PIE

PATENT INFORMATION EXTRACTION FORM

TOPIC : Artificial Intelligence based Learning and Skill assessment platform for Cybersecurity

Suggested expanded title for broader patent scope: "AI-Enabled Cybersecurity Education and Competency Assessment System configured for Interactive Training and Skill Testing of Students in Schools, Colleges, and Educational Institutes using Structured Cybersecurity Domains under Progressive Difficulty Modes and Time-Critical Simulated Scenarios"

SCHOOL: Chitkara University, Chandigarh-Patiala National Highway (NH-64), Village Jansla, Tehsil Rajpura, Distt. Patiala, Punjab 140401

INVENTOR'S DETAIL WHO UPLOADED THE PATENT ON CHALKPAD

NAME:Vedant Sareen

ROLL NUMBER: 2310991318 MOBILE NO: +91 7087603933

MAIL ID (UNIVERSITY) – vedant1318.be23@chitkara.edu.in

MAIL ID (PERSONAL) - **securecybernetics@gmail.com**

OTHER INVENTORS DETAIL

NAME	EMP CODE/ROLL	ADDRESS WITH EMAIL AND MOBILE NO.
Dr. Himanshi Babbar	**CET1001727**	**Chitkara University, Punjab, India; Himanshi.babbar@chitkara.edu.in; 8557008265**

Answer the following questions in brief: (use extra sheets if needed, submit pics/videos etc. which can help us to understand the invention better)

1. **What was the problem?**

   The current cybersecurity-based training platforms lack personalization and adaptive learning according to users' intellect. Famous platforms like TryHackMe and Hack The Box provide general challenges without addressing an individual's unique skill set, knowledge gaps, and learning pace. Beginners often get confused by the vast, unstructured information and lack a guided starting point, mostly in terms of specialized areas like Web Application Penetration Testing (WAPT) based on OWASP Top 10 and LLM Top 10. There are accessible AI models like HackGPT and SGPT and even organization-based AI chatbots that may help you address the issue related to a particular problem statement listed on the website, but no query is entertained beyond that, whereas an artificial intelligence-based tutor is required to provide real-time, recursive feedback and tailor the process of learning to the users' evolving capabilities. With abundant resources at every platform, there's an issue of static content that explains the existence of prebuilt and static labs, which do not dynamically adapt to the user's specific queries or learning gaps.

2. **How did you solve it (Inventive Step)?**

   We invented a system and method for an AI-powered/adaptive cybersecurity training platform. The inventive phase involves a central AI tutoring engine that performs some core functions listed below:

   A dedicated Starting Interface component is proposed and a considered suggestion:

   • **Purpose:** Assesses basic cybersecurity query knowledge and baseline command literacy before initiating topic-level training or lab deployment. (Addressed in initial skill assessment).

   • **Prompts:** Challenges students on how to ask an investigation question, how to define scope, and how to request a safe training lab within permitted boundaries. "Additional component for prompt engineering module at initial ranks".

   • **Integration:** ATE uses responses from the Starting Interface to initialize the skill profile and determine the appropriate entry level for the dynamic learning path. (Addressed in Dynamic Path Generation)

   - **Initial Skill Assessment:** It interacts with the user via conversational prompts and mini challenges that are only curated as per the user's mindset and knowledge base as the user progresses to use the platform to answer more questions according to their understanding of the concepts in order to create a detailed, initial skill-based profile, ranking the user on the leaderboard, where an anti-cheat system will be embedded to address if the user is authenticated by the means he is addressing and proctoring the user on fair usage.
   - **Dynamic Path generation:** It generates a personalized, modular learning-based curriculum that is highly focused on specific domains (example: OWASP Top 10 and LLM TOP 10), selecting and presenting "Rooms or Labs" based on the user's real-time performance.

- **Offensive/Defensive AI based generation:** On the user's request for addressing any vulnerability or CVE/CWE working analogy, the application will request the user to first define the CVE/CWE or vulnerability, and if the provided knowledge aligns with the correct definition of the same, the application will generate a webpage of the personalized isolated cloud storage to address the vulnerability by actually making the vulnerable webpage to simulate threat in real time, proceed step by step, and capture the flag that changes every time, and after that the user shall be addressed on how code should be to avoid/defend against vulnerability in any case.
- **Personalized Tutoring Path:** The artificial intelligence guides the user through the lab with step-by-step hints, explanations and questions while adapting in the real time to the user's actions. The lab shapes dynamically with CTFs and challenges that changes per session to avoid existing flags to be pasted through writeups and walkthroughs.
- **Proactive Defence Teaching:** After each vulnerability assessment phase, the application transits to a defence mode where the major goal is to guide the user to analyse and patch the vulnerability they just exploited, thereby teaching secure coding practices.

Remediation and Reporting: Each exploit requires a remediation and reporting, addressing the threat vectors, scope, POC etc. Learning from this system will ensure that user acknowledges correct format of reporting and presenting remediation.

3. **What were the other possible solutions and why they could not be done?**
    - **Existing E-learning Platforms (Coursera, Udemy):** These platforms provide structured video courses, but they always lack hands-on interactive lab environments, as they are passive methodologies for learning and do not provide real-time adaptive tutoring or practical exploitation.
    - **Current Cybersecurity Practicing Platforms:** While the platforms like HackTheBox and TryHackMe provide hands-on labs, the content is always static and nonadaptive, where they do not personalize the learning path according to the users' initial knowledge and will not generate custom labs based on the users' queries. The guidance provided is community driven or via prewritten write-ups, but not by any artificial intelligence-based agent.
    - **Enrolment in Coaching centers and physical classes**: This mode of education is costly, not scalable, and highly dependent on the tutors' expertise and availability, which cannot provide the instant on-demand lab generation too.

4. **What are the advantages of the solution proposed by you?**
    - **Personalized User based path generation:** Each user is given their own unique learning plan, which ranges from being a total beginner to an expert. Via recursive

assessment and profiling the application will improve itself refined with user's knowledge.

- **Deep Conceptual Understanding:** This method of making users explain the concepts beforehand is a way of verifying if their foundational knowledge is strong enough for them to learn through practical exercises.
- **Adaptive Difficulty:** Based on a user's performance, the system changes the level of difficulty of the labs and hints given to him/her.
- **Efficiency:** The users get their time saved since the system goes directly to their specific knowledge gaps and does not make them go through a lot of irrelevant information.
- **Comprehensive Skill Development:** The training of offensive (attack) and defensive (remediation) skills is combined in a single exercise which flows smoothly.
- **Scalability:** As a cloud-based platform that is powered by AI, it is able to provide the same high-quality tutoring to an unlimited number of users at once with prompted creation and dynamic cloud-based enhancements.

Addressing acknowledgment and respectful Amendment for Physical Kiosk Hardware Deployment:

The Physical Kiosk Hardware deployment offers advantages in supervised, high-stakes assessment environments, it introduces a significant limitation: hardware dependency reduces scalability, accessibility, and deployment reach.

The present invention is therefore amended to acknowledge that the preferred and more broadly applicable embodiment is a web-based or software-only deployment (Lockdown Browser based Web application), rather than a hardware-bound kiosk implementation.

5. **Explain the stepwise working of the innovation explaining all the components used in the invention and the specific function they are performing.**

Phase 1: User Initiation & Skill Assessment

A new top-level system component, the Central Control Unit (CCU), is introduced and was not present in the original patent disclosure and is considered suggestion:

• **CCU Function:** Orchestrates all system operations: authentication, curriculum delivery, lab deployment, AI inference, scoring, feedback, storage, anti-cheat controls, and network synchronization.

• **CCU Composition:** Comprises secure boot firmware, encrypted local storage, and a real-time scheduler to coordinate camera, microphone, telemetry, and lab sessions with addition to secure lockdown browser-based application logging system to ensure anti-cheat functionalities.

- **User Query:** The whole working analogy starts at User Interface (UI), where a user prompts a query such as “Teach me about SQL injection” or “How IDOR works and explain BAC”
- **Initial Analyses and Explanation Request:** The query will be analyzed by the AI tutoring engine (ATE), where the prompt analyzer (PA) will interpret the request. Instead of directly giving information, the ATE will invoke Explain Eval Module (EE), where this module challenges the user to first explain their current understanding of the concept (e.g., “How do you think SQL injection works?” or “Define Broken Access Control (BAC) in layman’s terms”).
- **Skill Profiling:** The user’s textual explanation is sent back to the ATE, and the PA and Adaptive Guidance and Scoring (AG) modules will analyze this response for its accuracy, depth, and terminology. Simultaneously, the User Profile Manager (UPM) is queried to retrieve the user’s historical skill data. The result will reflect the current and dynamic assessment of the user’s knowledge gap on the topic.

Phase 2: Dynamic Lab Generation and Delivery

- **Curriculum Generation:** The analyzed explanations pass through the Safety and Compliance Gate (SG) which is to ensure that the query and response shall remain within the platform's ethical and operational bounds (the platform will be addressed with transcripts and data sets from ethical sources setting up controls for the same, ranging from compliance like SPDI Rules, DPDP Act, NCSP etc). Once approved, the Curriculum Generator (CG) creates a personalized learning objective and query the Central Repository (CR), which contains sanitized vulnerability templates based on CVE/CWE metadata, and lab blueprints to determine the appropriate lab structure.
- **Orchestration Request:** The ATE will send a formal deployment instruction to the Cloud-Based Lab Orchestrator (CBO). This instruction will specify the vulnerability type and the desired difficulty according to user's skill assessment and the session based parameters.
- **Environmental Construction: inside the CBO:**
  - **The Environment Builder / template Engine (EB)** fetches the corresponding safe lab from the CR and instantiates it.
  - **The Deployment Service (DS)** deploys the template, creating a vulnerable web application.
  - The application is launched within a secure, **Ephemeral sandbox (SB)** that is dedicated solely to that user's session.
  - **The Flag Manager (FM)** creates a unique, randomly generated flag for this particular session and embeds it into the application automatically.
  - **The Network Isolator (NI)** makes sure that the sandboxed environment is controlled or has no external egress to avoid any misuse at all.
  - **The Secure Artifact Scanner (SAC)** monitors the deployed environment for any unintentional security risks before it is made public preventing leaks.

Phase 3: Guided Interactive Learning and Execution

- **User Interaction with Lab:** The user directly interacts with the vulnerable application via the interface in his/her isolated sandbox attempting to discover and exploit the vulnerability in order to capture the dynamic flag.
- **Real-Time Monitoring and Hint Generation:** The Activity Recorder and Telemetry (AR) module documents every action taken by the user in the laboratory. All this telemetry data is sent back to the ATE.
- **The Adaptive Guidance and Scoring (AG)** module performs a real-time evaluation of these actions.
- If the user is having a hard time or is showing a misunderstanding, the **Hint Generator (HG)** is giving context-aware, incremental hints to guide the user without disclosing the answers.

A computer-vision proctoring subsystem is proposed as a new component not described in the original patent and is considered suggestion:

• **Detection:** Detects head pose shifts and repeated gaze deviations consistent with peeking towards a phone, another desk, or unauthorized materials; correlates with interaction telemetry.

• **Enforcement:** Issues on-screen warnings and audible prompts; records events in Immutable Audit Logs (LOGS); may apply hint lock, time penalty, supervisor alert, or session pause per institutional policy.

• **Data Fusion:** Camera-derived signals are not used standalone; fused with performance signals by the Adaptive Guidance and Scoring (AG) module for integrity and adaptive guidance timing.

Phase 4: Analysis, Defence, and Closure

- **Flag Capture & Success Analysis:** The system records the user's event whenever he/she captures the flag. The ATE's Adaptive Guidance & Scoring (AG) module modifies the user's skill profile in the User Profile Manager (UPM), which signifies an improvement in that area.
- **Transition to Defence Mode:** The ATE has now moved the session from the "attack" mode to the "defence" mode. It is leading the user to the sandbox where the application’s code is and is then asking for the detection of the code segment that is prone to attack and a fix suggestion.
- **Remediation Guidance:** Step by step, the ATE, using the Central Repository (CR) as a source for safe coding snippets and patches, instructs the developer to fix the coding error, thus applying the secure coding principles.

A new consequence-oriented teaching module is proposed, not present in any phase of the original patent and is considered suggestion:

• **Purpose:** Presents real-life adverse case scenarios that may occur due to mistakes, negligence, or incompetence in cybersecurity practice and decision-making.

• **Content:** Delivers curated incident re-enactments and consequence narratives: data breach impact, business downtime, compliance penalties, privacy harm, and chain-reaction failures caused by weak access control, unsafe input handling, insecure secrets management, or flawed prompt workflows.

• **ATE Integration:** After a failed assessment item or incorrect remediation, the system automatically plays an appropriate adverse scenario and then provides a corrective micro-lesson.

An Explainable AI module is proposed to provide transparent scoring and targeted recommendations, entirely new to the original patent:

• **Scoring Rationale:** Explains why marks were awarded or deducted based on concept accuracy, procedural correctness, severity reasoning, and mitigation quality.

• **Weakness Mapping:** Maintains a weakness map organised by domain, task type, and difficulty level; feeds this map back to the curriculum generator for dynamic path generation.

Phase 5: Session Teardown & Logging

- **Session Conclusion & Forensic Capture:** CBO's Auto-teardown & Forensic Snapshot (TD) module finishes the sandbox after the learning goal has been accomplished. From the perspective of a Snapshot Final State, it can be an option for future review or evaluation.
- **Immutable Logging:** The whole procedure is logged through the Immutable Audit Logs (LOGS) under Security & Governance, which document every significant action: the original query, the AI's evaluation, laboratory establishment, user interaction, and flag collection. This provides a full and unchallengeable trail for security and compliance purposes. All laboratory artifacts along with flags are stored in the Personalized Isolated Cloud Storage (PIS).
- **Continuous Adaptation:** The entire interaction is directed back to the User Profile Manager (UPM), which not only means that the system will be smarter in the user's next session but also that a continually adapting learning path will be provided.

6. **Attach drawing hand-made/ computer made showing all the components of the Invention.**

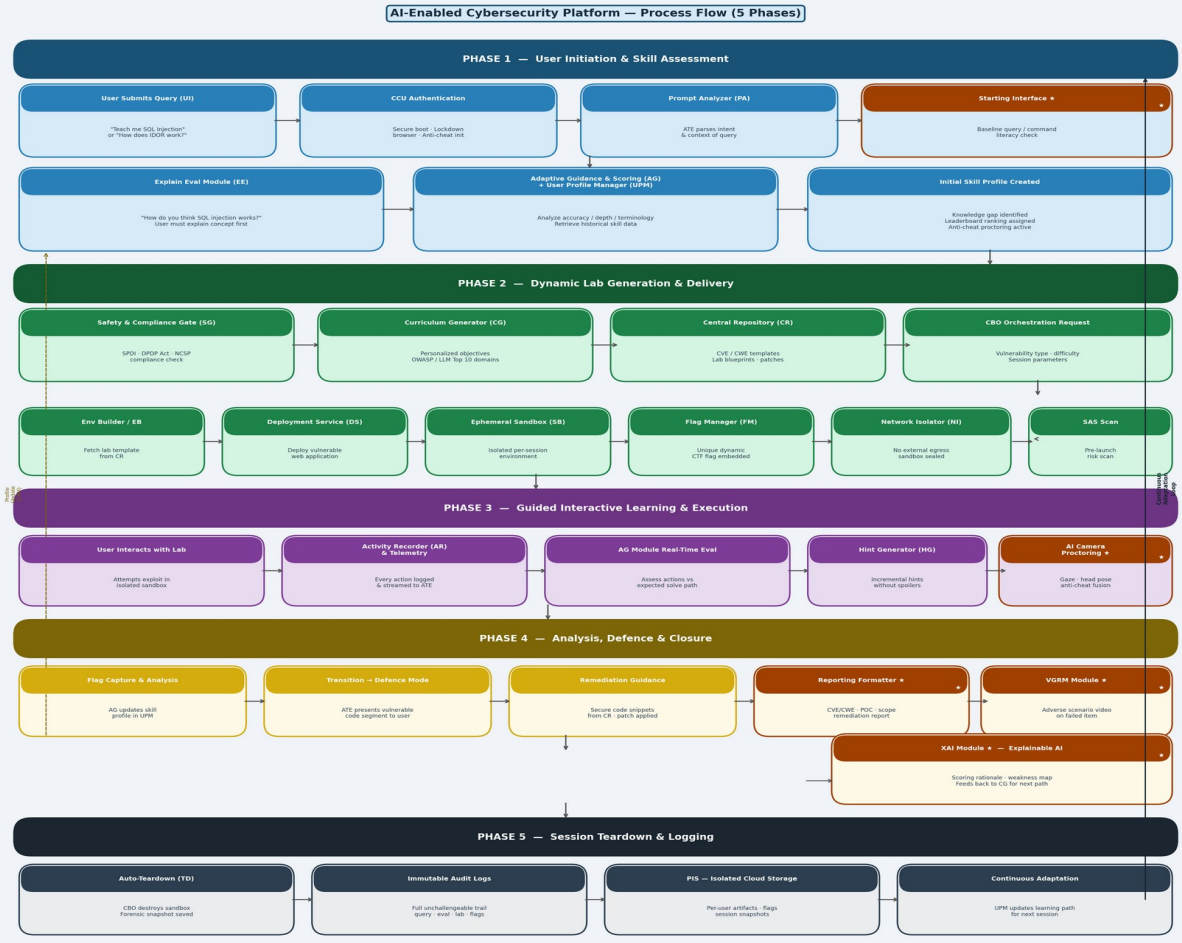


Figure 2 — Process Flow Diagram (5 Phases)

FIG. 4: AI TUTORING ENGINE (ATE) – INTERNAL ARCHITECTURE

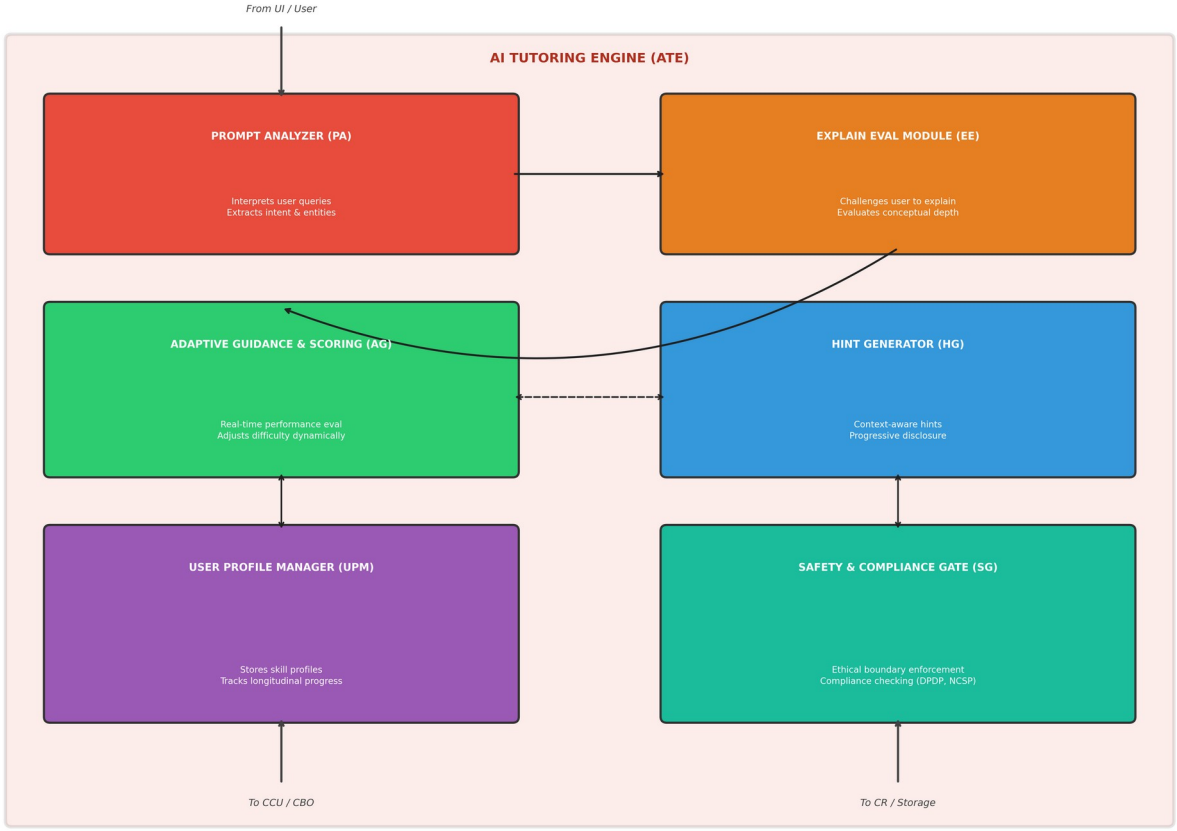


FIG. 1: OVERALL SYSTEM ARCHITECTURE – AI-POWERED CYBERSECURITY TRAINING PLATFORM

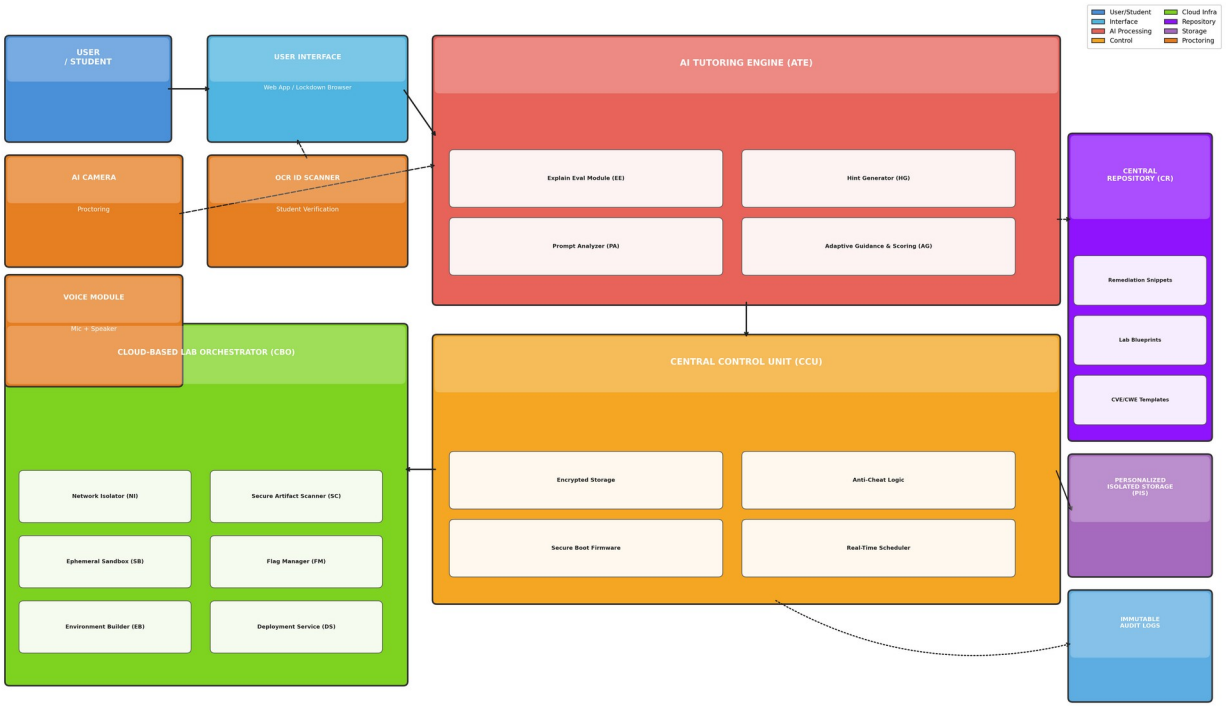


FIG. 2: COMPLETE 5-PHASE ASSESSMENT & REMEDIATION CYCLE

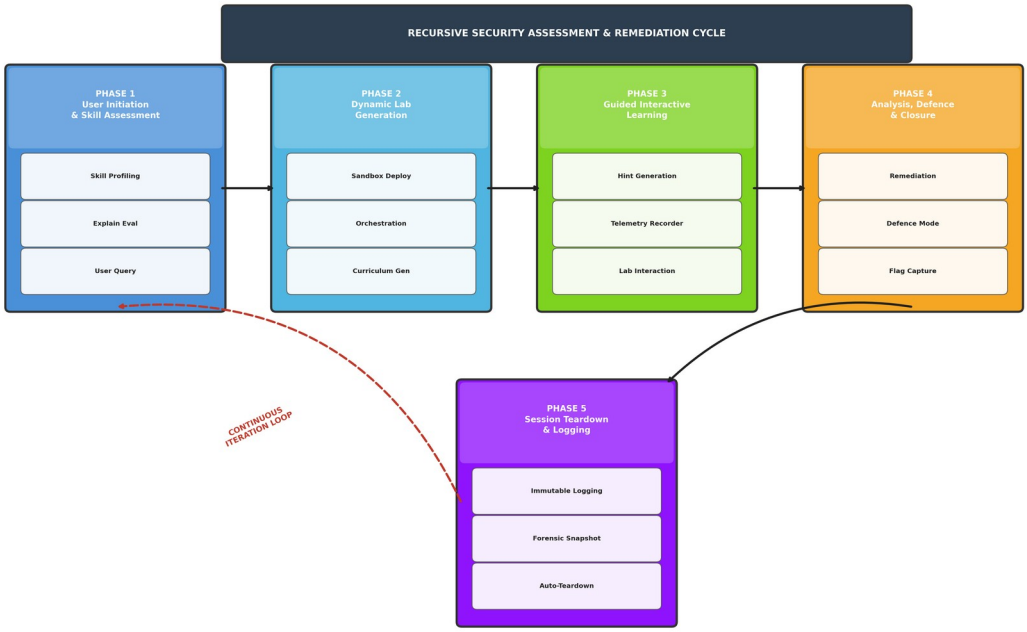
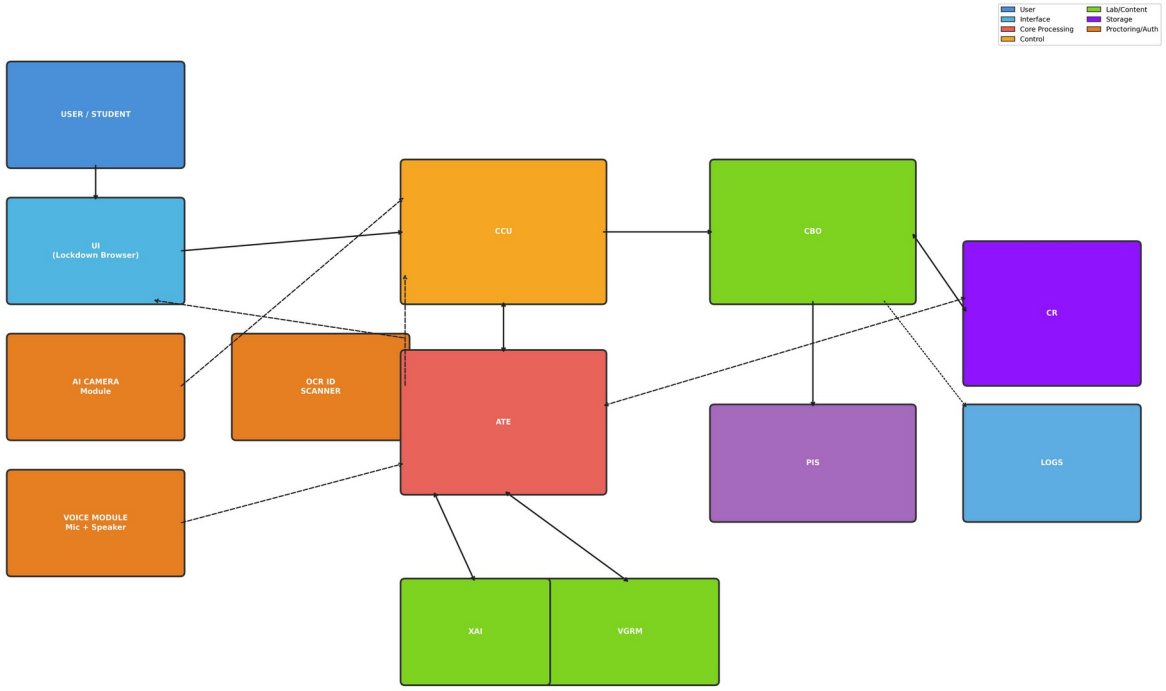


FIG. 3: SYSTEM COMPONENT INTERACTION & DATA FLOW DIAGRAM



Relevant Key phrases relating to your invention

S.NO.	Key phrases
1.	Adaptive Cybersecurity Tutor
2.	AI-Powered Penetration Testing Platform
3.	Dynamic Vulnerability Lab Generation
4.	Recursive Learning Analysis Engine
5.	Personalized Web Application Security Training
6.	Isolated Cloud-Based Cyber Range
7.	OWASP Top 10 AI Tutor
8.	Automated Skill Assessment for Cybersecurity
9.	AI-Guided Attack and Defence Training
10.	Explainable AI Scoring for Cybersecurity Competency
11.	Consequence-Driven Adverse Scenario Teaching Module
12.	Dynamic Flag Integrity and Anti-Cheat Mechanism