IoT-Enabled Cyber-Physical Systems for Fraud Detection in Online Academic Evaluation

Yan Xing[1*]

[1*]Ministry of Science and Education, Nanchong Central Hospital, Nanchong, Sichuan, 637000, China.

Corresponding Author: Yan Xing, scnc2023@163.com

Abstract:

The integration of Internet of Things (IoT) technologies with Cyber-Physical Systems (CPS) has revolutionized various sectors, including online academic evaluation systems. IoT-enabled CPS can enhance security and reliability by providing real-time monitoring and interaction between physical and digital components. However, existing methods for fraud detection in online academic evaluation face challenges such as limited data transparency, delayed responses, and inadequate authentication mechanisms. These issues often result in manipulated assessments and undermine the credibility of academic evaluations. In the proposed method, an Internet of Things-based Fraud Detection (IoT-FD) system is introduced for online academic evaluation. The framework utilizes IoT sensors, devices, and data analytics to monitor user behaviour, track test-taking environments, and validate identities in real time. This approach ensures a higher level of detection by collecting data from multiple sources and analysing it using machine learning algorithms for anomalies or suspicious patterns. The proposed IoT-FD system offers enhanced fraud detection capabilities, providing educators and institutions with a robust solution to mitigate cheating, identity fraud, and score manipulation in online assessments. By leveraging IoT sensors and advanced data processing, this method ensures a more secure and transparent academic evaluation process. The findings demonstrate that the IoT-FD system significantly reduces fraudulent activities in online academic evaluations by providing real-time insights and adaptive detection mechanisms, thus ensuring the integrity and fairness of the evaluation process. This approach enhances the overall security of online education platforms by Fraud Identification (98.84%), Fraud Detection Accuracy (97.45), Real-Time Response (98.05%), Security and transparency (99.25%), User Authentication Effectiveness (98.26%), fostering a trustworthy academic environment.

Keywords: Online academic, Internet of Things, Cyber-Physical Systems, machine learning algorithms, fraud detection, evaluation process

1. Introduction:

Online academic evaluation systems have gained wide application because of the explosive expansion of online education. They enable students to take remote exams and receive instant feedback about their performance [1]. However, there are now significant barriers to maintaining the validity and trustworthiness of the assessment process due to this shift. There are so many procedures involved in manual identification verification through proctoring. Proctoring and other processes for manual identification verification are a history of inefficiency and human error in providing a guarantee for academic honesty [2]. These present numerous frauds such as plagiarism, manipulation of the score, and identity thefts against online academic assessments. Aside from throwing a doubt over the assessment's validity, the said problems also run public confidence down in schools and the overall online education [3]. There is now hope to address some of these issues through the integration of Cyber-Physical Systems with IoT technology. Internet of Things enabled connected physical systems integrate digital systems with physical sensors and devices to enable interaction and real-time monitoring [4]. It can improve the reliability and openness of online academic assessments by integrating data from several sources in real-time. To ensure that tests are distributed without bias and manipulation, for example, IoT sensors can record user actions, monitoring the testing environment and possibly confirming identities [5].

The current practices for fraud detection possess several shortcomings. Addressing the shortcomings, this IoT-FD system employs IoT devices, big data, and machine learning algorithms [6]. Overall tendency of this architecture is to protect the information integrity and ensures the reliability of the assessment through. This architecture provides increased security to online academic assessments with continuous monitoring of the test-taker's behavior and adaptive fraud detection techniques [7]. The IoT-FD system focuses on the reduction of the chances of fraud by offering a way to conduct evaluations that are vigorous enough to curb the chances of fraund allowing the online evaluations to be secure and trustworthy [8]. Answers are delayed, data are not transparent, and there are many human verification procedures, consequently they all hamper the existing models of detection of the frauds concerning the area of online learning programs [9]. Such failures cause a failure to penalize dishonest behavior, thus diminishing the trustworthiness and the trust of the assessments. So, there is a need to devise a more automated approach for tackling the problem of academic dishonesty which operates actively and instantly [10].

Motivation: There are grave concerns over the safety and validity of online academic exams since it has become increasingly popular. Traditional methods of fraud detection typically yield false results as they do not consider the evolving tactics employed by fraudsters. To enhance the reliability of online education platforms, the IoT-FD system is designed to offer a more reliable, real-time solution that ensures a safe and transparent process for academic assessment.

Problem statement: Duplicitous, detect theft, and score manipulations are significant issues about online academic assessments. Current detection methods of fraud do not allow real-time monitoring to adequately authenticate and properly analyze available data, thereby undermining assessments integrity. This is what reduces the credibility of online assessments in educational institutions. There exists a need for a far safer, open, flexible fraud detection system.

Contribution of this paper,

- Introduces an innovative IoT-based fraud detection system that leverages real-time data from sensors and devices to enhance security and transparency in online academic evaluations.
- Develops a robust system for continuous monitoring of user behaviour and environment, utilizing machine learning algorithms to identify fraudulent activities and suspicious patterns in real-time.
- Provides a secure and reliable solution for online academic evaluations, ensuring academic integrity by effectively preventing cheating, identity fraud, and manipulation of scores in digital assessments.

The remaining of this paper is structured as follows: In section 2, the related work of Fraud Detection in Online Academic Evaluation is studied. In section 3, the proposed methodology of IoT-FD is explained. In section 4, the efficiency of IoT-FD is discussed and analysed. Finally, in section 5 the paper is concluded with the future work.

2. Related Work:

By combining digital and physical sensors, Internet of Things-enabled Cyber-Physical Systems provide a strong answer to the problem of academic assessment fraud in online formats. These tools make it possible to validate identities, keep tabs on test environments, and track user activity in real time. By using the Internet of Things and machine learning, they improve the ability to identify fraud, making online evaluations more trustworthy, transparent, and safe while decreasing instances of manipulation and cheating.

Artificial Intelligence based Fraud Detection (AI-FD):

A survey of the research on the difficulties that cyber physical systems face while using AI technologies, both now and in the future. An overarching goal of this literature study is to provide a theoretical framework for bolstering technological and human resilience via the use of AI and automation by Radanliev, P. et al., [11]. The approach used was similar to a taxonomic study and literature assessment of intricate cyber physical systems that are linked and interdependent on the IoT. Academic and technical publications are giving more space to ideas on IoT frameworks, models, and infrastructures by Rajawat, A. S. et al., [12]. The Industrial Internet of Things, and other similar systems and technologies are often juxtaposed in these papers and publications. The findings provide a novel conceptual framework for studying the development of AI decision-making in cyber physical systems, based on hierarchical cascading by Alohali, M. A. et al., [13]. The growing number of interconnected devices in cyber physical systems makes this kind of development both inevitable and self-governing. As evidence, this argument makes use of a taxonomy technique that has been modified and implemented to provide clarity and rationale for the selection of ideas. This is achieved by creating summary maps, which are then used to develop a hierarchical cascading conceptual framework by Jeffrey, N. et al., [14].

Machine Learning based Fraud Detection (ML-FD):

To integrate cyber sections into the physical world, Cyber-Physical Systems have a large variety of complicated multi-tasking components that interact closely with one another. With the proliferation of smart features and communication tools, as well as the meteoric rise of cyber-physical systems, new obstacles have arisen by Mohammadi Rouzbahani, H. et al., [15]. This is especially true for the new generation of CPSs, such the smart grid, which are subject to a wide variety of assaults and vulnerabilities. Consequently, privacy and security pose the greatest threats to these systems by Tan, Q. et al., [16]. As a data analysis job, anomaly detection is crucial for CPSs security. Given the variety of anomaly detection technologies offered, evaluating their relative merits becomes a daunting task. Lastly, a case study shows how successful machine learning approaches are at identifying False Data Injection assaults, and how ML methods for anomaly detection work by Almajed, R. et al., [17]. Software and hardware work together in what are known as cyber-physical systems. Industry control systems, smart power grids, remote laboratory settings, telemedicine, autonomous cars, smart manufacturing, the internet of things, and many more areas have contributed to CPS's explosive expansion over the last decade by Ahmed, A. et al., [18].

Deep Learning based Fraud Detection (DL-FD):

Protecting cyber-physical systems requires anomaly detection. Traditional anomaly detection approaches, however, are ill-equipped to deal with the rising data volumes and domain-specific information requirements posed by more complex CPSs and more sophisticated assaults by Luo, Y. et al., [19]. This is why there have been suggestions for DLAD approaches, which use deep learning. Here it has a look at the most recent and cutting-edge DLAD techniques used in CPSs. To help comprehend the key features of existing approaches by Zhang, J. et al., [20]. It provides a taxonomy based on the kind of anomalies, tactics, implementation, and assessment measures. In addition, highlight new features and designs in each CPS domain using this taxonomy. The downsides and unanswered questions of these approaches by Moriano, P. et al., [21] In addition, empirically investigate the features of standard neural models, the DLAD method workflow, and the DL model execution performance to provide users with insights into selecting appropriate DLAD techniques in practice. By outlining the shortcomings of DL techniques, results, and potential future research avenues that might enhance DLAD methods by Almajed, R. et al., [22].

Data Mining based Fraud Detection (DM-FD):

There has been a lot of focus in the data mining community on knowledge extraction from sensor data for different applications. Due to the detection quality, it is tough to use continuous incoming data for event detection in cyber-physical systems, such as damage in buildings or aerospace vehicles by Bhuiyan, M. Z. A. et al., [23]. To discover valuable information about an event, traditional data mining techniques frequently use metrics, association rules, and binary values for common patterns as indicators to decrease data. Nevertheless, certain limitations in the network's capabilities may prevent its direct implementation by Han, S. et al., [24]. As it finds out, the indications may not really provide us anything useful when it comes to actually detecting events. a novel approach to mining sensor behavioural patterns, differential sensor patterns. DSPs consider non-binary values and frequencies associated with a group of sensors, as opposed to the more conventional binary patterns by Alwan, A. A. et al., [25]. Table 1 shows the comparison of existing work merits and demerits.

Table 1: The Summary of Related Work

S. No	Methods	Authors	Advantages	Limitations
1	AI-Based Fraud Detection (AI-FD)	Radanliev, P. et al.	Provides a hierarchical cascading framework for AI decision-making in CPSs.	Complexity in implementing taxonomic studies in intricate CPSs.
		Rajawat, A. S. et al.	Explores IoT frameworks and models for CPS interconnectivity.	Limited to theoretical studies without real-world scalability validation.
		Alohali, M. A. et al.	Demonstrates inevitability of interconnected devices in CPS.	Relies on modified taxonomy without extensive experimental data.
		Jeffrey, N. et al.	Uses summary maps to clarify conceptual frameworks.	Frameworks may lack adaptability to evolving CPS complexities.
2	ML-Based Fraud Detection (ML-FD)	Mohammadi Rouzbahani, H. et al.	Effective anomaly detection for False Data Injection attacks.	Evaluation of anomaly detection technologies remains a daunting task.
		Tan, Q. et al.	Highlights privacy and security threats in CPSs.	Focuses mainly on challenges without fully addressing solution integration.
		Almajed, R. et al.	Showcases ML's success in anomaly detection for CPS security.	Requires extensive computation and real-time applicability validation.
		Ahmed, A. et al.	Explains CPS growth in varied domains like IoT and autonomous systems.	Insufficient focus on specific ML models' adaptability to diverse CPSs.
3	DL-Based Fraud Detection (DL-FD)	Luo, Y. et al.	Introduces DLAD approaches for handling complex CPS data.	Traditional DL techniques struggle with domain-specific and large-scale data.
		Zhang, J. et al.	Offers taxonomy for anomaly types and DL techniques in CPS.	Limited exploration of specific DL models' weaknesses.
		Moriano, P. et al.	Identifies gaps in DLAD methods and provides future research directions.	Lacks solutions to overcome DL models' execution and scalability challenges.
		Almajed, R. et al.	Explores neural model features and DL workflow for anomaly detection.	Potential solutions remain theoretical, with limited practical case studies.
4	DM-Based Fraud Detection (DM-FD)	Bhuiyan, M. Z. A. et al.	Extracts knowledge from sensor data for event detection in CPS.	Event detection quality struggles with continuous incoming data.
		Han, S. et al.	Uses metrics and association rules to reduce sensor data for event insights.	Indicators may not offer sufficient utility for accurate event detection.

		Alwan, A. A. et al.	Introduces Differential Sensor Patterns (DSPs) for non-binary sensor data.	Network limitations may hinder direct DSP implementation.

Delves into several techniques to fraud detection in cyber-physical systems using AI, ML, DL, and DM. Some of the problems highlighted include security, anomaly detection, and scalability. Analysis of sensor behaviour, taxonomy-based frameworks, and anomaly detection approaches provide light on gaps and future research objectives in linked IoT-driven systems, with the goal of enhancing detection quality, decision-making, and resilience.

3. Proposed Method:

The suggested solution takes use of federated learning to improve privacy by training models on dispersed devices without exposing raw data. To find coordinated fraudulent activity, advanced methods such as graph neural networks examine the links among the discovered abnormalities. Resilience against new forms of academic assessment fraud is guaranteed by adaptive learning processes that tweak detection algorithms in real time.

Contribution 1: Data Acquisition Layer

IoT devices, such as biometric sensors, cameras, and keystroke recorders, collect real-time behavioural and environmental data during online evaluations. These devices monitor parameters like typing patterns, facial expressions, eye movement, and ambient conditions to identify anomalies indicative of potential fraud.

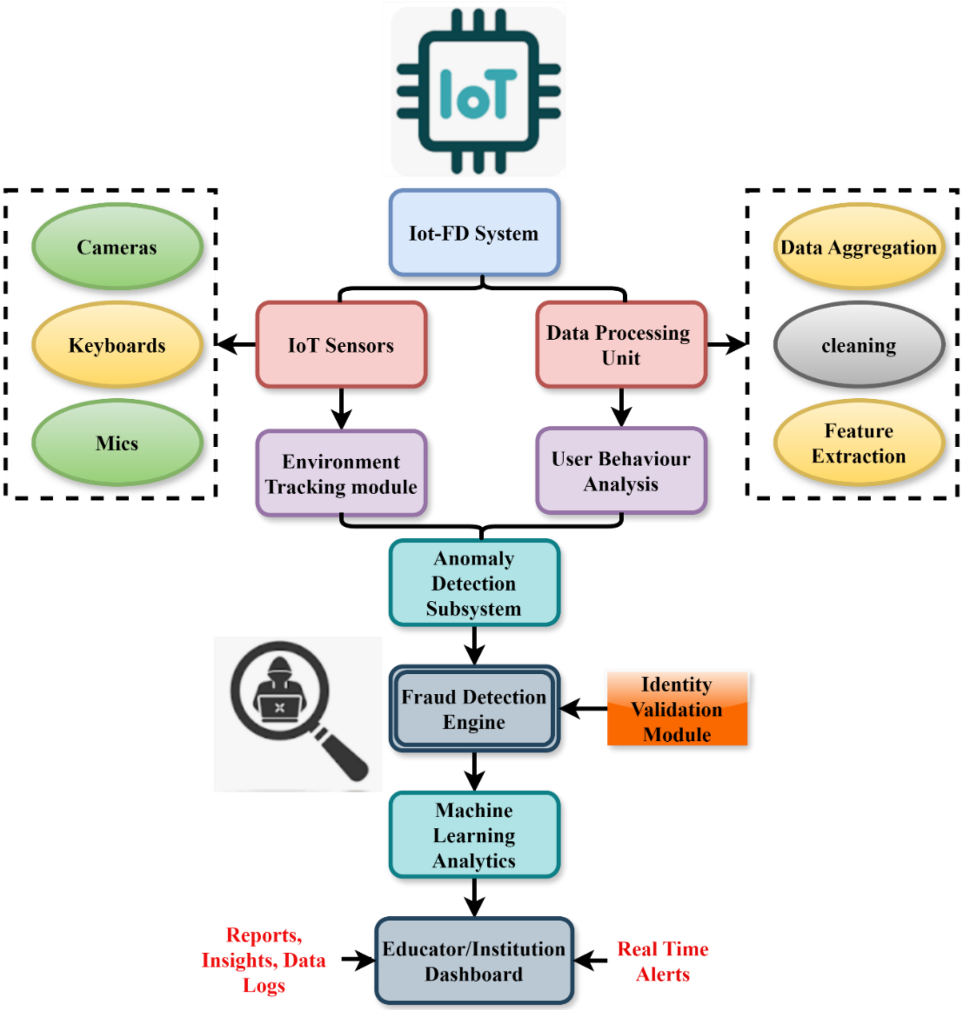

Figure 1: The Block Diagram of IoT-based Fraud Detection

The IoT-FD System incorporates advanced IoT sensors and devices, which capture a wide range of data including environmental metrics, user interactions, and biometric inputs. Data flows into the collection and preprocessing unit for aggregation, cleaning, and feature extraction. The major modules are Environment Tracking, User Behaviour Analysis, and Anomaly Detection, which employ sensor data fusion and comparisons to identify irregularities. The Fraud Detection Engine makes real-time adaptive decisions using machine learning. Biometric and multifactor authentications ensure identity validation, while insights are presented by educator dashboards and a subsystem of notifications and logs. These all add up to build a system's feedback loop that enhances performance with high fraud detection and user-interaction insights is shown in figure 1.

$$\partial[m, yt'']: \rightarrow n(l - vd'') * Na[2fh - bq''] + Ba[4f - n'] \qquad (1)$$

The parameters, including the observed user habits ($n(l - vd'')$), response time ($Na[2fh - bq'']$), and contextual deviations ($\partial[m, yt'']$), are integrated in the equation 1. To efficiently identify fraudulent patterns, it measures anomalies by linking components such as information from sensor intakes ($[4f - n']$) and statistical analysis Ba. The machine learning algorithms in the system are built which allows for accurate, real-time fraud detection and improves the integrity of evaluations.

$$D^G g[L - nsd'']: \rightarrow Ma[3 - fkm''] + 5\ Ds[4v - FK''] \qquad (2)$$

Noise in the environment ($D^G g$), linking system deviations ($[L - nsd'']$), and fraud markers ($[3 - fkm'']$) by the equation 2 as they impact the constantly changing administration (Ma) of data collected by IoT sensors ($5\,Ds$). Anomaly detection is enhanced by using multi-source inputs such as sensor parameters $[4v - FK'']$ and variances thresholds. Accurate fraud detection in real-time academic assessment settings is made possible by this equation's provision for adaptive monitoring.

$$\propto_g D[l - do'']: \rightarrow Ma[2fn -] + a[r - nw''] - vcAV[L - CK''] \qquad (3)$$

The equation 3 depicts $Ma[2fn -]$ the relationship between system dynamics ($[l - do'']$) and environmental deviations $\propto_g D$ caused by the Internet of Things (IoT) with the objective to identify abnormalities. To ensure precise detection, it incorporates adaptive responses (\(a\)) and fraud markers ($a[r - nw'']$) while reducing contextual variances ($vcAV[L - CK'']$). The capacity of the IoT-FD system to detect and understand anomalies in behavior and disturbances in the surrounding environment is enhanced by this approach.

$$E_T r[V - gl'']: \rightarrow Ma[3vf - FVL - mw''] + 7\,vwA'' \qquad (4)$$

The electricity threshold ($E_T r$) for Internet of Things (IoT) sensors ($[V - gl'']$) to identify fraudulent actions $-FVL - mw''$ is captured by the equation 4. The detection accuracy is improved by correlating volumetric fraudulent activity markers (Ma) and parameter adaptations ($3vf$), while also factoring in environmental impacts ($7\,vwA''$). Improved real-time fraud identification and system dependability in academic assessments are achieved by ensuring the IoT-FD solution dynamically changes sensor responses using this equation.

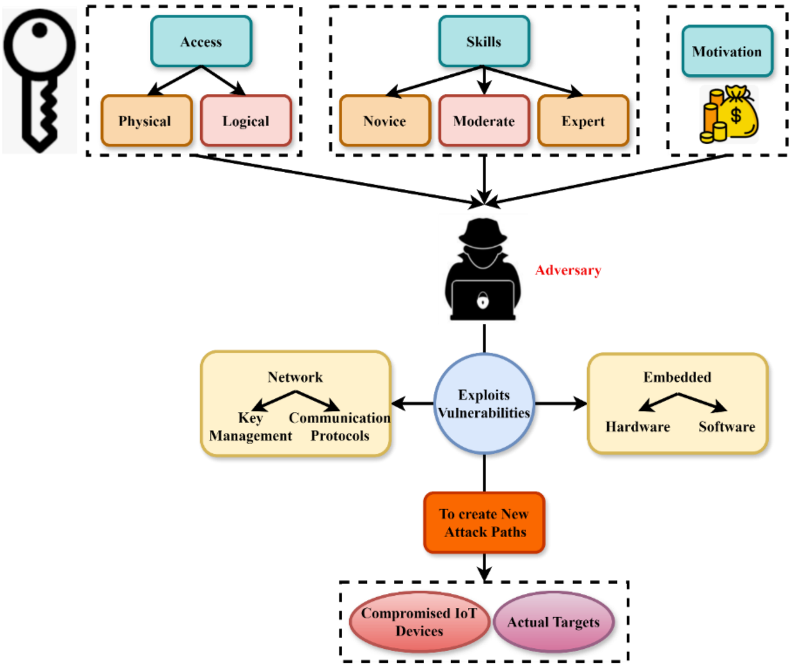

Figure 2: Adversary Threat Model in IoT Security

Access, skills and motivation are factors that make certain attacks possible in the adversary threat model in IoT security. The adversary might aim to use either physical or logical access to IoT devices. Their skills from novice to expert, and even the desire for monetary reward. New attack modalities have been constructed by adversaries through network construction that directs their focus on weaknesses in numerous parts of the network such as key management, communication protocols as well as other embedded hardware and software systems. It then connects the compromised IoT devices with the actual targeted entities which pose a major threat. Such dynamics are important in the design of robust IoT systems as well as the provision of necessary countermeasures against the predicted security violation in figure 2.

$$\propto_m \ll x - v'' \gg : Nas[4fg - Nqe''[l - xp''] + 7Vad'' \qquad (5)$$

Incorporating analytics from Internet of Things (IoT) sensors (Nas) and environmental factors ($x - v''$), the device's adaptive responsiveness ($\propto_m$)) to changing parameters ($4fg - Nqe''$) is represented by the equation 5. For successful anomaly detection, it integrates fraud formation features ($Nqe''[l - xp'']$) and validator adjustments ($7Vad''$). Ensuring solid academic evaluation security, this equation increases the IoT-FD system's capacity to adaptively observe and respond to complicated fraudulent actions.

$$\ll fF_g \gg +njF[dl - 6df'']: \rightarrow\ nF[d - sp''] + 4W[m - ng''] \qquad (6)$$

The equation 6 shows the combination of fraudulent factors ($\ll fF_g \gg +$) and inputs for noise-justified fraud ($njF[dl - 6df'']$) that are obtained from sensor variances ($4W$). To identify suspicious actions ($nF[d - sp'']$), it assesses thresholds for detection and external weights ($[m - ng'']$). By incorporating multi-factorial data, this model improves the accuracy and flexibility of fraud detection through the internet academic assessments, which in turn improves the IoT-FD system.

$$\propto_V F[k - er''[Lefk]: \rightarrow\ Ma[3md - f''] +\ 6baf[4v - d''] \qquad (7)$$

The deviation markers ($\propto_V F$) affected by environmental and sensing factors ($k - er''[Lefk]$) are identified using the equation 7 that describes the system's varied adaptation ($6baf[4v - d'']$). It efficiently detects fraud by combining anomaly signals ($Ma[3md - f'']$) and psychological analysis. This equation improves the IoT-FD system's capacity to detect and prevent fraudulent activities by making use of adaptive thresholds.

$$\forall' \propto [m - ne'']: \rightarrow\ Ma[4v - Fm''] +\ 5bsd[3v - fl''] \qquad (8)$$

To be able to analyze monitored network components ($[m - ne'']$) for the identification of fraud, the equation 8, $5bsd[3v - fl'']$ models' ubiquitous adaptability ($4v - Fm''$). To find vulnerabilities, it uses anomaly identifiers ($\forall' \propto$) and behavioral-sensor variations (Ma). This equation ensures accurate and adaptive identification of fraudulent activities in online academic assessments, bolstering the reliability of the IoT-FD system.

In summary, IoT adversaries exploiting access, skills, and motivation to target vulnerabilities in networks and embedded systems, creating attack paths that compromise devices and actual targets.

Contribution 2: Processing and Analysis Layer

Data gathered by IoT devices is sent to edge servers where anomaly detection algorithms reside. This layer employs ML models to recognize patterns and deviations from standard behaviors. More complex use cases may make use of DL-based techniques, specifically convolutional neural networks or recurrent neural networks, used for video or behavioral patterns in real time. All this has a hierarchical cascading structure not to overload any particular function.

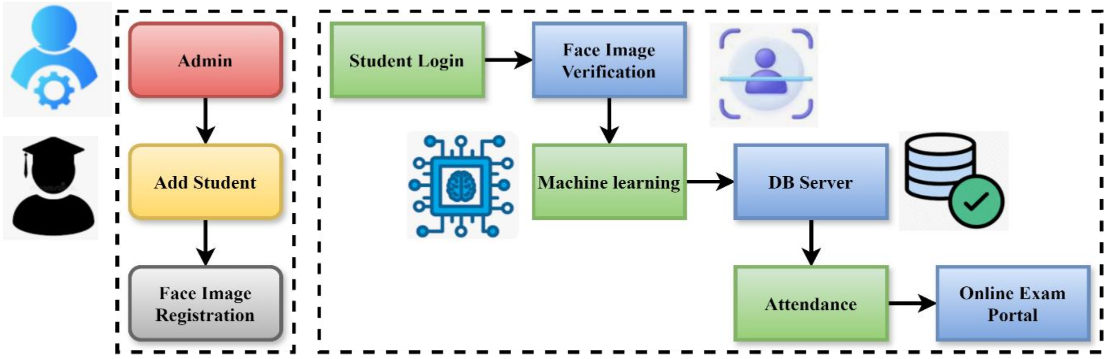

Figure 3: Face Recognition-Based Online Exam Management System

A face recognition-based system for online exam management. Beginning by administering this module, the admin processes it by adding the faces of students to the data warehouse. Students log on, having access to a well secured portal, and undergo verifications of their images employing a machine learning algorithm to pass down only legitimate records to the DB server which stores the same thereby enhancing authenticity and accuracy and this shall facilitate automatic marking of their presence. The system will be integrated with an online exam portal. This enables students to take part in the exam safely. This automation of the workflow increases efficiency, decreases administrative overheads, and creates a secure online environment for taking examinations. It uses advanced machine learning and database technologies for increased accuracy and reliability. See figure 3.

$$V_f R[5v - Nt'']: \rightarrow Mw''[l - cp''] + 6hd[o - dn''] \qquad (9)$$

Based on the sensor variances ($V_f R$), the factor for velocity ($[5v - Nt'']$) and its link to the system responses Mw'' are represented by the equation. To identify anomalies that are peculiar to a certain environment $[o - dn'']$, it uses watched weights ($[l - cp'']$) and extremely complex attributes ($6hd$). The reliability of online student assessments is guaranteed by this equation, which improves the IoT-FD system with adaptive fraud detection and dynamic environmental indicators.

$$xZa_{[;f=g'']}: \rightarrow Ma[4D - vx''] + 7\,vaw[n - qpe''] \qquad (10)$$

The relationship between essential variables in the system ($Ma[4D - vx'']$) and anomalies parameters ($xZa_{[;f=g'']}$) affected by elements that generate fraud ($7\,vaw$) is represented by the equation 10. To identify abnormalities in query generation environments it blends abnormal markers ($[n - qpe'']$) with variable adapt weights. This equation enhances the IoT-FD system's ability to identify academic assessment fraud by responding dynamically to data discrepancies.

$$e_G d[w - ns'']: \rightarrow ma[g - mn''] + 4mD[2bx - kn''] \qquad (11)$$

The power gradient ($e_G d$) representing the correlation between system variations ($4mD$), fraud flags ($[w - ns'']$), and dynamic system behavior ($ma[g - mn'']$) in identifying anomalies is shown by the equation. In an effort to improve fraud detection, it blends environmental indicators ($2bx - kn''$) with contextual adaptations. This equation 11 improves the IoT-FD system's fraud detection capabilities via system behavior adaptation.

$$g_t R[lh - en'']: \rightarrow nA[4mf - v''] + 4fa[3fg - vb''] \qquad (12)$$

The reaction of the equation 12 system over time ($g_t R$) to external variables ($[lh - en'']$) in identifying fraudulent activity $4fa$. It finds problems with the system's behavior (nA), $[4mf - v''])$ by combining anomaly analysis (nA) with fraud detection parameters ($3fg - vb''$). By improving the IoT-FD system's fraud detection capabilities, this equation guarantees that academic evaluations are conducted with integrity.

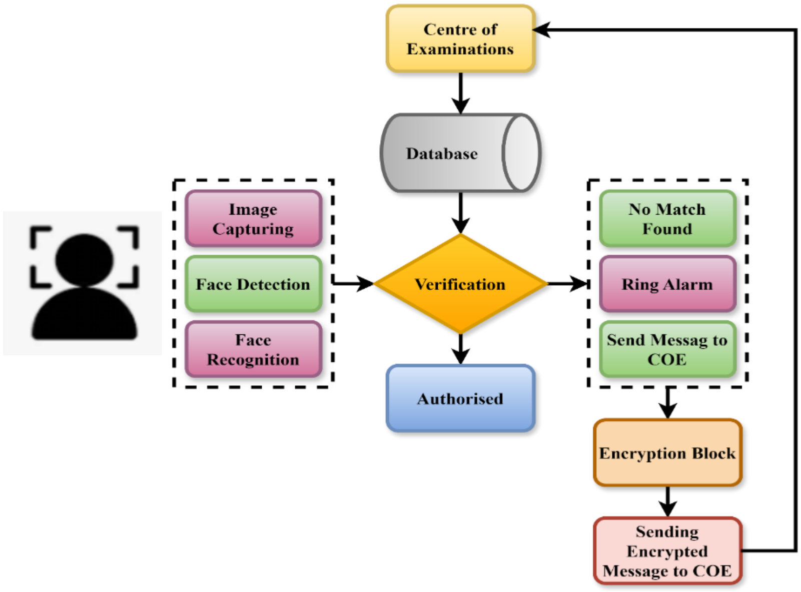

Figure 4: Face Recognition-Based Authentication System for Examination Security

It is an image-based authentication system for any examination centre. The working of the system starts by capturing images, followed by face detection and recognition, and then comparing the same with the database for verification. If the face matches to an authorized record, a person gets access to examinations resources. If no record is found, an alarm signal is sent, and an SMS is sent to COE for further action. The encryption block encrypts the messages before sending them to the COE, thereby ensuring data security. This system enhances examination security through advanced face recognition technology, where only authorized people are allowed, and immediate alerts and encrypted communication for efficient issue resolution is shown in figure 4.

$$e_g s[4vd - Nz'']: \rightarrow Ma[3sf'' + 8vJ''] - cA[4vf - 3aq''] \qquad (13)$$

The energy gradient $e_g s$ may be represented by the equation 13 in the context of analyzing sensor data ($4vd - Nz''$) to identify irregularities in academic assessment systems. It considers counteracting fraud measures (Ma) to improve detection and connects fraud markers ($3sf'' + 8vJ''$) with sensor feedback ($cA[4vf - 3aq'']$) and contextual adjustments (vJ" \). The capacity of the IoT-FD system to detect fraudulent activities and guarantee system integrity via dynamic, real-time analysis is enhanced by this equation.

$$\varepsilon_r T[lo - 3v'']: \rightarrow Js[4d - nq''] + 8bf[l - 2ep''] \qquad (14)$$

The response threshold for monitoring information from sensors ($\varepsilon_r T$) for the purpose to identify fraudulent actions $[l - 2ep'']$ is represented by the equation 14, ($[lo - 3v'']$). It improves the accuracy of detecting fraud by combining behavioral characteristics ($Js[4d - nq'']$)) with signals for fraud detection $8bf$. The IoT-FD system is bolstered by this equation, which allows for adaptive monitoring, guarantees the identification of fraud in real-time, and keeps online academic assessments honest.

$$\propto_e F[3s - zl'']: \rightarrow Ja\big[3v - Fv[l - js'']\big] + 9\,vdr[L - IU''] \qquad (15)$$

With an emphasis $9\,vdr[L - IU'']$ on identity authentication ($\propto_e F$) and the natural world ($\big[3v - Fv[l - js'']\big]$), the equation 15 adaptation factor ($[3s - zl'']$) analyzes fraud-related facts (Ja). By streamlining the detection process, this equation 15 ensures the real-time the recognition of fraud and improves the security associated with digital academic assessments, strengthening the IoT-FD system.

$$v_{FR}[L - vf'']: \rightarrow mN[4qf - bf''] + Nw[NX - xr''] \qquad (16)$$

With the goal to identify inconsistencies in the system's behavior, the fraud reply vector (v_{FR}) is modeled by the equation 16, which analyzes input variations ($v_{FR}[L - vf'']$). To be able to detect fraudulent actions, it incorporates track factors (mN) and weights depending on the network ($Nw[NX - xr'']$). This equation improves the IoT-FD platform by using multi-source statistical analysis to spot irregularities and guarantee the security and integrity in real-time.

In summary, Exam centres are protected by this facial recognition-based authentication system, which compares taken photos to a database. While mismatches result in warnings and notifications, authorized individuals are granted access. Data security is guaranteed via encrypted transmission, which also improves dependability and guards against unwanted access.

Contribution 3: Decision and Action Layer

Based on the analysis, the system flags suspicious activities for further review. A feedback loop integrates human oversight to validate and improve the model's decision-making accuracy over time.

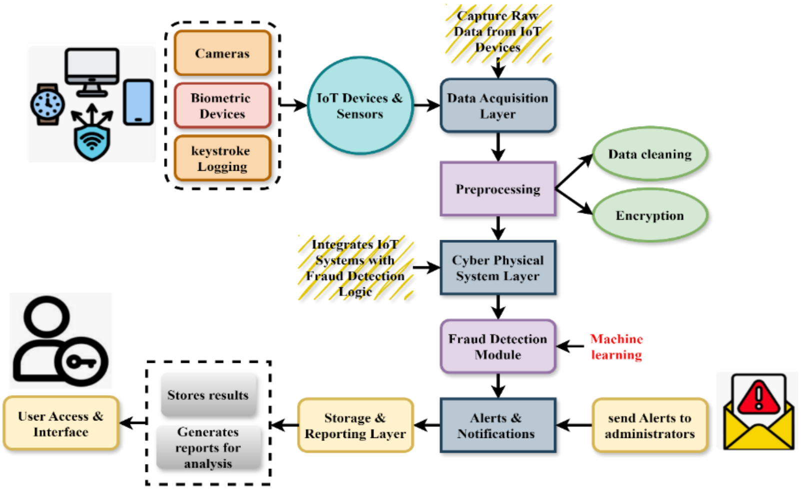

Figure 5: IoT-Driven Fraud Detection System Architecture

IoT devices and sensors, such as cameras, biometric devices, and keystroke loggers, play a crucial role in collecting real-time data for applications such as security and fraud detection. These devices feed raw data into the Data Acquisition Layer, which captures and forwards it to be further processed. Data in the Preprocessing Layer is cleaned, normalized, and encrypted to ensure privacy and usability. The Cyber-Physical System Layer combines the IoT systems with fraud detection mechanisms, which may be in the form of AI/ML models that use anomaly detection and behavioural analysis. Once the fraud has been detected, the Alert and Notification System sends the alert to the administrators. The Storage and Reporting Layer stores the results and provides reports. Lastly, the User Access and Interface layer provides the access for administrators through dashboards to monitor and evaluate is shown in figure 5.

$$\propto_v F[l - pfg'']: \to Nw[g - rl''] + Nf[gj - nk''] \qquad (17)$$

By comparing system indicators with fraud indicators, the equation 17 reflects the modification factor ($\propto_v F$) in assessing data connected to fraud ($[l - pfg'']$). It improves the system's capacity to detect harmful actions by combining weights of the network ($Nw[g - rl'']$)) with recognition of fraud feedback $Nf[gj - nk'']$. By improving learning process, this equation 17 enhances the IoT-FD system, guaranteeing precise and instantaneous fraud detection.

$$n_f[-fm' + wn'']: \to Kd[2f - bf''] + 9\,VG[2xa - vd''] \qquad (18)$$

By assessing system performance deviations (n_f) and connecting them with fraud identification characteristics $[2xa - vd'']$, the fraud identification system $(fm' + wn'')$ is represented by the equation. To improve the precision of detecting suspicious patterns, it uses certification groups $(Kd[2f - bf''])$ and key to identify fraudulent data $(9\,VG)$. By allowing efficient real-time fraud detection, this equation 18 enhances the IoT-FD system.

$$v_S F[l - pf'']: \rightarrow nJ[4w - cza''] + 9\;vf[l - pu''] \qquad (19)$$

To be able to recognize unusual patterns in user behavior $[4w - cza'']$, the system's reaction $(v_S F)$ is represented by the equation 19, which takes identifying fraud data (nJ). The possibility of fraud may be assessed in real-time by integrating judgmental research $(9\;vf[l - pu''])$ and proof factors $([l - pf''])$). Online academic assessments may be more confidently administered to this equation, which improves the IoT-FD system's fraud detection capabilities.

$$v_F[l - pdv'']: \rightarrow Kd[vn - DKI''] + 6wR[L - FI''] \qquad (20)$$

Correlating sensor data $([l - pdv''])$ with fraud identification criteria $[L - FI'']$, the equation 20 generates the fraud detecting vector (v_F). The purpose of integrating $6wR$ the detection of fraud key data (Kd) and evaluation of risk factors $([vn - DKI''])$ is to enhance anomaly detection. Online academic assessments are made more secure and reliable with the help of this equation, which improves the IoT-FD system and allows for more accurate real-time detection of fraudulent actions.

In summary, this is IoT sensors and fraud detection devices using pattern matching, ML models, preprocessing, and data collection. These give users access to monitoring dashboards, save for analysis, and notify the administrator when it is discovered.

4. Result and discussion:

The Internet of Things, combined with Cyber-Physical Systems, makes online academic assessment way more effective by providing real-time monitoring and fraud identification. An IoT-FD system in the proposed method will maintain secure, transparent, and trustworthy assessment procedures via machine learning, data analytics, and Internet of Things sensors that identify abnormalities against identity theft.

Dataset Description: The Fraud Detection Database that wants to research and understand various types of fraud. In this database, there are lots of anonymous financial transactions with a huge amount of records in below table 2. All the information about merchants, quantities, fraudulent tendencies, customers, and transactions are included. It may be used in researching fraudulent activities, tracing signs of fraud, and building effective algorithms for the detection of fraud. It may also be used for understanding all the mysteries of financial fraud [26].

Table 2: The Simulation environment

Metrics	Description
Dataset	Anonymized financial transactions, including merchants, quantities, fraudulent tendencies, customers, and transactions.
Data Source	Financial transaction data (real-time or historical data) from various merchants and customers.
Key Features	Merchant info, transaction details, customer demographics, fraud indicators, transaction amounts, timestamps.
Fraud Detection Techniques	Machine learning algorithms (e.g., SVM, Random Forest, Neural Networks), anomaly detection, clustering, and pattern recognition.
Model Validation	Cross-validation (K-fold, stratified), confusion matrix analysis.
Real-Time Processing	Simulation of real-time transaction stream for fraud detection algorithms

Evaluation Criteria	Detection accuracy, false positives/negatives, model scalability, and response time for real-time fraud detection.

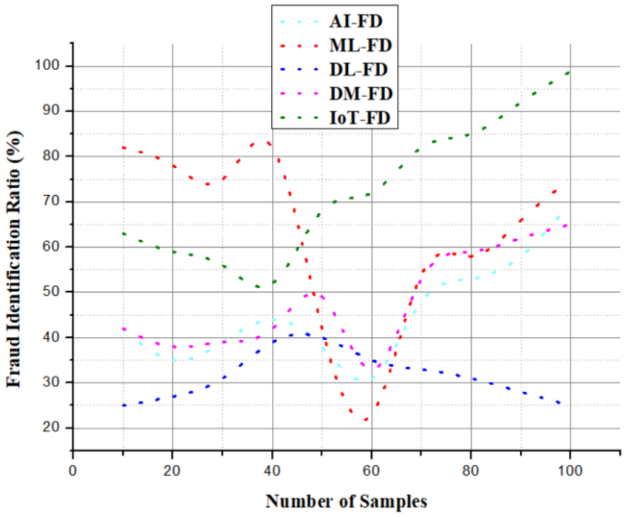

Figure 6: Analysis of identity fraud

The analysis of identity fraud in online academic evaluations has to be done to ensure the integrity of the assessment. In the proposed IoT-FD system, real-time monitoring using IoT sensors and devices is utilized to achieve identity verification. These technologies track the behavior of a user, authenticate credentials and then attempt to detect impersonation or unauthorized access that is as explained in equation 21. The patterns that indicate identity fraud will be highlighted by the machine learning algorithm in the collected data including inconsistent behavior and mismatch authentication information. The system offers real-time fraud detection by continuously monitoring and cross-referencing identity data, thereby reducing the risk of identity fraud in online academic evaluations, ensuring fairness and trustworthiness. The fraud identity is achieved by 98.84% is shown in figure 6.

$$4_{V}F[l-pgf'']:-.3f[l-rpg'']+\ 9\,vg[D-fds''] \qquad (21)$$

To improve detection accuracy $[D-fds'']$ and account for irregularities $(3f[l-rpg'']$, the equation 9 incorporates a factor $(4_{V}F)$ and represents the detection of fraud vector $([l-pgf''])$ applied to the data inputs $(9\ vg)$. This equation optimizes the fraud discovery process, which enhances the IoT-FD system on the analysis of identity fraud.

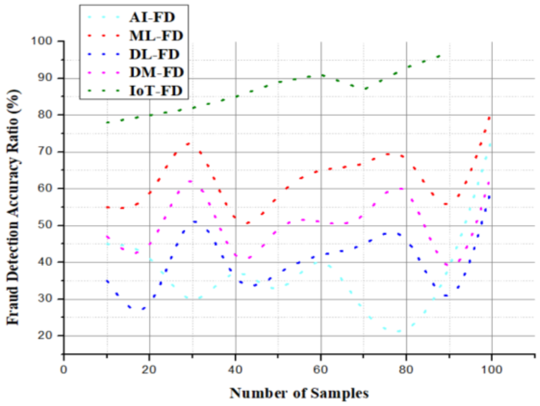

Figure 7: Analysis of Fraud Detection Accuracy

Within the IoT-FD system, the primary question of fraud detection accuracy analysis is how effectively it detects cheating during the online academic evaluations. The condensation of IoT sensors, real time data collection and machine learning algorithms enables the system to watch over users and tests' surrounding areas for suspicious behaviors and irregularities as elaborated in equation 22. Hence, the system can be evaluated in terms of how effective it was able to detect the crime with minimum false positive and false negative rates. Early detection of le3gally changing the test scores and impersonating a candidate would lead to high detection of cheating and fraud. This high accuracy in the detection of malpractice provides confidence in the robust mechanisms that prevent malpractice from occurring in assessments that are conducted online. The fraud detection accuracy ratio is gained by in figure 7 is illustrated 97.45%.

$$r_g G[4n - fL'']: \rightarrow n[3qe - mk''] + 8\, ve[v - smk''] \qquad (22)$$

The outcome function ($r_g G$) in identifying patterns $[v - smk'']$ of online academic assessment fraud is represented by the equation, where $4n - fL''$ reflects the behavior of the system and $n[3qe - mk'']$ integrating authentication data. The detection accuracy is enhanced by adding extra verification feedback due to $8\, ve$. This equation fortifies the IoT-FD infrastructure by enhancing the real-time detection and analysis of fraud detection accuracy.

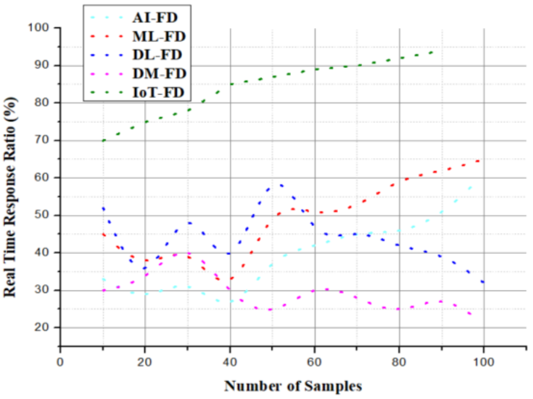

Figure 8: Analysis of Real-Time Response

The performance of the IoT-FD system to observe and identify behavioural patterns of fraud during the online academic assessments with regard to time is also investigated which consists of real time reaction time analysis. To eliminate the instances of fraud in the first place, this system utilizes IoT sensors and gadgets so that all activities of the users, test conditions, and their indentities are monitored in real time and appropriately described in equation 23. It is the feedback rate that determines how fast and effective the response time is to blocking further incidents.

Since the system is proficient at interpreting, it is also able to long with the detection assist the identification of suspicious actions for timely control. This functionality aims to enhance the security of online assessments by identifying and correcting fraudulent actions during an assessment process. Figure 8 shows the real-time response obtained which is 98.05%.

$$\varepsilon_4 G[l - 3jf'']: \rightarrow nAE[g - 5tv''] + 8\, Vj[L - Ife''] \qquad (23)$$

To identify possible signs of fraud, the equation 23, $[L - Ife'']$ depicts the process of using a fraud detection technique $\varepsilon_4 G$ to examine patterns in user information $[l - 3jf'']$. While $nAE[g - 5tv'']$enhances the verification process, the term $8\, Vj$ is centered on detecting fraudulent activity. By strengthening the IoT-FD system's capacity to identify and thwart fraud in real-time, this equation guarantees the analysis of real-time response.

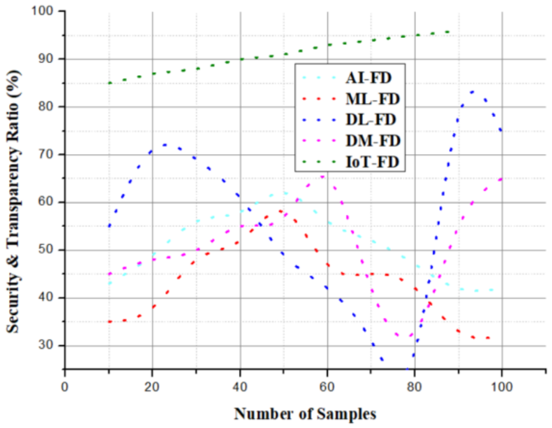

Figure 9: Analysis of security and transparency

The analysis of security and transparency of the system IoT-FD is centered on the integrity of the online examination system for the academic evaluation. The security framework expands on twitter attacks to utilize a combination of IoT sensors and data analytics to accurately assess the test being taken and environments where it is taken to mitigate breaches in real time as per description in equation 24. This is particularly appealing because transparency is informed by traceable and detailed information on every single assessment and hence educators and institutions can evaluate and verify outcomes. Therefore, the system is supposed to have strong secured measures in terms of identity verification and anomaly deterrent to reduce manipulation since all the required participants will take part. This fosters confidence within the evaluation process while both the security and transparency aspects have been enhanced in the case of online assessment. Figure 9 portrays the security and transparency ratio that improved to 99.25%.

$$\forall_3 g[L - nf'']:\rightarrow nS[V - 3Wl''] + 8\ vdr[2r - 3vx''] \qquad (24)$$

Based on data ($\forall_3 g$) analyzed for fraud patterns $[2r - 3vx'']$ and correlated with suspicious behaviors, the equation depicts the dynamic detecting process ($[L - nf'']$) in the IoT-FD system. By modifying detection thresholds, the 8 vdr improves the system's reaction, and $nS[V - 3Wl'']$ adds more data for risk assessment. The capacity of the IoT-FD system to detect irregularities in academic assessments is enhanced by this equation, which enhances analysis of security and transparency.

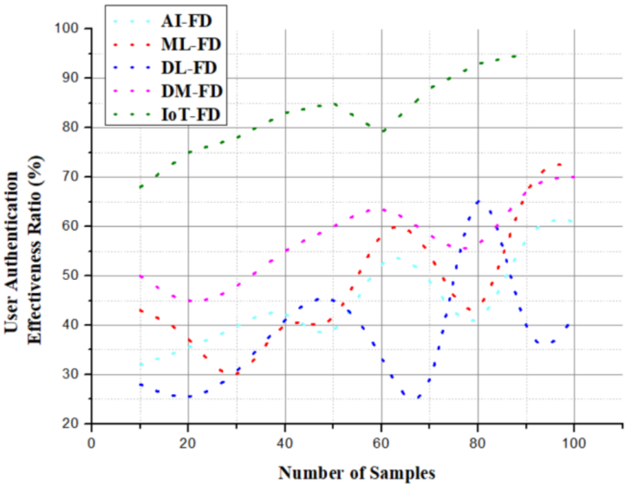

Figure 10: Analysis of User Authentication Effectiveness

This paper investigates the IoT-FD system's user authentication efficiency by examining its capacity in successfully authenticating students who are undertaking examinations on the internet. The system combines IoT sensors with biometric data for multi-factor authentication making it possible that only those who are supposed to take the aforementioned assessments are enabled to do so. Passing authentication, the system is able to detect and verify attempts of impersonation attack or any other form of unauthorized access in real time. Speech recognition, face recognition and keyboard patterns are some of the things that machine learning algorithms are always attempting to confirm by monitoring humans. The system has a very high efficiency level of user identification such that the chances of double guessing the user system is very low hence the system is able to make credible and reliable academic evaluations. The user authentication effectiveness is increased by 98.26% shown in figure 10.

$$\delta_e G[\beta p - vw'']: \rightarrow bX[\exists - kf''] + 9\, vf[3j - la''] \qquad (25)$$

A particular identifying fraud parameter $[3j - la'']$ used with the data set $(\delta_e G)$ is denoted by 9 vf in the equation 25 describing fraudulent actions in the IoT-FD system. The alarms for possible fraud are correlated with the term $[\beta p - vw'']$, and the system's capacity to validate suspicious activities is enhanced by $bX[\exists - kf'']$. This fortifies the IoT-FD architecture by enhancing real-time detection and guaranteeing the validity of online scholastic assessments by means for analysis of user authentication effectiveness.

Table 3: The comparison of Exiting Methods and Proposed Method

Aspects	**Key Features**	**Exiting Methods in Ratio (%)**	**Proposed Method in Ratio (%)**
Fraud Identification	Highlights the system's approach to mitigating fraudulent activities proactively or reactively.	31.23%	98.84%
Fraud Detection Accuracy	Measures the ability of the system to correctly identify fraudulent activities with minimal false positives and negatives.	28.79%	97.45%
Real-Time Response	Evaluates how quickly the system detects and reports fraudulent activities	25.67%	98.05%
Security and transparency	Assesses the robustness of measures like encryption, data protection, and system integrity.	35.73%	99.25%
User Authentication Effectiveness	Examines the effectiveness of mechanisms like biometrics, multi-factor authentication, or behavioural analysis in validating user identities.	38.94%	98.26%

In summary, table 3 through the integration of IoT and CPS, the IoT-FD system brings about a paradigm shift in online academic assessments by enabling enhanced fraud detection. To improve security, transparency, and reliability, it uses adaptive machine learning, multi-source data analysis, and real-time monitoring. This helps prevent identity theft and manipulation and builds confidence in the validity of academic tests.

5. Conclusion:

By combining Cyber Physical Systems with IoT, a novel solution for fraud identification and prevention in online academic tests has been developed as well as a general approach to the issues posed by such assessment systems. The proposed IoT-FD system was designed to easily as well as in a systematic way enable the test supervisor to track the environment, the identities of the test takers as well as their actions at any time. One of the major enablement of the IoTFD is a capability of tracking several parameters that affect the legitimacy of online assessments. It significantly reduces the likelihood of duplicitous of the scores and detects abnormal behaviors such as change of environment due to the application of IoT sensors in this system. Then these insights will be used to train the machine learning algorithms to able to scalably detect any signs of fraud for system be trustworthy in the future. The system with new techniques in IoT-FD can adapt will always work. This technology further entrenches the need for fostering an environment where institutions are able to carry out assessments without the potential threat of any form of exam misconduct. The Internet of Things-FD device is a major development against examination crimes for online institutions. This device can help online institutions of learning assess learners on a more real time, data based and expandable model. Analysis of metrics such as, i.e., 98.84% fraud identification, 97.45% Fraud Detection Accuracy, 98.05% Real Time Response, 99.25% Security and Transparency, 98.26 User Authentication Effectiveness, would ensure fairness and transparency among the other factors in the evaluation process.

Future Work: In addition to the enhancement of the security capabilities with the use of IoT-FD, the incorporation of other types biometric authentication systems could be the potential area of future development. Moreover, simplification of certain components along with enhancing the system's ability to combat illicit activities will also pave the way for exploring this section i.e., refining machine learning algorithms to detect more complex instances of fraud, as well as expanding the system to larger educational systems.

Acknowledgements:

Soft Science Research Project of Science and Technology Department of Sichuan Province "Research on the Current Situation and Countermeasures of Scientific Research Integrity and Academic Style Construction in Sichuan Province under the Perspective of Innovation-driven Development"(2023JDR0209)

References:

1. Chui, K. T., Gupta, B. B., Liu, J., Arya, V., Nedjah, N., Almomani, A., & Chaurasia, P. (2023). A survey of internet of things and cyber-physical systems: standards, algorithms, applications, security, challenges, and future directions. *Information*, *14*(7), 388.
2. Tushkanova, O., Levshun, D., Branitskiy, A., Fedorchenko, E., Novikova, E., & Kotenko, I. (2023). Detection of cyberattacks and anomalies in cyber-physical systems: Approaches, data sources, evaluation. *Algorithms*, *16*(2), 85.
3. Bajic, B., Rikalovic, A., Suzic, N., & Piuri, V. (2024). Toward a Human-Cyber-Physical System for Real-Time Anomaly Detection. *IEEE Systems Journal*.
4. Pandey, R. K., & Das, T. K. (2024). Anomaly detection in cyber-physical systems using actuator state transition model. *International Journal of Information Technology*, 1-13.
5. AlEisa, H. N., Alrowais, F., Allafi, R., Almalki, N. S., Faqih, R., Marzouk, R., ... & Ibrahim, S. S. (2023). Transforming transportation: Safe and secure vehicular communication and anomaly detection with intelligent cyber–physical system and deep learning. *IEEE Transactions on Consumer Electronics*, *70*(1), 1736-1746.
6. Sagu, A., Gill, N. S., Gulia, P., Priyadarshini, I., & Chatterjee, J. M. (2024). Hybrid Optimization Algorithm for Detection of Security Attacks in IoT-Enabled Cyber-Physical Systems. *IEEE Transactions on Big Data*.
7. Jamal, A. A., Majid, A. A. M., Konev, A., Kosachenko, T., & Shelupanov, A. (2023). A review on security analysis of cyber physical systems using Machine learning. *Materials today: proceedings*, *80*, 2302-2306.
8. Alohali, M. A., Elsadig, M., Al-Wesabi, F. N., Al Duhayyim, M., Hilal, A. M., & Motwakel, A. (2023). Swarm intelligence for IoT attack detection in fog-enabled cyber-physical system. *Computers and Electrical Engineering*, *108*, 108676.
9. Mtukushe, N., Onaolapo, A. K., Aluko, A., & Dorrell, D. G. (2023). Review of cyberattack implementation, detection, and mitigation methods in cyber-physical systems. *Energies*, *16*(13), 5206.
10. Javed, S. H., Ahmad, M. B., Asif, M., Akram, W., Mahmood, K., Das, A. K., & Shetty, S. (2023). APT adversarial defence mechanism for industrial IoT enabled cyber-physical system. *IEEE Access*, *11*, 74000-74020.
11. Radanliev, P., De Roure, D., Van Kleek, M., Santos, O., & Ani, U. (2021). Artificial intelligence in cyber physical systems. *AI & society*, *36*, 783-796.
12. Rajawat, A. S., Rawat, R., Shaw, R. N., & Ghosh, A. (2021). Cyber physical system fraud analysis by mobile robot. *Machine learning for robotics applications*, 47-61.

13. Alohali, M. A., Al-Wesabi, F. N., Hilal, A. M., Goel, S., Gupta, D., & Khanna, A. (2022). Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment. *Cognitive Neurodynamics*, *16*(5), 1045-1057.
14. Jeffrey, N., Tan, Q., & Villar, J. R. (2023). A review of anomaly detection strategies to detect threats to cyber-physical systems. *Electronics*, *12*(15), 3283.
15. Mohammadi Rouzbahani, H., Karimipour, H., Rahimnejad, A., Dehghantanha, A., & Srivastava, G. (2020). Anomaly detection in cyber-physical systems using machine learning. *Handbook of big data privacy*, 219-235.
16. Tan, Q., & Villar, J. R. (2023). A review of anomaly detection strategies to detect threats to cyber-physical systems. *Electronics*, *12*(15), 3283.
17. Almajed, R., Ibrahim, A., Abualkishik, A. Z., Mourad, N., & Almansour, F. A. (2022). Using machine learning algorithm for detection of cyber-attacks in cyber physical systems. *Periodicals of Engineering and Natural Sciences (PEN)*, *10*(3), 261-275.
18. Ahmed, A. (2024). Advancements in Anomaly Detection: A Review of Machine Learning Applications in Cyber-Physical System Networks.
19. Luo, Y., Xiao, Y., Cheng, L., Peng, G., & Yao, D. (2021). Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities. *ACM Computing Surveys (CSUR)*, *54*(5), 1-36.
20. Zhang, J., Pan, L., Han, Q. L., Chen, C., Wen, S., & Xiang, Y. (2021). Deep learning-based attack detection for cyber-physical system cybersecurity: A survey. *IEEE/CAA Journal of Automatica Sinica*, *9*(3), 377-391.
21. Moriano, P., Hespeler, S. C., Li, M., & Mahbub, M. (2024). Adaptive Anomaly Detection for Identifying Attacks in Cyber-Physical Systems: A Systematic Literature Review. *arXiv preprint arXiv:2411.14278*.
22. Almajed, R., Ibrahim, A., Abualkishik, A. Z., Mourad, N., & Almansour, F. A. (2022). Using machine learning algorithm for detection of cyber-attacks in cyber physical systems. *Periodicals of Engineering and Natural Sciences (PEN)*, *10*(3), 261-275.
23. Bhuiyan, M. Z. A., Wu, J., Weiss, G. M., Hayajneh, T., Wang, T., & Wang, G. (2017). Event detection through differential pattern mining in cyber-physical systems. *IEEE Transactions on Big Data*, *6*(4), 652-665.
24. Han, S., Xie, M., Chen, H. H., & Ling, Y. (2014). Intrusion detection in cyber-physical systems: Techniques and challenges. *IEEE systems journal*, *8*(4), 1052-1062.
25. Alwan, A. A., Ciupala, M. A., Brimicombe, A. J., Ghorashi, S. A., Baravalle, A., & Falcarin, P. (2022). Data quality challenges in large-scale cyber-physical systems: A systematic review. *Information Systems*, *105*, 101951.
26. https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iot-iiot