evolving sophisticated ways to carry out their activities without trace. A more disturbing trend in the certificate fraud regime is the involvement of insiders (institutional staff). An insider can be compromised to manipulate the system and issue fake certificates. A good example of institutional fraud is the Busoga University scandal [3]. In 2016, the University awarded over 1000 degree certificates to South Sudanese in one month. In some cases, such individuals will attend such institutions but will not meet the minimum requirement. A typical case is the Makerere University scandal [4]. The University sacked 88 staff members who were found to be involved in collecting bribe and altering student's grades and issuing fraudulent certificate. Institutional certificate fraud is difficult to detect since the issued certificate is backed by the issuing institution records.

The growing concern of certificate fraud and the threat it poses to the economy and human lives necessitate the development of a sophisticated scheme for detecting and preventing certificate fraud. Traditional methods of detecting fake certificates are becoming inefficient and lack transparency [5]. Third parties such as employers often contact issuing institutions to confirm the validity of a certificate. This is usually costly, time-consuming and depends on humans who may be compromised in the verification process. In this age of digital certification, emerging technologies such as blockchain present a viable alternative to mitigate certificate fraud. Blockchain provides the needed security and transparency in the certificate verification system [6] [1] but lack capacity to detect or prevent institutional certificate fraud. The sophisticated nature of today's certificate fraud, in addition to the challenge of institutional fraud demands a robust technique for the detection and prevention of digital certificate fraud.

Generally, before fraud is established, there may be certain activities or behaviors that are exhibited in the process leading to certificate issuance. With digitization, these activities may include login times, IP addresses, device type used, and unusual grading. By analyzing such data, a robust fraud detection system can be developed. It is expected that these access logs and behaviors should have a pattern for legitimate certificate issuance. We believe that if these logs and behaviors are captured, any abnormality or deviation from the norm can be flagged as suspicious. Therefore, access log data and behavioral analytics become important tools for developing behavioral fraud detection scheme in which suspicious certificates may be detected before they are issued.

Thus, preventing circulation of fake certificates. The realization of behavioral fraud detection and prevention system is of utmost important in the current digital education landscape, as it tackles the problem of institutional fraud. By leveraging behavioral analytics and machine learning techniques, fraudulent activities could be predicted before certificates are issued. This holds substantial practical implication for stakeholders in the education ecosystem. To the best of the authors knowledge, this is the first attempt to use access log and behavioral analytics to detect academic certificate fraud.

The main contributions of this paper include but not limited to:

(i) Proposing a novel behavioral fraud detection and prevention scheme for academic certificate regime

(ii) Using machine learning based behavioral fraud detection system providing for the evolving landscape of fraud and the vulnerabilities in future.

(iii) The use of access log to detect academic certificate fraud before certificates are issued essentially prevents circulation of fraudulent certificates.

(iv) Presents a solution to the challenging problem of institutional fraud.

A. Problem Statement

The vulnerability and inefficiency of existing certificate fraud detection and prevention systems underscore the urgency for developing a robust solution. Traditional methods are insufficient for the current digital certificate landscape. Blockchain provides solutions to data alteration and can handle post-issuance fraud, but not pre-issuance fraud. Pre-issuance certificate fraud often occur before certificates are issued. This is often perpetrated by compromised members of staff. Institutional certificate fraud often eludes existing detection systems. Even blockchain is not able to predict or detect behavior leading to certificate issuance. It is expected that there may be some 'digital' activities or behaviors during the certification process. Thes may include logins, IP addresses, location, actions and device type. By leveraging such behavioral data, a robust anomaly detection system can be developed. This will essentially address the problem of pre-issuance fraud otherwise known as institutional fraud.

B. Novelty of the study

The application of access log and behavioral analytics for fraud detection in the education landscape remains relatively sparse. The novelty of this study is in the use behavioral access logs with machine learning for academic certificate fraud detection. While some studies have data [7], no study have used access logs to detect certificate fraud. This presents a significant challenge. Academic certificates issuance and its processing have unique features that may influence log patterns and the efficacy of detection models. This work intends to leverage this uniqueness to develop a robust machine learning based academic certificate fraud detection model.

The rest of this paper is organized as follows. Section II reviews related works. Section III describes the proposed approach to certificate fraud detection and model evaluation metrics. Section IV presents the experimental results and discussion. Finally, the conclusion of the paper is given in section V.

II. RELATED WORKS

Access logs and user behavior are fast becoming important tools in fraud detection and prevention. Behavioral analytics profiles user's normal behaviors and help identify suspicious activities in real-time. This provides for a proactive approach in fraud detection. Fraud detection systems built on user's behaviors have been studied and demonstrated in different domains such as finance and cybersecurity.

In [8], the challenges of digital fraud are discussed and a solution based on access log was proposed. The author acknowledged the importance of access log data in mitigating digital crime. "Log analysis provides useful way for alerting, monitoring, security and compliance, auditing, incident response and forensic investigations". The author developed a machine learning based log parsing module to detect anomalies in data. Both isolation forest algorithm and outlier detection methods were tested. The results show increase in fraud detection rate and minimized false alarms rate.

Authors in [9] developed a machine learning based model for detecting fraudulent websites. Their work uses weblog data which consist of URL, domain, and path characteristics to extract relevant user behavioral features. The behavioral features were used to train Random Forest classification algorithm. The developed model was used to determine if a website address is phishing or legitimate.

The authors in [10] developed a technique for fraud detection and prevention in web advertising networks. They used web access log to validate the fraud detection technique.

In a more recent work, [11] discussed the problem of fraudulent access to online services such as internet banking, credit card and e-commerce. Phishing, malware infection, and list-based attack are some of the many ways fraudsters gain access to websites and steal customer's information. They acknowledge that existing solutions can be expensive and have low detection accuracy. With fraud prevention software, it is difficult to get all customers to install them. Therefore, they proposed a fraud detection technique that is based on real-world server-side access log data. In their work, they analyzed attribute information, historical information and user behavior such as IP address, browser fingerprints, OS, location and time of access.

Authors in [7] have identified the problem of rogue certificates been issued by trusted certificate authorities. They discuss the potential threat of this behavior. Certificate authorities can be compromised to issue fraudulent certificates. And it is important to have tools for detecting such fraud. The authors developed a machine learning based method for detecting rogue certificates from trusted certificate authorities. Their model is trained using features extracted from issuing behaviors and certificate attributes. The model was able to identify "technically valid certificates that are potentially malicious".

[12] propose an anomaly-based insider threat detection system that is user adaptive. It is user adaptive because it is able to select the best feature extraction method for each user based on covariance. The authors proposed to use time information conversion method to convert numerical time information into location information. With deep learning, this helps the model to obtain user behavior rhythm from user behavior data. This captures insider threat behaviors.

In [13], the authors identify the problem of continuous financial fraud detection in enterprise systems. The authors try to demonstrate how audit trails in enterprise systems can be used for continuous fraud detection. They propose a methodology for continuous financial fraud detection in enterprise systems that is based on security audit logs, changes in master records and accounting audit trails. They discuss continuous assurance and fraud detection and their application in enterprise systems.

The proposal is carried out using the following three steps: (i) monitoring threat in security audit logs (ii) automated audit trail data extraction and analysis, and (iii) determination of fraud occurrence using forensic investigation techniques.

The extracted data turns out to be user's behavior. Specific fraud is detected by monitoring and analyzing the user behavior in audit trail. The authors demonstrated the proposed method by using mySAP enterprise system to analyze audit trail in order to detect financial fraud.

Authors in [14] have introduced a discussion on the problem with Euro-pay MasterCard VISA (EMV) chip in the credit card business. They highlighted that the implementation of EMV has resolved several challenges of the old Magnetic stripe card technology. However, despite the intrinsic security characteristics of this technology, internet and online payment and transactions makes these chip cards vulnerable. Fraudsters can compromise payment platforms and potentially steal details of these cards for their own benefits.

To solve this lingering problem, the authors propose a methodology that uses transaction logs. These historical logs represent customer online behavior. They propose to analyze the historical transaction logs to identify customer's normal behavior and anomalies using machine learning technique. They developed machine learning model that can detect fraudulent activities.

In [15], authors discuss fraud as the most significant avoidable threat for mobile network operators. The developed an ensemble learning based International Revenue Share Fraud detection model. The model leverages call logs to identify fraudulent call patterns. The call attributes used to form the data include time, duration, source and destination numbers and completion status. Here, Random Forest and support vector machine algorithm were used to implement the proposed ensemble learner. The choice of random forest is informed by its ability to handle imbalanced data that is common in mobile network fraud scenarios.

The current study undertakes to leverage the two important tools: behavioral analytics and machine learning that have been used in other domains for academic certificate fraud detection and prevention.

A. Behavioral Patterns and Fraud Detection

Access logs have become very important in understanding insider behavior in our today's digital world. The features generated from access logs produces rich patterns that represent behavioral interactions. Some of the common behavioral attributes include, timestamps, device type, ip addresses, location, and their derivatives. These unique behavioral patterns can be leveraged to identify fraudulent activities in transactions. Table 1 gives examples of use cases of these features in different domains. In this study, we seek to investigate the feasibility of using behavioral patterns from access logs to combat certificate fraud. While access logs may share similar structures, user behaviors stand at variance. Our approach leverages these behavioral variations and machine learning to demonstrate the feasibility of a proactive and enhanced certificate fraud detection

Table 1. Examples of Behavioral Patterns Used in Other Domains

Behavioral Feature	General Role	Example of Use in Other Domains	Reference
Timestamp	Detects unusual activity times	Used in financial fraud detection to flag logins or transactions performed outside normal working hours	[16], [17]
Location	Verifies geographic origin	Applied in cybersecurity to detect suspicious logins from unexpected locations	[18]
Device Type	Identifies the device used	Used in e-commerce to flag purchases from unrecognized devices	[19]
Source IP	Monitors access origins	Applied in network intrusion detection to detect abnormal or malicious IP addresses	[11]

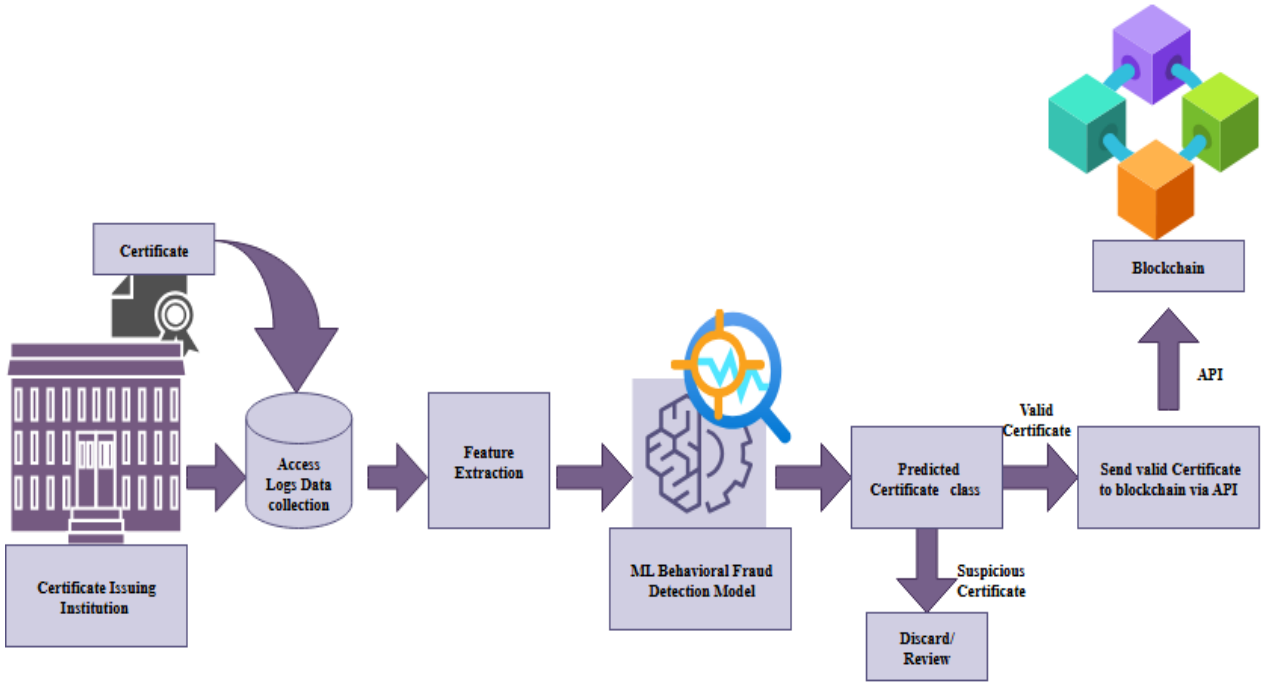

Figure 1. Framework of the proposed certificate fraud detection system

III. THE PROPOSED APPROACH

Real-time fraud detection presents a significant challenge. This is because of the ever-evolving nature of fraud tactics and behaviors. Conventional fraud detection techniques are becoming less accurate, requiring much time and resources. This study presents a proof-of-concept for the use of access logs to detect certificate fraud. The method is designed to leverage the analytic ability of machine learning to provide real-time fraud detection. The framework for the propose methodology is as shown in Fig 1. The experimental and simulation methodology is employed in this study. This comprises data collection and preprocessing including feature extraction, machine learning modeling, training and evaluation. The access log data were processed and used to train the machine learning algorithm to generate a model for fraud detection.

A. Case Study: Detecting Certificate Fraud

To demonstrate the effectiveness of the proposed system, consider the following suspicious certificate request:

Scenario Description:
(i) A certificate was issued at 02:15 AM.
(ii) The request originates from an off-campus location.
(iii) The device used for this action is unfamiliar for this user.

Case Study Pseudocode:
Algorithm: Certificate_Fraud_Detection_System
Input: Certificate_Request
Output: Decision (issue/review)

Step 1. Receive request:
User submits certificate issuance request
request → pass to model pipeline.

Step 2. Extract relevant behavioral features:
Features = [Off_hours, Location, Device, Source_IP]
Step 3. Predict activity type
label = model.predict(features)

Step 4. Decision:
if label == "Fraudulent":
decision = “Review”
Block_Certificate(Certificate_Request)
Notify_Administrator(Certificate_Request)
else:
decision = “Issue”
Issue_Certificate(Certificate_Request)
Push_To_Blockchain(Certificate_Request)

Step 5. Return
return decision

B. Data Description

Obtaining real academic certificate data from any HEI can be challenging due to the privacy restrictions. This makes accessing publicly available HEI access logs datasets for research purposes difficult. Therefore, as a proof-of-concept a publicly available enterprise access log dataset on Github is employed for this study [20] [21]. The dataset contains 8 attributes and 5000 log entries. This dataset is adopted because it contains many attributes that relates to access logs in HEIs. It also contains behavioral patterns that can be associated with certificate issuance. The class distribution of the dataset is given in Figure 2. This exploration indicates an imbalance dataset.

C. Data Preparation and Simulation

The dataset used in this work was originally generated as enterprise access logs data for identity-based threat detection. In order for the dataset to be useful in this study, there is need to modify it to mimic HEI’s access logs. This includes data cleaning, selection and scenario simulation. The following

steps were executed to generate a simulated HEI access log dataset:

- First, attributes that are relevant to academic certificate were carefully selected from the original data to form the modified dataset. The selected attributes are listed in Table 2.
- The selected raw access log data is cleansed. All log entries that were tagged malicious were removed, leaving only entries with benign targets. This provided us with clean standard feature vectors representing normal user behavior.
- Certificate fraud scenarios were created and anomalies injected into the modified dataset to ensure that at least 10% of the data entries represent suspicious activities.
- Finally, the target classes were labeled as shown in Table 3. The normal (legitimate activities) behaviors were labeled as 0, whereas the simulated anomalies (fraudulent activities) were labeled as 1.

These steps produce standard access logs data for certificate issuance in HEIs. It is this simulated dataset that will be used to demonstrate the proof-of-concept.

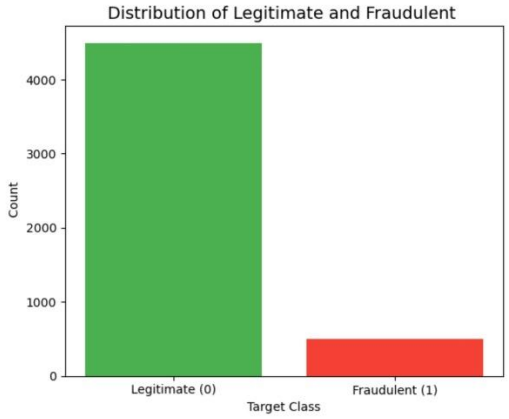

Figure 2. Distribution of Access Logs Data

Table 2. Selected raw data attributes

S/ No.	Feature Name	Description
1	timestamp	Date and time of the log event
2	masked_user	Anonymized user identifier
3	source_ip	IP address of the originating event
4	action	Action performed (e.g., login, logout, delete, modify)
5	location	Place where certificate is issued
6	Device_type	Type of device used (desktop, mobile, tablet)
7	target	Ground truth label (benign or malicious)

Table 3. Class labels

S/No.	Class Name	Label
1	Legitimate activities	0
2	Fraudulent activities	1

D. *Feature Extraction*

Extracting relevant features from access log data is an important step towards anomaly detection during certificates issuance. The result and performance of the machine learning model depend heavily on how well the extracted features describe the certificate categories. Four representative features were extracted from the raw access log data due to their importance in anomaly detection. These four features are listed in Table 4. It is these four features that will be used to build a machine learning model.

Table 4. Extracted Features

S/No.	Feature Name	Description
1	IP Address	Source IP
2	Location	Place from which activity was performed
3	Device	Type of electronic device used
4	Off_hours	Derived from timestamp

E. *Machine Learning Modeling*

Machine learning algorithms are trained using the processed data to recognized normal and abnormal patterns. The develop fraud detection model can be used to predict any suspicious behavior in real-world.

1) Model training and validations: The machine learning model is trained to ensure that it makes accurate predictions. To achieve this, the dataset is divided into training and testing sets. The training set is used to build a model. The test set on the other hand is used to evaluate the developed model. In this study, cross validation technique is employed to divide the data and build a robust model for behavioral fraud detection. The model that is optimized makes the most accurate detections. In cross validation, the dataset is randomly divided into disjointed sub-groups known as k-folds. And for any set of parameters, the model is trained on k-1 folds of the data and tested or evaluated on the remaining fold. This procedure is repeated until every fold is tested and evaluated. The average detection error is computed. This produces a stable and robust model. This process is repeated for different parameter values and the values with the least detection error are selected as optimal parameters. In this study, a 5-fold cross validation was used as shown in Figure 3.

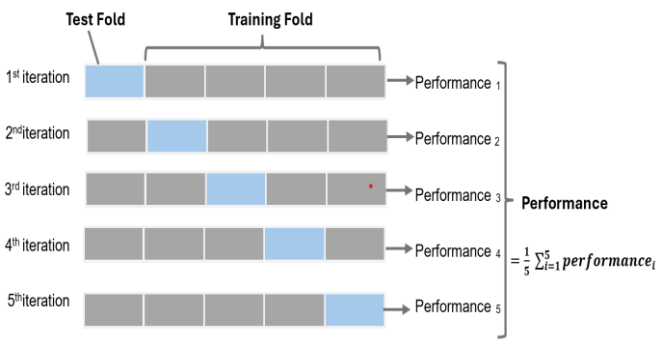

Figure 3. Division of dataset based on 5-fold cross validation

F. Performance Evaluation Matrics

The developed ML model is evaluated on the test set. First, only the features are presented to the model. The model makes predictions on these features. The result is evaluated by comparing the predicted outputs from the actual outputs. The following metrics are used for evaluating the performance of ML classifier model: confusion matrix, accuracy, precision, recall and F1 score. These metrics are chosen based on the fact that certificate fraud detection is considered as a binary classification problem in this study.

1) Confusion matrix: The confusion matrix is widely used in ML classification problem. Here, it is used to evaluate the true positive, which in our case is the fraud detection rate and the false positive alarm. The standard format for the confusion matrix is shown in Table 5. In the confusion matrix, TP is True Positive, which indicates the number of non-fraudulent certificates correctly identified. FP stands for False Positive (false alarm) which shows the number of non-fraudulent cases that are incorrectly classified as fraudulent. FN stands for False Negative, which gives the number of fraudulent cases that are misclassified as non-fraudulent. TN stands for True Negative, which shows the number of fraudulent cases that are correctly classified as fraud. The developed model is expected to have high TP and low false alarm rate (FP).

Table 5. Confusion Matrix

		Predicted	
		Positive	**Negative**
Actual	**Positive**	TP	FN
	Negative	FP	TN

The True Positive rate is given by the (1),

$$TP_{rate} = \frac{TP}{TP+FN} \quad (1)$$

The False Positive rate is given by (2),

$$FP_{rate} = \frac{FP}{TN+FP} \quad (2)$$

2) Accuracy: Accuracy gives us the ratio of the total number of cases that are correctly classified. The accuracy of a model is given by (3),

$$Accuracy = \frac{TP+TN}{TP+FP+FN+TN} \quad (3)$$

3) Precision and Recall: Precision shows how well a model predicts positive outcomes, which in our case is non-fraudulent certificates. Recall on the other hand determines the model's ability to predict non-fraudulent cases. Equation 4 and 5 are the formulas for calculating precision and recall respectively.

$$Precision = \frac{TP}{TP+FP} \quad (4)$$

$$Recall = \frac{TP}{TP+FN} \quad (5)$$

4) F1-score: F1-score is a weighted harmonic mean of precision and recall. F1-score is given by (6).

$$F1 = \frac{2*Precision*Recall}{Precision+Recall} \quad (6)$$

IV. RESULTS AND DISCUSSION

The current study investigates the use of access logs to predict fraudulent behaviors that lead to issuance of fake certificates. The HEI access logs data was simulated from enterprise access logs dataset. This work seeks to answer the research question on how machine learning can detect fraudulent issuance behavior before certificates are recorded on the blockchain. As a proof-of-concept, logistic regression, a simple but effective algorithm is employed to build the certificate behavioral fraud detection classifier. The basic idea behind logistic regression as a supervised anomaly predictor is to learn a decision boundary that separates the legitimate and fraudulent certificates.

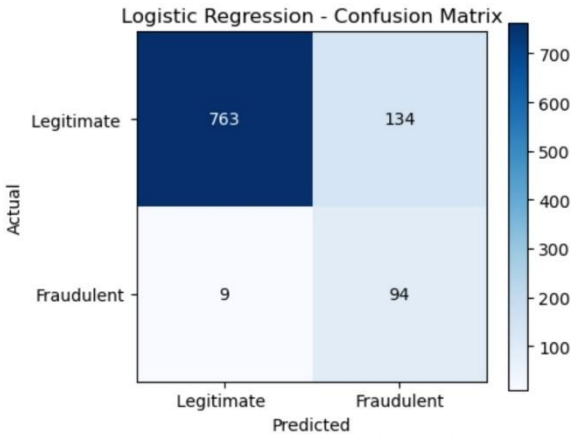

Figure 4. Confusion matrix of the model

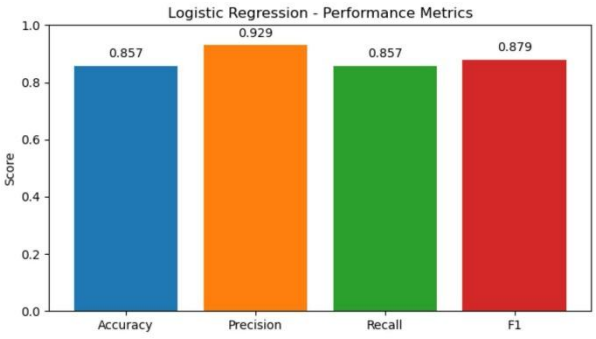

Figure 5. Performance of Logistic Regression Model

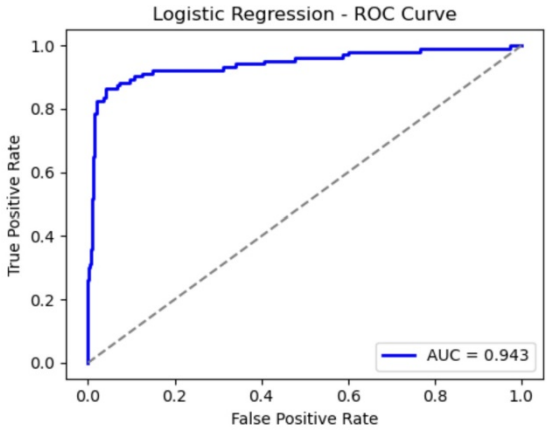

Figure 6. Area under the curve analysis of logistic regression model

To evaluate the behavioral fraud detection model developed, the metrics defined in section 4 were considered in the analysis. Firstly, the confusion matrix of the model is generated as shown in Figure 4. During training, the model learns the feature-target mapping and use this knowledge in classifying new data to determine legitimacy.

The recall and FNR determine the model's success rate. A good model is expected to have a recall of approximately 100%, with FNR turning towards 0%. The result from Figure 5 shows a recall of 85.7%. This means that the logistic regression model was able to correctly detect legitimate certificate with 85.7% success. On the one hand precision shows the model's ability to correctly detect legitimate certificates during testing. On the other hand, FDR indicates the rate at which the model detects legitimate certificate wrongly. The result presented in Fig 6, shows that the developed model achieved a precision of 92.9%. This means the model was able to correctly detect legitimacy with 92.9% precision.

The Area Under the Curve (AUC) which represents the relationship between the TPR and the FPR is shown in Figure 6. The target is to achieve an AUC value of 1. An AUC of 1 show that a model can correctly detect legitimate certificates and correctly detect fraudulent certificates. Our model achieved an AUC of 0.943. This means it is able to correctly detect legitimate certificates and correctly detect fraudulent cases with 94.3% success rate. However, this result does not agree with recall and FNR. Overall, the accuracy of the evaluated model is 85.7%.

A. *Comparison with Existing Solutions*

Traditional certificate verification methods are often manual, time-consuming, and prone to human error [23]. While blockchain-based solutions offer strong security guarantees, they can be costly and complex to implement [24]. In contrast, the proposed system leverages machine learning to achieve faster, more scalable, and automated fraud detection.

Table 6. Comparative Analysis of the proposed system with existing systems

Aspect	Manual Verification	Blockchain-based	Proposed ML System
Speed	Slow	Moderate	Fast
Scalability	Limited	High	High
Cost	High	High	Moderate
Accuracy	Moderate	High	High
Automation	Low	Partial	High

V. CONCLUSIONS

The rise in certificate fraud presents a significant challenge in the education landscape across nations of the world. To address this problem, this paper described a proof-of-concept access logs-based behavioral certificate fraud detection system. Specifically, this work focus on the performance of machine learning algorithm to enhance academic certificate fraud detection. The proposed approach is based on the use of access logs as features to establish legitimacy and anomaly in certification process. As a proof-of-concept, logistic regression is used to model the relationship between the access logs features and the legitimacy of certificates. The performance of the developed model has been rigorously evaluated based on standard machine learning metrics. The experimental result demonstrates the accuracy and efficacy of the proposed approach.

A. *Limitations*

This study provides a proof-of-concept on the use of access logs in certificate behavioral fraud detection. The proposed system leverages machine learning to facilitate fraud detection. Although the result demonstrates the efficacy of the proposed approach in identifying behavioral fraud, there are some limitations.

1) Dataset constraints: Lack of publicly available HEI access logs data. The dataset used was derived from enterprise access logs. This may make it restricted. It may also lack other relevant and insightful HEI attributes.

2) Lack of fraud instances: To be able to use the dataset effectively, artificial scenarios of fraud were injected manually. Many real-world fraudulent behaviors may not be captured by this technique. This essentially limits the dataset.

B. *Future Works*

Further research work will consider the following,

(1) To generate and incorporate more complex fraud scenarios to improve the robustness of the proposed approach.

(2) Investigate additional techniques including explainable AI to assess the effectiveness of the proposed approach

(3) Validate the proposed approach with real-world HEI certificate access logs.

(4) To build and deploy a prototype of the most effective model for real-world certificate behavioral fraud detection..

VI. REFERENCES

[1] Kumutha K., & Jayalakshmi S., "Blockchain Technology and Academic Certificate Authenticity - A Review," in *Lecture Notes in Networks and Systems*, Singapore, 2022.

[2] Serranito D. T., "A Blockchain-based Platform for Sharing and Verifying Education Certificates," Tecnico Lisboa, 2020.

[3] Tariq A., Binte Haq H., & Taha Ali S., "Cerberus: A Blockchain-Based Accreditation and Degree Verification System," *arXiv,* pp. 1-14, 2019.

[4] Trines S., "Academic Fraud, Corruption, and Implications for Credential Assessment," World Education Services, 2017.

[5] Jenifer A., Mahadik P., Sanskar S., Gupta T., and Meshram Y., "Certificate Issuing and Verification Application Using Blockchain," *International Journal of Software Computing and Testing,* vol. 10, no. 1, pp. 21-28, 2024.

[6] Abdelmagid R., Abdelsalam M. & Alsheref F. K., "A Blockchain Framework for Academic Certificates Authentication," *International Journal of Advanced Computer Science and Applications,* vol. 15, no. 7, pp. 297-305, 2024.

[7] Dong Z., Kane K., & Camp L. J, "Detection of Rogue Certificates from Trusted Certificate Authorities using Deep Neural Networks," *ACM Transactions on Privacy and Security,* vol. 19, no. 2, pp. 1-31, 2016.

[8] Sharma S., "Efficient Log Analysis using Advanced Detection and Filtering Techniques," School of Computing, National College of Ireland, Ireland, 2019.

[9] Ibrahim K. K. & Obaid J. A., "Fraud Usage Detection in Internet Users Based on Log Data," *International Journal of Nonlinear Analysis and Applications,* vol. 12, no. 1, pp. 2179-2188, 2021.

[10] Tripathi G., Ahad M. A., and Casalino G., "A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges," *Decision Analytics Journal,* pp. 1-21, 2023.

[11] Kunimoto M. & Okubo T., "Analysis and Consideration of Detection Methods to Prevent Fraudulent Access by Utilizing Attribute Information and the Access Log History," *Journal of Information Processing,* vol. 31, pp. 602-608, 2023.

[12] Song S., Gao N., Zhang Y., & Ma C., "BRITD: Behavior Rhythm Insider Threat Detection with Time Awareness and User Adaptation," *Cybersecurity,* vol. 7, no. 2, 2024.

[13] Best P. J., Rikhardsson P., & Toleman M., "Continuous Fraud Detection in Enterprise Systems through Audit Trail Analysis," *Journal of Digital Forensics & Law,* vol. 4, no. 1, 2009.

[14] Deepika V., Gokila S., Janani E. R. G., & Kanagaraju P., "Detection of Fraud using Transaction Behavior in Credit Card," *International Journal of Advance Research in Science and Engineering,* vol. 8, no. 3, 2019.

[15] Mayeni R., Dube S., Ndlovu B., Maduva M., & Kiwa F. J., "A Novel Ensemble-based Machine Learning Model for Anomaly Detection in CDRs to Identify International Revenue Share Fraud," in *7th European Conference on Industrial Engineering and Operations Management*, Augsburg, Germany, 2024.

[16] Khalid A. R., Owoh N., Uthmani O., Ashawa M., Osamor J., & Adejoh J., "Enhancing Credit Card Fraud Detection: An Ensemble Machine Learning Approach," *Big Data Cognitive Computing,* vol. 8, no. 6, 2024.

[17] Chaudhary A., & Behl S., "AI-Powered Systems for Detecting Financial Fraud in Real Time," *The Eastasouth Journal of Information System and Computer Science,* vol. 1, no. 2, pp. 132-139, 2023.

[18] Amuda O. K., Akinyemi B. O., Sanni M. L., & Aderounmu G. A., "A Predictive User Behavior Analytic Model for Insider Threats in Cyberspace," *International Journal of Communication Networks snd Information Security,* vol. 14, no. 1, pp. 150-159, 2022.

[19] Zhang Z., Yin H., Rao S. X., Yan X., Wang Z., Liang W., Zhao Y., Shan Y., Zhang R., Lin Y., and Jiang J., "Identifying E-Commerce Fraud Through User Behavior Data: Observations and Insights," *Data Science and Engineering,* vol. 10, pp. 24-39, 2025.

[20] Manas-stack13, "Access-Log-Anomaly-Detection-Dataset," 20 May 2025. [Online]. Available: https://github.com/Manas-stack13/Access-Log-Anomaly-Detection-Dataset?tab=readme-ov-file#readme.

[21] Udayakumar S. K., Ragothaman H., & Khare K. M., "A Novel Dataset and a Hybrid Ensemble Approach for Anomaly Detection in Enterprise-Access-Logs for Anomaly Detection," in *International Conference on Data Science, Agents, and Artificial Intelligence*, Chennai, India, 2025.

[22] Garcia V., Sanchez J. S., & Marques A., "Synergetic Application of Multi-Criteria Decision-Making Models to Credit Granting Decision Problems," *Applied Sciences,* vol. 9, no. 23, pp. 1-15, 2019.

[23] Saleh O., Ghazali O., & Al maatouk Q., "Graduation Certificate Verification Model: A Preliminary Study," *International Journal of Advanced Computer Science and Applications,* vol. 10, no. 7, pp. 575-582, 2019.

[24] Caramihai M., & Severin I., "A Blockchain-Based Solution for Diploma Management in Universities," *Sustainability,* vol. 15, no. 20, 2023.

.