Decentralized Blockchain Based AI Proctoring System

# Desetti Srinuvasa Rao1, Adapaka Lavanya2, Jami Vivek3, Jallepalli Bhargavi4, Adapa Nanibabu5

1Assistant Professor, Department of Computer Science and Engineering, GMR Institute of Technology, Rajam, Andhra Pradesh, India.

2,3,4,5B. Tech, Student, Department of Computer Science and Engineering, GMR Institute of Technology, Rajam,Andhra Pradesh, India.

## *Abstract*—The rise of online learning has made education more flexible but also increased concerns about cheating in online exams. To prevent this, AI-powered proctoring systems (AIPS) use smart monitoring with advanced object detection, especially the YOLO algorithm. YOLO helps track face direction, mouth movement, mobile phone use, and the number of people in a room to stop cheating. If suspicious activity is detected, the system can end the exam automatically. Audio monitoring adds extra security by detecting unusual sounds or voices in the background. To ensure certificates are real and not faked, blockchain technology is used to store them securely. This makes achievements trustworthy and prevents tampering. With AI and deep learning improving over time, these systems become more accurate, reducing mistakes and making the process smoother for students. Schools can adjust these tools to match their exam rules, making online tests fair and reliable. As digital education grows, such technology will be key in keeping academic standards strong.

**Keywords:**

*AI-based Proctoring System(AIPS), YOLO, Blockchain technology, Real-time object detection,Malpractice deterrence.*

# INTRODUCTION

As online education becomes more popular, maintaining fairness in assessments has become a major challenge. Traditional exam monitoring methods are less effective in virtual settings, leading to concerns about academic dishonesty. To address this, AI- powered proctoring systems (AIPS) provide an advanced solution using real-time monitoring and object detection techniques like the YOLO algorithm. These systems track face orientation, mouth movement, mobile phone usage, and the number of people present to prevent cheating. Suspicious activities trigger alerts, and in severe cases, the exam may be automatically terminated. Additionally, audio monitoring enhances security by detecting unusual sounds or background voices. To further protect the integrity of academic achievements, blockchain technology is used for secure certificate issuance. This ensures that certifications remain tamper-proof and verifiable. With continuous advancements in AI and deep learning, AIPS improves detection accuracy while reducing false alarms, making online exams more reliable. Institutions can customize these systems to align with their specific exam policies, ensuring a secure and fair assessment process. As online education continues to evolve, AI-based proctoring combined with blockchain security will play a crucial role in maintaining academic standards and trust.

1. **Need for Advanced Proctoring in the Post-Pandemic Era** The COVID-19 pandemic accelerated the adoption of online learning platforms, but it also exposed vulnerabilities in maintaining academic integrity. With students taking exams remotely, the traditional invigilator-based supervision model proved insufficient, highlighting the urgent need for scalable, intelligent proctoring solutions.

## Overview of AI-Powered Proctoring Features

AIPS systems go beyond basic webcam monitoring. They integrate computer vision, natural language processing, and audio analysis to detect a wide range of suspicious behaviors.

* + **Eye gaze tracking** to detect if a student is looking away from the screen for extended periods.
	+ **Face recognition** to confirm student identity and detect the presence of unauthorized individuals.
	+ **Mobile phone detection** to ensure no secondary devices are being used during the exam.

## Challenges in Implementation

Despite their benefits, AIPS systems come with challenges such as:

* + **Privacy concerns** regarding continuous monitoring and data storage.
	+ **Bias in AI models**, which may inaccurately flag certain behaviors based on lighting, camera quality, or cultural differences.
	+ **Internet connectivity issues**, especially in rural or underdeveloped regions, can disrupt real-time monitoring.

## Blockchain for Academic Integrity

Blockchain not only secures certificates but also provides a transparent ledger that institutions, employers, and students can access for verification. This reduces the risk of forged degrees and simplifies the hiring process by providing instant credential validation.

# LITERATURE REVIEW

The advent of online learning has necessitated the development of reliable and scalable online proctoring systems. Singh et al.

[1] present a comprehensive model leveraging deep learning and computer vision techniques for automated proctoring using YOLO. This system integrates face recognition to ensure student identity and relies on real-time object detection to identify potential malpractice. The authors compare live, recorded, and AI-based proctoring, asserting that AI-driven solutions enhance scalability and reduce human bias. However, they emphasize the privacy trade-offs, given the persistent video surveillance and data storage. As a potential mitigation, the study suggests deploying edge AI for on-device processing to reduce data transmission overhead and increase data security [1].

In proctoring systems, gaze estimation serves as a critical indicator for attention and potential malpractice. Ghosh et al. [2] offer an extensive survey of deep learning techniques for automatic gaze analysis. They categorize the challenges faced in real-world applications, such as varying lighting conditions, eye occlusions, and inconsistent image quality. The authors emphasize the need for robust gaze estimation methods, particularly those that can function under unsupervised and weakly supervised learning paradigms. These insights are crucial for the development of scalable and adaptable AI proctoring systems. However, they also acknowledge limitations in vector accuracy and the persistent challenges associated with natural lighting variations, making it difficult to ensure consistent monitoring across different environments [2].

Building upon this, Wang et al. [3] review vision-based gaze estimation, diving deeper into intrinsic challenges like head pose variations, image blur, and personal biases. Their work also explores social gaze behavior and meta-learning approaches to refine gaze tracking in unconstrained settings. Public datasets and the need for context-aware algorithms are highlighted, which could significantly benefit remote proctoring tools aiming to detect subtle patterns in student behavior. The survey indicates that future developments should consider causality in eye movements and incorporate behavioral data to more accurately flag suspicious activities [3].

Venkateswarlu [4] explores a geometric approach to gaze estimation, where iris circle orientation is inferred from a single image using projective geometry. The method is computationally efficient and tested against real image datasets, demonstrating robustness in various scenarios. However, it suffers from low accuracy compared to deep learning-based approaches and depends heavily on high-resolution imagery. While this method contributes a mathematically elegant alternative, it lacks the adaptability and precision needed in modern online exam environments that require real-time inference and minimal hardware constraints [4].

The pandemic accelerated the adoption of AI-based proctoring systems, as highlighted by Khanna et al. [5]. Their study reviews software platforms that use facial recognition and behavior analysis to ensure academic integrity during online exams. These systems benefit educational institutions by automating scheduling, feedback, and identity verification. The AI models interpret behavioral cues in real time to flag anomalies. Despite these advancements, the authors note a gap in hardware standardization and a lack of measures to handle edge cases like identical twins or spoofed images [5].

Atoum et al. [6] take a component-wise approach by detailing a six-element model comprising user verification, gaze tracking, voice and text detection, active window tracking, and phone detection. Their system achieves a high accuracy rate in identifying various cheating methods but faces scalability challenges due to its reliance on multiple sensors and real-time processing. Furthermore, human proctoring still plays a partial role in certain edge cases, leading to concerns around time complexity and resource utilization. Their findings support the idea that hybrid systems—combining AI automation with selective human oversight—may be more practical at scale [6].

The importance of a lightweight and multimodal detection system is stressed by Kaddoura and Gumaei [7], who designed a proctoring framework integrating CNNs with discrete Fourier transform (DFT) features. Their model utilizes dual cameras, EEG sensors, and speech analysis to detect cheating. This multi-sensor approach allows for nuanced interpretation of human behavior. However, the hardware-intensive nature of the setup restricts widespread adoption, particularly in developing regions. The study suggests that future research should aim to minimize dependency on specialized equipment while maintaining accuracy through innovative algorithms [7].

Biometric solutions such as fingerprint authentication also offer promising results, as Bawarith et al. [8] elaborate. Their e-exam system combines fingerprint recognition with eye-gaze tracking and keystroke biometrics for continuous authentication. The paper acknowledges the ecological benefits of digital exams while calling attention to persistent gaps in seamless integration of these tools. Notably, they advocate for the use of keystroke dynamics for continuous verification—an idea that aligns well with decentralized platforms that prioritize lightweight and verifiable identity checks without relying on video streams [8].

Abbas and Hameed [9] present a systematic review of deep learning-based approaches for detecting abnormal student behavior. They identify common tactics such as tab switching, unapproved gaze shifts, and presence of background noise. Their study promotes a multi-factor authentication and surveillance framework that combines biometric data with behavioral monitoring. However, the complexity of integrating all these elements in a user-friendly interface remains a bottleneck. They advocate for additional controls like browser lockdown features and emphasize the necessity for intuitive interfaces to support non- technical users [9].

In recent years, the integration of face recognition technology has become a central pillar in proctoring systems. Idemudia et al. [10] introduced a smart examination system that employs facial recognition to tackle identity fraud and cheating in online exams. Their system matches a student's live face with a pre-stored image and uses this validation to authorize access. Furthermore, continuous scanning during the test ensures that the same person is taking the exam throughout. The study also mentions that upon detecting repetitive discrepancies in facial matching or behavior, the system will prevent the user from continuing the exam. However, the paper also highlights a gap in current research— there is minimal exploration of deeper facial analytics such as facial expressions or styles, or handling occlusion scenarios [10]. Such enhancements could potentially provide a more nuanced layer of identity verification and behavior monitoring.

Assal et al. [11] present another innovative approach focusing on real-time video-based monitoring that captures and analyzes the facial region, particularly around the eyes, to detect cheating behaviors. The system combines webcam footage with an overhead camera for a more comprehensive view and uses a

microphone to assess the test taker's audio environment. A key strength is the video storage mechanism, which allows for manual verification post-exam. Nonetheless, one of the system’s limitations is its reliance on only webcam inputs for real-time cheating detection, which might not catch all suspicious actions or resource misuse if students maneuver off-camera or manipulate their setup [11].

Further advancing these solutions, Asinathan et al. [12] developed ProctorEx, an automated AI-powered online exam invigilation system that tracks both webcam video and browser activities. The system leverages deep learning algorithms to detect irregular facial movements and unauthorized browser switches. It can raise real-time alerts to instructors and even detect multiple persons on screen, which is a common tactic used for cheating. This platform emphasizes the scalability of AI proctoring to handle large-scale online assessments without human invigilators. However, it inherently assumes the availability of a functional webcam for all participants, which may not always be feasible in under-resourced regions [12].

Moving from system design to behavioral impact, Dendir and Maxwell [13] conducted a study examining the effectiveness of online proctoring in reducing cheating during online courses. They found statistically significant reductions in cheating incidents in courses that used AI-enabled proctoring compared to those that did not. The research provides empirical evidence supporting the efficacy of automated invigilation tools in maintaining academic integrity. Interestingly, the study also suggests that the mere presence of surveillance (even if automated) may serve as a psychological deterrent against dishonest behaviors. However, privacy concerns and ethical implications continue to be debated among educators and learners alike [13].

Abbas and Hameed [14] provide a systematic review of deep learning-based online exam proctoring systems that focus on detecting abnormal student behavior. Their paper aggregates research efforts in using AI for proctoring, highlighting key components such as facial recognition, head pose estimation, and natural language processing. A notable contribution of the study is the identification of 13 distinct datasets used to train and evaluate these systems, emphasizing the breadth of research in this space. However, the authors caution against the bias and fairness concerns associated with AI models—particularly in facial recognition systems, which can struggle with diverse skin tones or facial features. This underlines the need for fairness- aware model training and more inclusive datasets to ensure equitable proctoring outcomes [14].

Kar and Corcoran [15] review the landscape of eye-gaze estimation technologies, which are increasingly relevant for proctoring and attention monitoring. Their survey categorizes eye-gaze tracking systems across five platforms: desktop computers, TV panels, head-mounted devices, automotive setups, and handheld devices. In the context of education and proctoring, such systems are valuable not only for detecting potential cheating but also for health monitoring—such as identifying fatigue or stress through irregular eye movements. However, the authors acknowledge several practical limitations, including the setup complexity, reduced accuracy in varying lighting or head movement conditions, and high hardware costs. These challenges make widespread deployment difficult, especially in low-resource settings [15].

To enhance the robustness of student authentication, Labayen et al. [16] propose a multimodal biometrics-based system that integrates facial recognition, voice authentication, and keystroke

dynamics. The system is designed for real-time authentication during online exams and lectures, ensuring that the same student remains present throughout the session. Its continuous and non- intrusive monitoring makes it a compelling alternative to conventional proctoring. Moreover, the system is compatible with existing learning platforms, enhancing its adoption potential. Still, the authors recognize the cost-related barriers associated with deploying such advanced biometric tools at scale, especially for institutions in the Global South [16].

Kaddoura, Popescu, and Hemanth [17] explore how machine learning models have supported online learning and assessment during and after the COVID-19 pandemic. Their review focuses on the challenges educators faced, including scalability, academic integrity, and learner engagement, and how ML solutions were implemented to tackle these. The authors highlight benefits such as cheating detection, personalized learning pathways, and improved system efficiency. A particularly important insight is the adaptability of ML models to different student behaviors and learning styles, which opens up avenues for intelligent tutoring systems and adaptive assessments in future implementations [17].

In a subsequent work, Kaddoura and Gumaei [18] delve into the performance of deep learning algorithms for face recognition, focusing on real-world, uncontrolled datasets such as images from Facebook. The study tests several algorithms—PCA, SVM, and IPCA—on these images, finding that while SVM achieved the highest accuracy (~65%), lighter models like IPCA offer better speed-memory trade-offs for deployment in large-scale systems. Their findings underscore a recurring issue in AI-based authentication: even the best models may struggle in uncontrolled environments, where variability in lighting, angles, and image quality introduce accuracy limitations. These results reinforce the need for robust models that generalize well beyond ideal test conditions [18].

To address some of these ethical concerns and improve trust in proctoring outcomes, decentralized technologies can play a transformative role. By integrating blockchain for certification and data integrity, platforms can ensure that exam results are tamper- proof and verifiable without centralized control. This aligns well with the need for decentralized academic record systems, where students have custody of their verified credentials and proof of exam completion without relying on a single authority. While not covered in depth in the reviewed papers, this direction offers immense potential for future work that combines AI-powered surveillance with decentralized record-keeping, thereby enhancing both exam integrity and student agency in online learning ecosystems.

In conclusion, the convergence of AI, computer vision, gaze estimation, and behavioral analytics with biometric authentication has significantly enhanced the capability of online proctoring systems. The reviewed literature shows a consistent trend toward greater automation, scalability, and sophistication in cheating detection [1][5][6][7]. At the same time, challenges persist in terms of scalability, accuracy in real-world environments, and privacy- preserving methods. As future work, combining AI models with edge processing, federated learning, or zero-knowledge proof mechanisms could address many of these concerns. Moreover, integrating AI with blockchain-based decentralized certification will further bolster the transparency, auditability, and credibility of online assessments, leading toward a more secure and equitable digital education landscape.

# TECHNOLOGIES USED

## React:

React is an open-source JavaScript library maintained by Meta (formerly Facebook) used to build user interfaces for web applications. It emphasizes component-driven development, enabling modular, maintainable, and reusable UI structures. React is particularly favored for its virtual DOM, one-way data binding, and declarative nature.

## Key Concepts:

JSX (JavaScript XML): A syntactic extension of JavaScript that allows developers to write HTML-like code inside JavaScript files.

Components: Reusable building blocks of UI that can manage their own state.

State and Props: State manages dynamic data within a component, while props allow data to be passed between components.

Hooks: Functions that let you use state and other React features in functional components (e.g., useState, useEffect, useContext).

## Benefits of Using React:

1. **Component-based architecture** – Encourages reusable and maintainable code.
2. **Fast performance** – Uses Virtual DOM to update only the necessary parts of the UI.
3. **One-way data binding** – Makes the app’s data flow more predictable and easier to debug.
4. **Rich ecosystem** – Offers many libraries and tools for routing, state management, and more.
5. **JSX syntax** – Lets you write HTML-like code in JavaScript, improving readability.
6. **Strong community support** – Plenty of resources, solutions, and tutorials available.
7. **Ideal for SPAs** – Helps in building fast and dynamic single-page applications.
8. **Easy testing and debugging** – Tools like React Developer Tools simplify the process.
9. **Supports mobile app development** – With React Native, you can build cross-platform apps.
10. **High job demand** – Widely used in the industry, increasing job opportunities.

## Understanding Verifed

**Product Summary**: Verifed is an AI-integrated exam proctoring platform that incorporates blockchain verification mechanisms to maintain exam integrity and result authenticity. Built with a focus on real-time surveillance, identity validation, and tamper-proof certification, Verifed is suitable for remote learning environments.

## Key Modules of Verifed:

Student Onboarding: KYC process with Plug Wallet integration AI Proctoring: Monitors user presence, gaze, and anomalies Exam Interface: Clean and responsive layout for taking tests

Blockchain Verification: Submits test hashes and timestamps to Internet Computer Protocol (ICP) and Solana.

Admin Dashboard: Real-time logs, AI alerts, and test management.

## Frontend Stack:

React (with Vite for bundling) TypeScript

TailwindCSS React Router

shadcn/ui for component styling.

## Why React Was Chosen

React was selected as the primary frontend library for Verifed due to:

1. **Scalability:** Verifed’s architecture demands a modular and scalable approach. React's component system made it easier to build separate logical units for the student, proctor, and admin views.
2. **Dynamic Interactivity:** With live AI video feeds, bot messaging, wallet connection states, and test timers, React’s state management and declarative rendering were essential.
3. **Developer Productivity:** React’s integration with TypeScript and Vite provided faster development loops, excellent IntelliSense, and easy refactoring.
4. **Community and Tooling:** React has extensive documentation, support, and libraries such as react-router, zustand, and react-query which were used in Verifed.

## Core React Features in Verifed:

**Component-Based Architecture:**

StudentDashboard.tsx: Displays user information, exam schedule, and blockchain status.

ProctorView.tsx: Monitors AI flags, user camera, and mic activity. BotChat.tsx: Dynamic chatbot assistant with context-aware tips. **Hooks in Action:**

useEffect: Handles API calls and side effects like wallet state checks and test submissions.

useState: Manages real-time changes like proctoring alerts and bot responses.

useContext: Provides global authentication and blockchain wallet states.

## AI Proctoring Flow Live Camera Feed:

Used a <video> element rendered via React and connected to webcam.

React state updated in real-time as AI flags detected unusual behavior.

## User Monitoring Component:

Displays warnings, triggers re-verification steps if multiple faces are detected.

Uses canvas overlay for face detection boxes.

## Modular Alerts:

AI flags like eye movement, face absence, or external person detection generate modals.

Alerts are logged via a REST API using axios in useEffect.

## React Contribution:

Easy to trigger re-renders on new AI inputs

Made overlay and canvas management intuitive using refs

## Blockchain Verification View:

**Purpose:** To show that an exam result is recorded on-chain and is tamper-proof.

The **Blockchain Verification View** is designed to provide transparency and trust by showcasing that an exam result has been securely recorded on the blockchain. Its primary purpose is to prove that the result is immutable and cannot be altered once submitted. This not only ensures authenticity but also builds credibility for both students and institutions.The component includes several important features. Firstly, it displays the **transaction hash,** which acts as a unique identifier for the blockchain record. This hash serves as a reference point that users can use to track the transaction directly on a blockchain explorer. Secondly, the component shows the **timestamp in UTC**, providing a standardized and verifiable indication of when the transaction was submitted to the blockchain. This helps validate that the data was recorded within the intended time frame. Lastly, it includes a **link to IPFS (InterPlanetary File System) or ICP (Internet Computer Protocol)** where the actual exam result or verification file is stored. This ensures that the data is not only stored in a decentralized way but also can be independently accessed for audit purposes.From a React development perspective, the component makes use of **React Router's dynamic routing** to identify which exam result to display, based on parameters like result ID or user ID. It also employs **conditional rendering** to show verification success or failure messages depending on whether the transaction hash and file links are valid. Additionally, useEffect is utilized to trigger a fetch request to retrieve the corresponding blockchain data immediately after the component is mounted, ensuring the user sees the latest verification status without having to manually refresh or trigger any actions.

This setup not only provides a technically robust verification process but also enhances the user experience with real-time feedback and access to trustworthy proof of record.

## Component Features:

View Transaction Hash Timestamp Display (UTC)

IPFS or ICP link to verify content

## Admin Panel & Analytics:

The **Admin Panel & Analytics** interface, primarily structured within the AdminDashboard.tsx component, serves as the control center for monitoring and managing exam sessions. Its core purpose is to provide proctors and administrators with powerful tools to oversee student activity, assess the integrity of exam attempts, and respond to issues in real-time. The dashboard includes a comprehensive **table with sortable columns** such as *Student ID*, *AI-generated flags*, and *Exam Time*, allowing admins to quickly organize and scan through large volumes of data.

The dashboard also supports **searchable logs** and a complete **exam history,** enabling fast retrieval of individual student records or flagged events. One of the most impactful features is the display of **real-time proctor alerts** and **exam interruption statistics**, which helps admins take immediate action when suspicious behavior or technical issues are detected. This ensures smooth exam operations and strengthens the reliability of the AI proctoring system.

To build this efficiently, the dashboard leverages powerful React libraries. The react-table library handles the dynamic and interactive data table, offering features like pagination, sorting, and filtering out-of-the-box. Meanwhile, react-chartjs-2 is used to visualize exam trends and alert data through sleek, interactive charts, helping admins understand patterns at a glance.React’s strengths shine through in this component. With **component-level control**, each log, alert, and analytic card can be independently rendered, styled, or updated without affecting the entire page. React's **efficient state management** ensures only the necessary components re-render when updates occur, maintaining high performance. Lastly, the dashboard relies on **event-driven updates**, using state hooks and side effects (useEffect) to reflect changes in real-time, such as incoming alerts or updated exam data

— making the interface both responsive and reliable.

## Features Enabled by React:

Component-level control over each card and log Efficient update cycles via state changes

Event-driven updates for real-time analytics

## UI/UX Design with shadcn and Tailwind:

The UI/UX design of the application is crafted using a combination of shadcn/ui and TailwindCSS, resulting in a modern, responsive, and accessible interface. The design system is built around the philosophy of clean components and rapid development. With shadcn/ui, the project benefits from well-structured, pre-styled components that are both developer-friendly and accessible by default, ensuring compliance with best practices in user interface design.

TailwindCSS plays a crucial role in the layout and visual consistency of the application. By applying utility-first classes, developers were able to rapidly prototype interfaces and maintain consistent spacing, typography, and responsiveness across components. The integration of Tailwind also enabled seamless

theming using design tokens, including support for dark mode, enhancing the overall user experience for different environments and user preferences.To promote maintainability and scalability, the UI layer features a set of reusable components such as Button, Card, Modal, Input, and AlertDialog. These were customized where needed but remained consistent with the broader design language, helping to unify the user experience across different parts of the application.

From a performance perspective, this approach offers clear advantages. Both shadcn and TailwindCSS contribute to a minimal CSS footprint, since styles are generated and purged based on actual usage. Moreover, all components are responsive out of the box, ensuring the application performs smoothly across devices without additional overhead.

## Design System:

Used shadcn/ui to create clean, accessible components

TailwindCSS classes enabled rapid prototyping and consistent spacing

## Reusable Components:

Button, Card, Modal, Input, AlertDialog

Theming via Tailwind variables and darkMode support

## Integrating Solana for NFT-Based Certification in Verifed:

Solana is a high-performance blockchain platform specifically engineered for speed, scalability, and low-cost transactions. It stands out in the Web3 ecosystem by supporting thousands of transactions per second (TPS), making it one of the fastest blockchains currently in operation. Solana is also optimized for developer flexibility, offering support for smart contracts written in Rust or C, and is especially suited for decentralized applications (dApps) that demand high throughput and real-time interaction.

One of Solana’s most innovative features is Proof of History (PoH) — a cryptographic clock that provides a verifiable passage of time between events. This mechanism allows nodes to maintain time consistency without requiring global consensus for every single timestamp, significantly reducing latency. Another core innovation is the Sealevel Runtime, which enables parallel execution of smart contracts, drastically improving efficiency and throughput. Combined with ultra-low fees, Solana becomes ideal for use cases involving micro-transactions, such as issuing or transferring certificate NFTs in educational or verification systems.

From a development perspective, Solana is highly interoperable, making it easy for smart contracts to interact with wallets like Phantom or other token programs. This enhances user experience while simplifying developer integration.Solana powers a wide range of applications including DeFi protocols, NFTs and digital marketplaces, fast payment systems, and even decentralized identity platforms. Its unique combination of scalability, low cost, and high performance has made it a go-to choice for next-generation blockchain solutions.

## Solana Use Cases:

DeFi apps

NFTs and marketplaces

Payment systems Decentralized identities

## Verifed and the Need for NFTs:

The integration of **NFTs (Non-Fungible Tokens)** within the Verifed platform serves a powerful and focused purpose: to provide **tamper-proof, blockchain-verified certificates.** In this system, NFTs function as **digital credentials** that guarantee the **authenticity, traceability,** and **ownership** of a student’s exam results. By leveraging blockchain technology—specifically the Solana network—Verifed ensures that each certificate is permanently recorded, cannot be altered, and is easily accessible to both the student and relevant third parties.

There are several compelling reasons why **NFTs** were chosen for this use case. First, they provide an **immutable record of certification**, meaning that once a certificate is minted and stored on-chain, it cannot be changed or deleted. Second, NFTs are **easily shareable—**students can store them in their wallets or share a direct link, making it simple to present their achievements for academic or professional purposes. Third, NFTs are **verifiable by third parties,** including employers and educational institutions, who can independently confirm the legitimacy of the certificate using blockchain explorers or integrated verification tools.

Within the Verifed workflow, this process is seamlessly implemented. Once a student successfully completes an exam and clears all **AI proctoring checks**, a **certificate NFT is minted** on the **Solana blockchain**. This NFT is then **automatically sent to the student’s wallet**, giving them a secure, decentralized, and verifiable proof of achievement that they own and control.

## Here’s a simplified example of the connection logic:

const connectWallet = async () => {

const resp = await window.solana.connect(); setWalletKey(resp.publicKey.toString());

};

This function initiates a connection with the user’s Phantom wallet and stores their public key, which is essential for NFT minting, transaction signing, and blockchain verification processes.

## NFT Metadata & Token Standards:

To ensure consistency, compatibility, and rich data representation, Verifed adopts the Metaplex Token Metadata standard, which is widely used in the Solana ecosystem for NFT issuance. This standard provides a robust framework for attaching meaningful metadata to each NFT, making the tokens more than just identifiers—they become complete digital certificates that can be interpreted by wallets, marketplaces, and verification tools.Each certificate NFT minted by Verifed includes structured metadata fields such as the Exam ID, hashed student name (to protect privacy), exam date, score, and a custom design or logo representing Verifed. This structured data not only supports authenticity and ownership but also enhances visual recognition and trust, as the NFT can be previewed in compatible wallets like Phantom or on-chain explorers.

## Here's a simplified example of the metadata JSON structure used:

{

"name": "Verifed Exam Certificate", "symbol": "VRFD",

"uri": "https://verifed-ipfs.io/exam1234.json", "creators": [{ "address": "...", "share": 100 }]

}

In this example, the name field describes the NFT as an official Verifed certificate, and the symbol uniquely identifies the Verifed NFT collection (VRFD). The uri points to a JSON file hosted on IPFS, containing extended metadata like date, exam details, and visual assets. The creators field tracks the minting authority, allowing Verifed to be recognized as the sole issuer.Using this metadata standard ensures that Verifed’s NFTs are discoverable, consistent, and verifiable across various Solana-based platforms and tools, while maintaining a flexible structure for future enhancements.

## Minting NFTs with Solana Programs:

In Verifed, the process of minting NFTs is at the heart of transforming exam results into verifiable, blockchain-based credentials. The minting workflow begins when a Solana smart contract (also called a program) is triggered through an RPC (Remote Procedure Call). This is typically initiated once a student passes the exam and clears proctoring verification.

The first step involves preparing and uploading the NFT metadata—which includes exam details, the student's hashed name, and certificate design—to a decentralized storage platform such as Arweave or IPFS. This ensures the metadata remains publicly accessible, tamper-proof, and persistent. Once uploaded, a URI pointing to this metadata is generated and used during the minting process.

Next, an NFT is minted on the Solana blockchain and sent directly to the student’s wallet address, such as Phantom. This NFT acts as a permanent, cryptographically verifiable record of the student’s exam completion and performance.

The minting system is built using a powerful and modern tech stack:

* Solana Web3.js is used on the client side to handle wallet interactions, fetch accounts, and initiate transactions.
* Anchor, a popular Solana framework, is employed to simplify smart contract development, offering safety and structure through Rust macros.
* Metaplex SDK provides streamlined utilities for NFT creation, particularly around setting metadata, managing ownership, and updating authorities.

## Here’s a simplified example of the minting function:

const mintNFT = async () => {

const mint = await metaplex.nfts().create({ uri: metadataURL,

name: "Verifed Certificate", sellerFeeBasisPoints: 0,

updateAuthority: wallet.publicKey,

});

};

This code uses the Metaplex SDK to mint an NFT with the specified metadata URI and assigns the wallet’s public key as the update authority. The sellerFeeBasisPoints is set to zero since these certificates are not intended for resale but strictly for verification.By leveraging these tools and steps, Verifed ensures a secure, automated, and scalable NFT minting flow, bringing trust and transparency to digital certification.

## Smart Contract (Program) with Anchor:

The Verifed platform leverages the Anchor framework to develop its Solana smart contracts, simplifying the traditionally complex process of writing on-chain programs. The smart contract is responsible for orchestrating the NFT minting workflow securely and efficiently. Specifically, the contract handles three main tasks: creating new mint accounts, verifying transaction authority, and assigning metadata to each certificate NFT.Anchor structures the program logic using clearly defined contexts and macros, making the code more readable, maintainable, and secure.

One of the core instructions defined in the contract is mint\_certificate, which initiates the NFT creation process once a student has passed the proctoring checks. This instruction ensures that only valid users can mint their certificates, using strict authority checks and predefined logic.

To enhance security and maintain control, the program also uses a custom Program Derived Address (PDA) as the exam authority. This PDA acts as the signing authority for minting actions, ensuring that NFTs are only issued by Verifed’s approved contract logic, not arbitrary users or external scripts.

## Here’s a simplified example of the Anchor instruction context used for minting:

#[derive(Accounts)]

pub struct MintCert<'info> {

#[account(init, payer = user, space = 8 + 32)] pub cert: Account<'info, Certificate>, #[account(mut)]

pub user: Signer<'info>,

}

In this snippet, the MintCert context ensures that a new certificate account is initialized, paid for by the user, and sized appropriately for storing certificate data. The Signer trait ensures that only authenticated users can trigger this action, helping prevent unauthorized minting.By using Anchor, Verifed benefits from automatic account validation, clean error handling, and secure program logic, making it a reliable backbone for managing blockchain-based academic credentials.

## Exam Completion to NFT Mint Flow:

The end-to-end flow from completing an exam to receiving a blockchain-verified NFT certificate on Verifed is designed for

both security and user convenience. It begins when a student finishes their exam through the Verifed platform. Immediately after, the AI proctoring module analyzes the exam session to verify the student’s integrity—ensuring there were no violations or anomalies during the test.Once the exam is cleared, the backend takes over the minting process. A secure minting keypair—accessible only to the backend—is used to sign the transaction, thereby confirming the legitimacy of the request. This step ensures that NFTs can only be minted by the Verifed backend and not forged by clients or outside actors.With the transaction signed, an NFT is minted on the Solana blockchain. The NFT contains rich metadata including the exam ID, score, timestamp, and student’s hashed identity. This metadata is hosted on decentralized storage (IPFS or Arweave), and the resulting NFT is automatically sent to the student's Phantom wallet address.

## Exam to NFT Minting – Visual Flow:

****

*Fig 1: Visual Flow*

# Dataset

Dataset was created. It has 4 classes cheating, non-cheating, closed eyes, gadgets. Different models are trained and found out the best accuracy model for the project the accuracies are as shown. The dataset is done using the different classes as following:

*Fig 2: Dataset*

The dataset shown above is a collection of facial images that are crucial for training and testing the AI-based proctoring system used in the Verifed platform. These images represent various head poses and orientations under controlled conditions, making the dataset particularly useful for head pose estimation, identity verification, and face orientation tracking during online examinations.

Each file is named using a pattern like ID\_angle\_orientation.jpg, where:

ID denotes the unique person identifier (e.g., 1, 2, 3, …)

angle refers to the degree of head rotation (e.g., 0°, 18°, 27°, 90°, etc.)

The suffix (0, 70, 80, etc.) may represent tilt angle, lighting intensity, or yaw variation.

By combining different angles and lighting, the dataset simulates a realistic environment where candidates may move slightly or look away, allowing the AI to better detect and flag suspicious behaviors.

## Purpose in the AI Proctoring System:

The primary use of this dataset is to train and validate machine learning models that detect abnormal or unauthorized behavior during remote examinations. Here's how it contributes to different modules:

1. **Face Detection and Alignment:** Using this dataset, models can be trained to detect faces under varied angles and align them for consistent feature extraction. This is essential to ensure the system can detect a student’s face even if they’re not looking directly at the camera.
2. **Head Pose Estimation:** By training on images labeled with angle metadata, the AI learns to estimate the yaw, pitch, and roll of the head. This enables real-time monitoring to check if the student frequently looks away, which could indicate cheating.
3. **Identity Verification:** The frontal images in the dataset help in training models to match the face of the student at login with their registered profile. This prevents impersonation or face spoofing attacks.
4. **Attention Monitoring:** The variation in pose data (from straight to extreme side views) helps the system differentiate between natural movements and potentially suspicious behavior, like turning towards another screen or person.

It’s important to note that any facial dataset used in AI proctoring must be handled with strict privacy considerations. If this dataset is synthetic or anonymized, it ensures ethical training. Otherwise, usage must comply with data protection laws like GDPR or India’s PDP Bill, especially if the dataset involves real student data. This image dataset plays a foundational role in the effectiveness of the Verifed AI proctoring system. It supports the creation of intelligent models that enhance exam security without invading student privacy. With diverse head poses, real-time attention tracking, and identity matching capabilities, it ensures trustworthy, fair, and secure online assessments, empowering institutions to adopt remote exams with confidence.

## RESULTS

****

*Fig 3: Landing Page*



*Fig 4: Dashboard*

**

*Fig 5: Connect Wallet*

**

*Fig 6: Proctoring*



*Fig 7: Cheating Detected*

**

*Fig 8: Writing Exam*

**

*Fig 9: Result page*

**

*Fig 10: Mint NFT to the wallet*



*Fig 11: Verify NFT*

# CONCLUSION

The decentralized blockchain-based AI proctoring system represents a significant advancement in ensuring secure, transparent, and tamper-proof online examinations. By leveraging blockchain’s immutability and AI’s real-time monitoring capabilities, this system addresses major concerns related to exam malpractice, identity verification, and data integrity. Unlike traditional proctoring methods, which often suffer from privacy issues and centralization risks, this approach enhances trust among stakeholders by maintaining a decentralized, auditable, and verifiable record of examination activities.Furthermore, the integration of AI-driven analytics ensures intelligent decision-making, reducing human intervention while maintaining accuracy and fairness. The decentralized nature eliminates single points of failure, making the system more resilient against cyber threats. This innovation not only improves academic integrity but also paves the way for broader applications in certification processes, corporate training, and secure assessments across industries. As technology continues to evolve, further research and optimization can enhance scalability, reduce computational overhead, and improve accessibility. Ultimately, this system sets a foundation for a future where online assessments are both reliable and ethically conducted.

# REFERENCES

1. Singh, T., Nair, R. R., Babu, T., & Duraisamy, P. (2024). Enhancing Academic Integrity in Online Assessments: Introducing an Effective Online Exam Proctoring Model using YOLO. Procedia Computer Science, 235, 1399-1408.
2. Ghosh, S., Dhall, A., Hayat, M., Knibbe, J., & Ji, Q. (2023). Automatic gaze analysis: A survey of deep learning based approaches. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *46*(1), 61-84.
3. Wang, X., Zhang, J., Zhang, H., Zhao, S., & Liu, H. (2021). Vision-based gaze estimation: a review. *IEEE Transactions on Cognitive and Developmental Systems*, *14*(2), 316-332.
4. Venkateswarlu, R. (2020, October). Eye gaze estimation from a single image of one eye. In Proceedings Ninth IEEE International Conference on Computer Vision (pp. 136-143). IEEE.
5. Khanna, V., Brodiya, S., & Chaudhary, D. (2021). Artificial intelligence based automated exam proctoring system. Int. Res. J. Eng. Technol.(IRJET), 8(12), 558-560.
6. Atoum, Y., Chen, L., Liu, A. X., Hsu, S. D., & Liu, X. (2019).

Automated online exam proctoring. IEEE Transactions on Multimedia, 19(7), 1609-1624.

1. Kaddoura, S., & Gumaei, A. (2022). Towards effective and efficient online exam systems using deep learning-based cheating detection approach. Intelligent Systems with Applications, 16, 200153.
2. Bawarith, R., Basuhail, A., Fattouh, A., & Gamalel-Din, S. (2017). E-exam cheating detection system. International Journal of Advanced Computer Science and Applications, 8(4).
3. Abbas, M. A. E., & Hameed, S. (2022). A Systematic Review of Deep Learning Based Online Exam Proctoring Systems for Abnormal Student Behaviour Detection.
4. Idemudia, S., Rohani, M. F., Siraj, M., & Hajar, S. (2016). A smart approach of E-Exam assessment method using face recognition to address identity theft and cheating. International Journal of Computer Science and Information Security (IJCSIS), 14(10).
5. Assal, M., Said, A., Essam, A., Hamza, H., & Nabil, M. Smart Online Examination Anti-Cheat System.
6. asinathan, V., Yan, C. E., Mustapha, A., Hameed, V. A., Ching, T. H., & Thiruchelvam, V. (2022). ProctorEx: An Automated Online Exam Proctoring System. Mathematical Statistician and Engineering Applications, 71(3s2), 876-889.
7. Dendir, S., & Maxwell, R. S. (2020). Cheating in online courses: Evidence from online proctoring. Computers in Human Behavior Reports, 2, 100033.
8. Abbas, M. A. E., & Hameed, S. (2022). A Systematic Review of Deep Learning Based Online Exam Proctoring Systems for Abnormal Student Behaviour Detection
9. Kar, A., & Corcoran, P. (2017). A review and analysis of eye- gaze estimation systems, algorithms and performance evaluation methods in consumer platforms. IEEE Access, 5, 16495-16519.
10. Labayen, M., Vea, R., Flórez, J., Aginako, N., & Sierra, B. (2021). Online student authentication and proctoring system based on multimodal biometrics technology. IEEE Access, 9, 72398- 72411.
11. Kaddoura, S., Popescu, D. E., & Hemanth, J. D. (2022). A systematic review on machine learning models for online learning and examination systems. PeerJ Computer Science, 8, e986.
12. Kaddoura, S., & Gumaei, A. (2022). Towards effective and efficient online exam systems using deep learning-based cheating detection approach. Intelligent Systems with Applications, 16, 200153.