AI-Powered Education: Prompts & Cybersecurity

Presented by:

Ass. Prof. Farah Jemili, ISITCOM, University of Sousse

1st Summer School - Sousse, 26/09/2025

Farah JEMILI

- Associate Professor in Computer Science
- Researcher in Artificial Intelligence & Big Data Analysis
- Internship Director at ISITCOM, University of Sousse
- Scientific Referent at the Tunisian Agency for Evaluation and Accreditation in Higher Education and Scientific Research (ATEA)
- Member of the Erasmus+ EduGame Project, Sousse Team


invideo/tunisie
Welcome to Tunisia,

University of Sousse

Founded in 1986

- 4 Faculties
- 10 Institutes
- 3 Schools
- 3830 Students
- 2175 Teachers
- 919 Administrative Staff

1
- Arts, Humanities, and Social Sciences

2
- Technology and Engineering

3
- Health Sciences

4
- Economic Sciences and Management

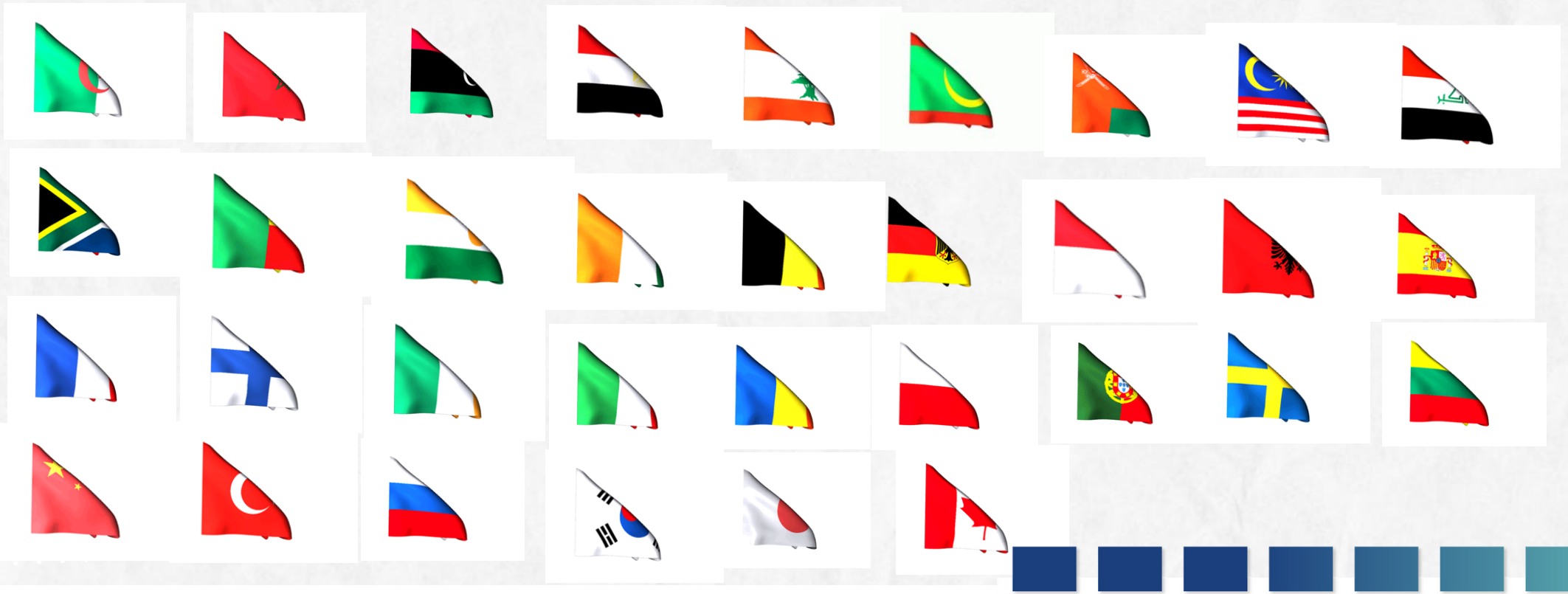
5
- Agronomic Sciences

UNIVERSITY OF SOUSSE
جامعة سوسة
Socially Responsible University

International Partnerships

- **Bilateral Agreements Since 2004**

117



International Projects

- **Erasmus+ Program**

  43 ICM Bilateral Agreements
  31 CBHE Projects

- **02 ENICIBCMED Projects**

- **05 Horizon Europe projects**

- **01 European Research Council Project (ERC)**

39 projects

4 Projects coordinated by the University of Sousse

ISITCOM

Founded in August 2001

- 1369 Students
- 92 Faculty members
- 40 Technical and Administrative Staff

Main Programs

3 Licences

- Telecommunication
- Embedded Systems & Internet of Things
- Computer Science & Multimedia

2 Professional Masters

- Web Services & Multimedia
- Network Services & Security

Research Master

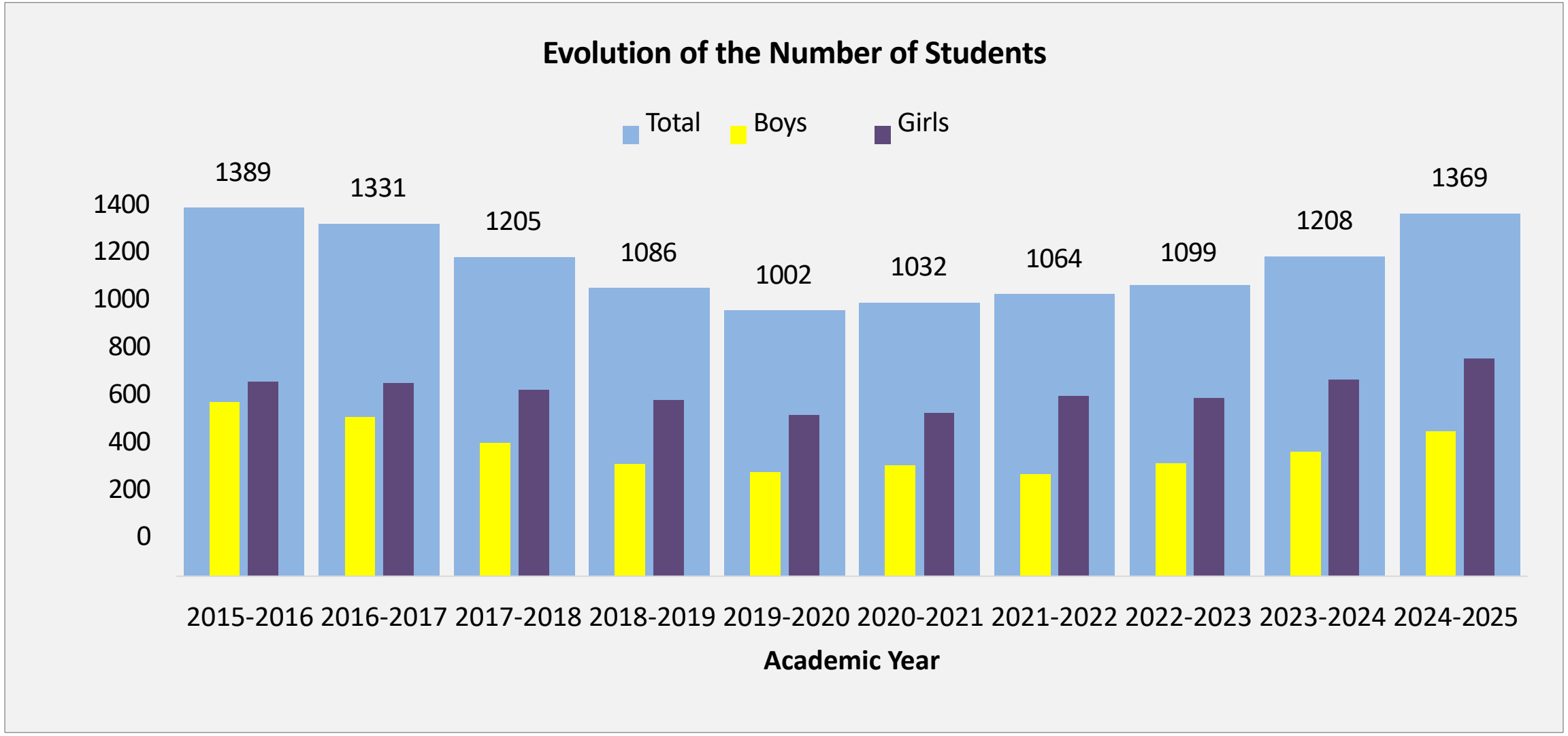
- Artificial Intelligence & Data Analysis

Engineering

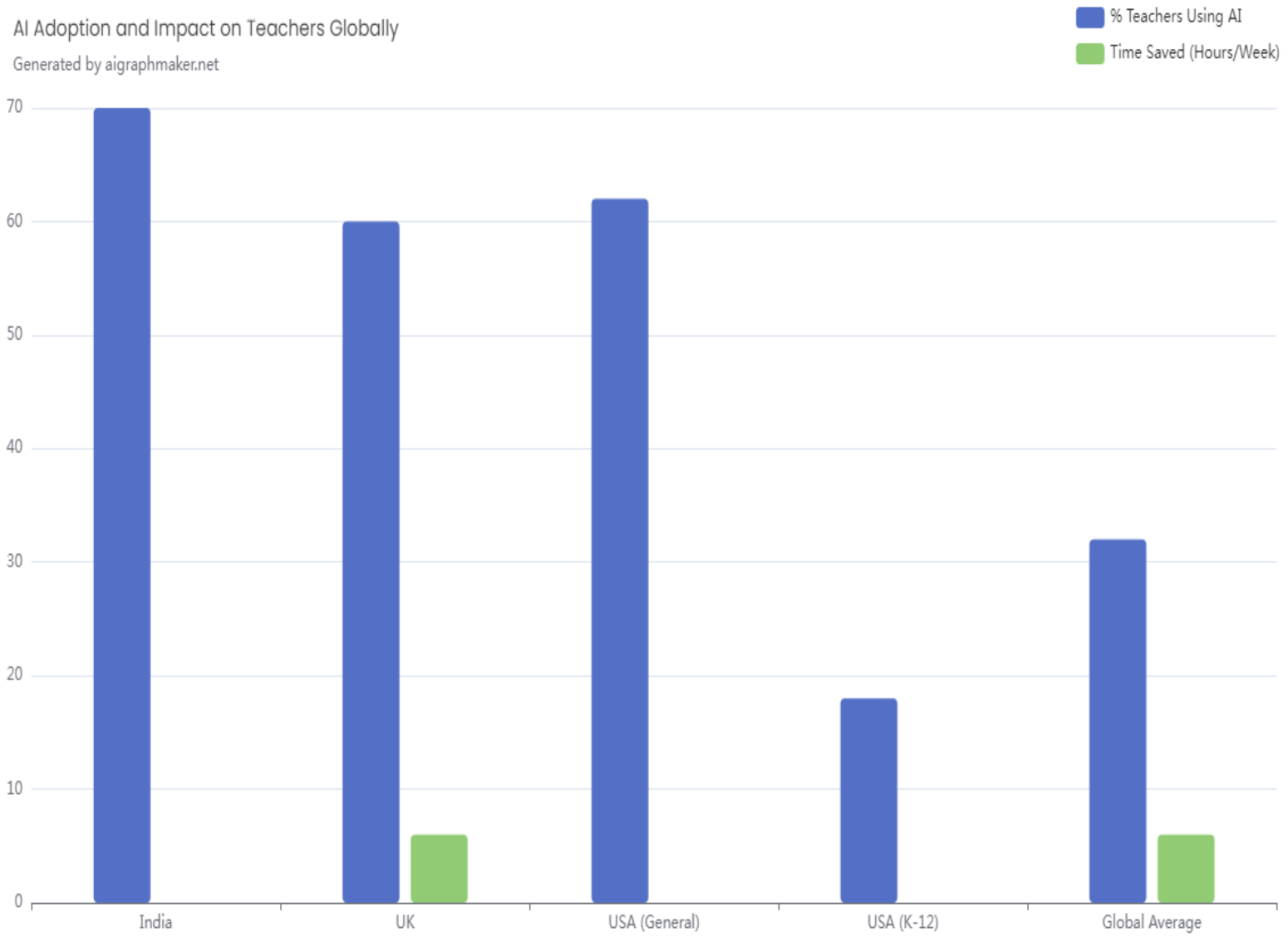
- Teleinformatics

Doctorate

- Computer Science

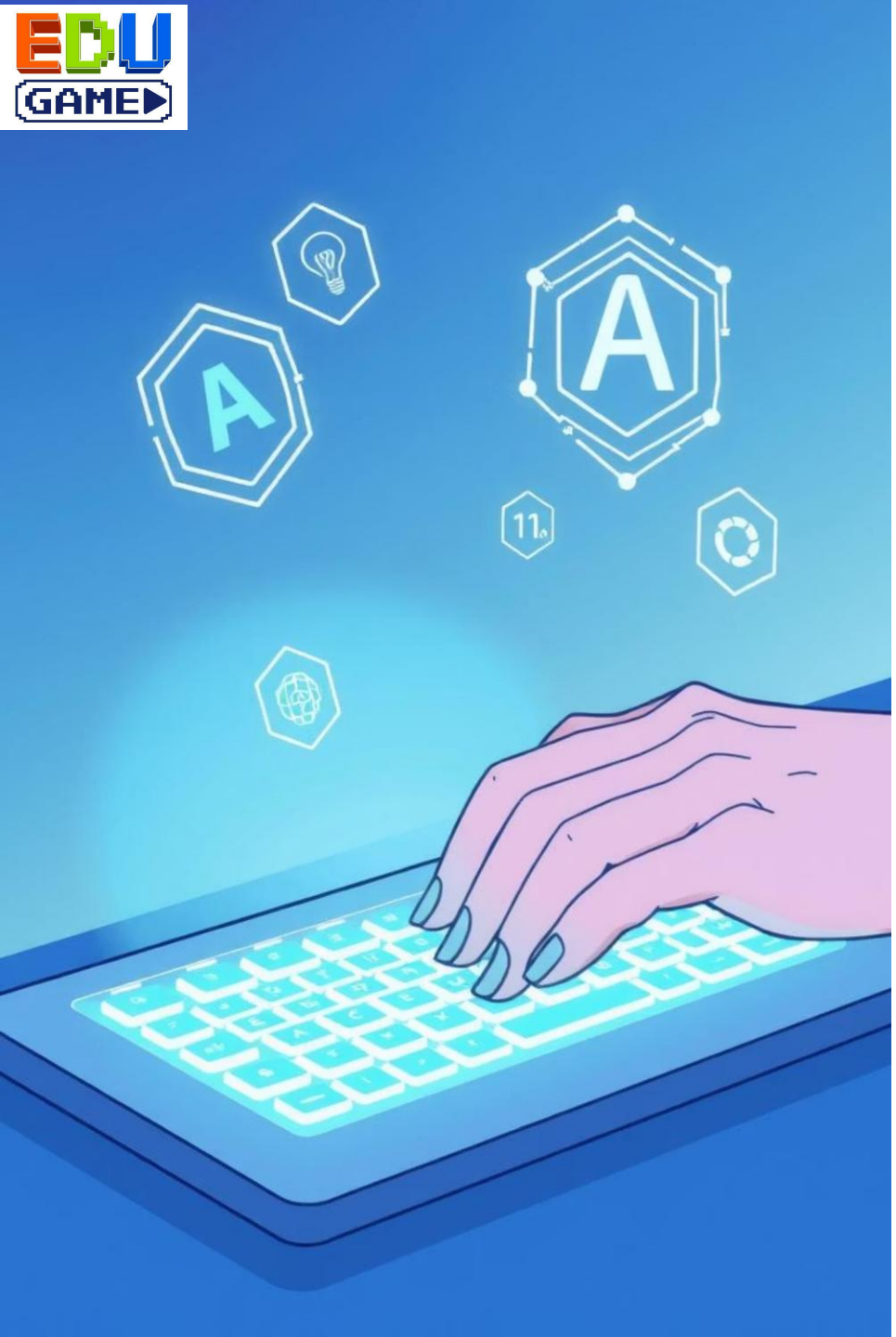

Evolution of the Number of Students
Total
Boys
Girls
1389
1331
1205
1086
1002
1032
1064
1099
1208
1369
1400
1200
1000
800
600
400
200
0
2015-2016
2016-2017
2017-2018
2018-2019
2019-2020
2020-2021
2021-2022
2022-2023
2023-2024
2024-2025
Academic Year

Usage of AI Tools by Teachers (Global Snapshot, 2024-2025)



AI Powered Education: Prompt Engineering

AI-powered education is revolutionizing how we learn and teach. This presentation explores the **transformative potential of artificial intelligence** in academic settings, focusing on the critical role of prompt engineering.



What is Prompt Engineering?

Defining the Art

Prompt engineering is **the strategic strategic craft of designing inputs** to to effectively guide AI in generating generating desired outputs.

Essential for AI Tools

It is crucial for **maximizing the utility** of **utility** of AI-driven tools like ChatGPT, ChatGPT, Copilot, and other conversational agents.

Shaping AI Responses

This skill is **vital for eliciting accurate, useful, and ethically sound responses** from from artificial intelligence systems.

Why Prompt Engineering Matters in Matters in Education

Enhances Personalized Learning

Tailors educational content and experiences to **individual student needs and learning learning styles**, fostering deeper understanding.

Cultivates Better Questions

Empowers students **to formulate precise and insightful queries**, improving their their research and critical thinking abilities.

Supports Teacher Productivity

Assists educators in **efficiently designing engaging assessments, dynamic lessons, and lessons, and comprehensive curriculum materials**.

Fosters Creativity & Critical Thinking

Encourages **innovative problem-solving and the development of analytical skills** by **skills** by interacting effectively with AI.

Techniques of Prompt Engineering

Clear & Specific Instructions

Begin with explicit commands to guide the AI, ensuring clarity and avoiding ambiguity in requests.

Contextualizing the Question

Provide relevant background information to help the AI understand the scope and intent of the query.

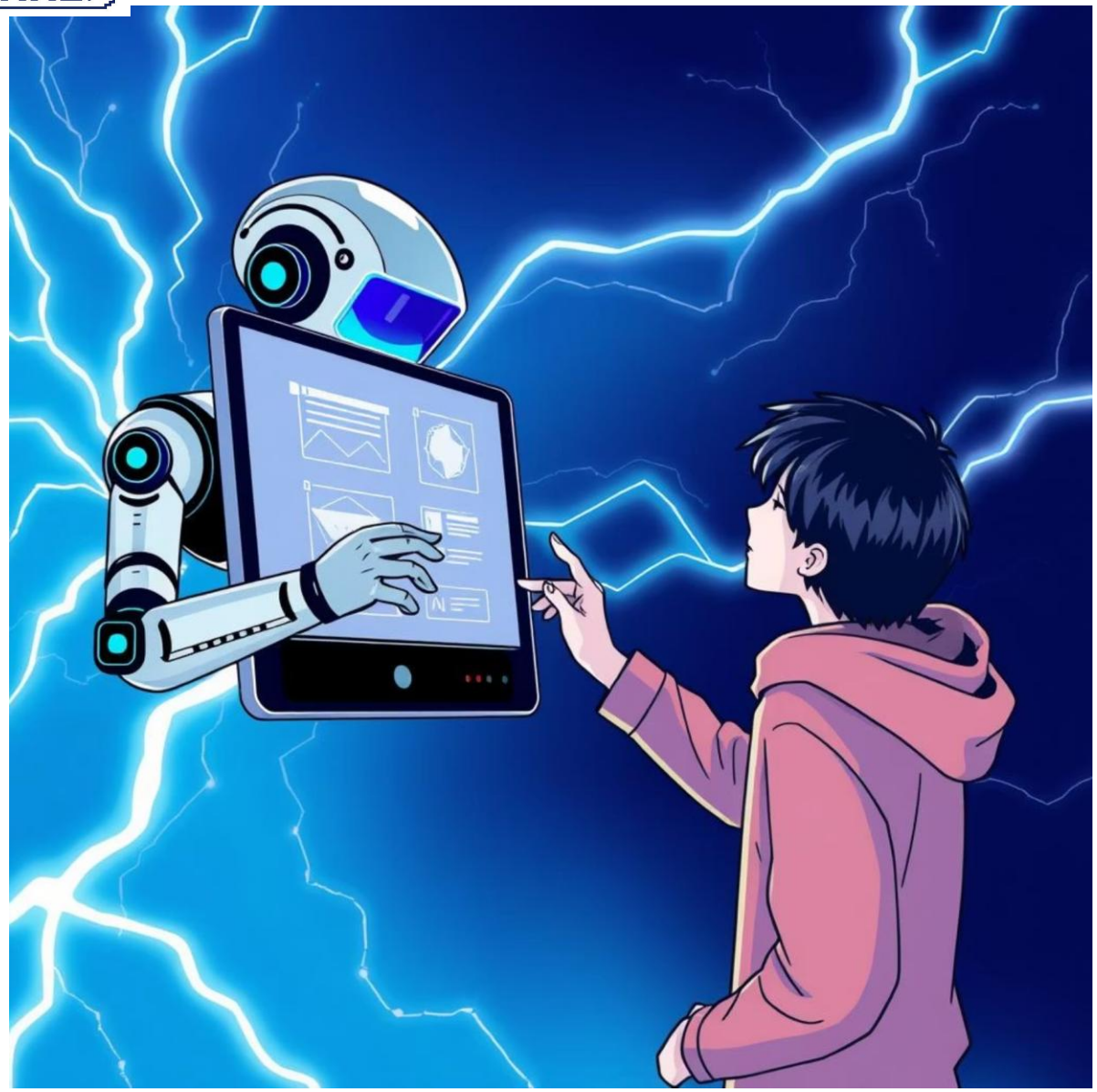
Role Assignment

Instruct the AI to "Act as a teacher" or "Act as a historian" to frame its response from a specific perspective. specific perspective.

Iterative Refinement

Continuously adjust and improve prompts based on initial AI responses to achieve optimal outcomes.

Examples in Education



Example: Quiz with Educaplay

Creating Quizzes & Exercises

Generating Explanations

AI Tools in Education (General Overview)

Tutoring & Q&A

Platforms like ChatGPT and Perplexity AI offer instant answers and personalized tutoring support.

Assessment & Feedback

Tools such as Gradescope and Turnitin AI assist in grading and detecting plagiarism, streamlining evaluation.

Content Creation

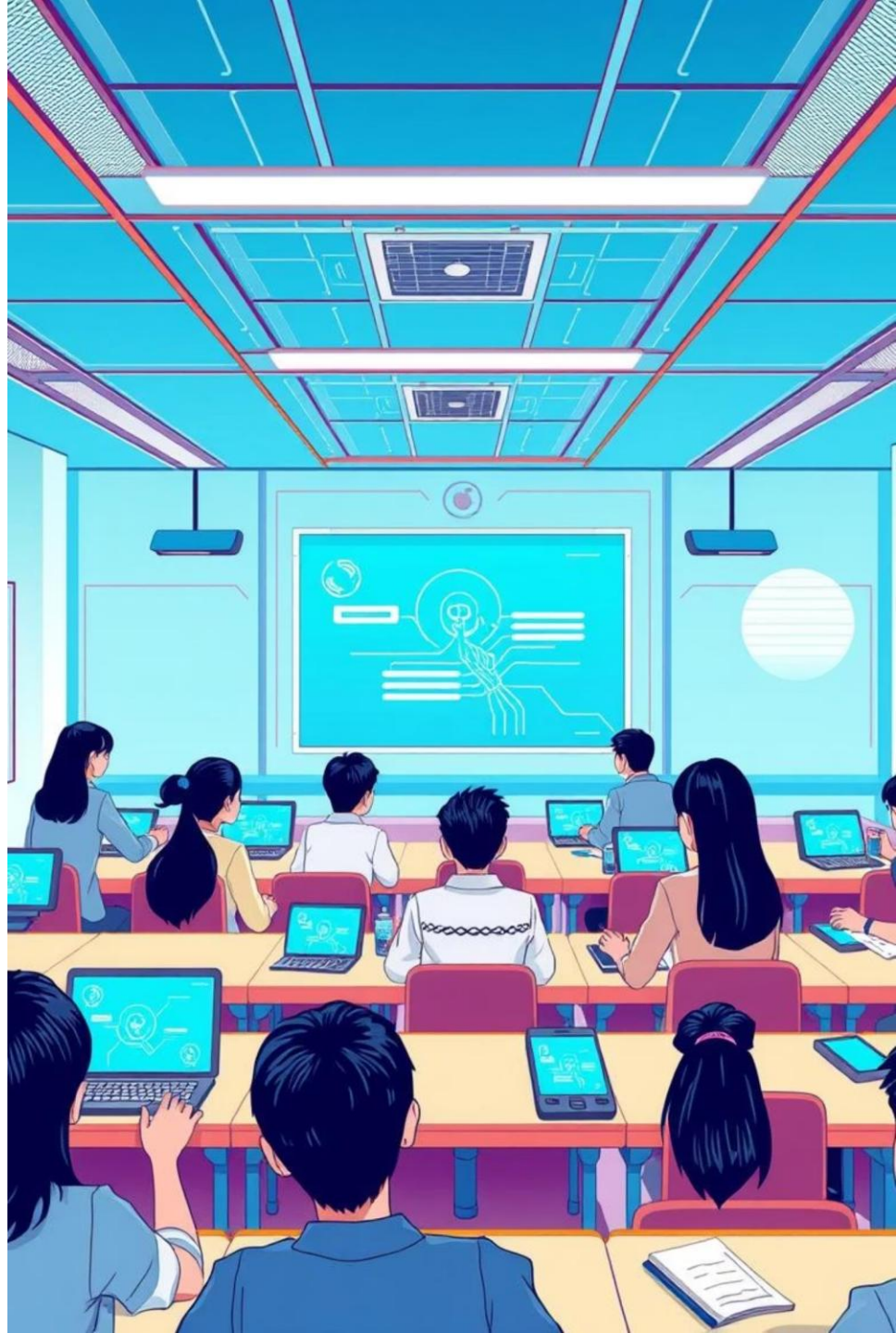
Canva AI and Quizlet AI empower users to create engaging visual content and interactive study materials.

Language Learning

Apps like Duolingo AI and Elsa Speak utilize AI for adaptive language instruction and pronunciation feedback.

Examples of AI Tools Transforming Education in 2025

Discover how artificial intelligence is revolutionizing the learning experience, making education **more accessible, personalized, and engaging** for students and educators alike.

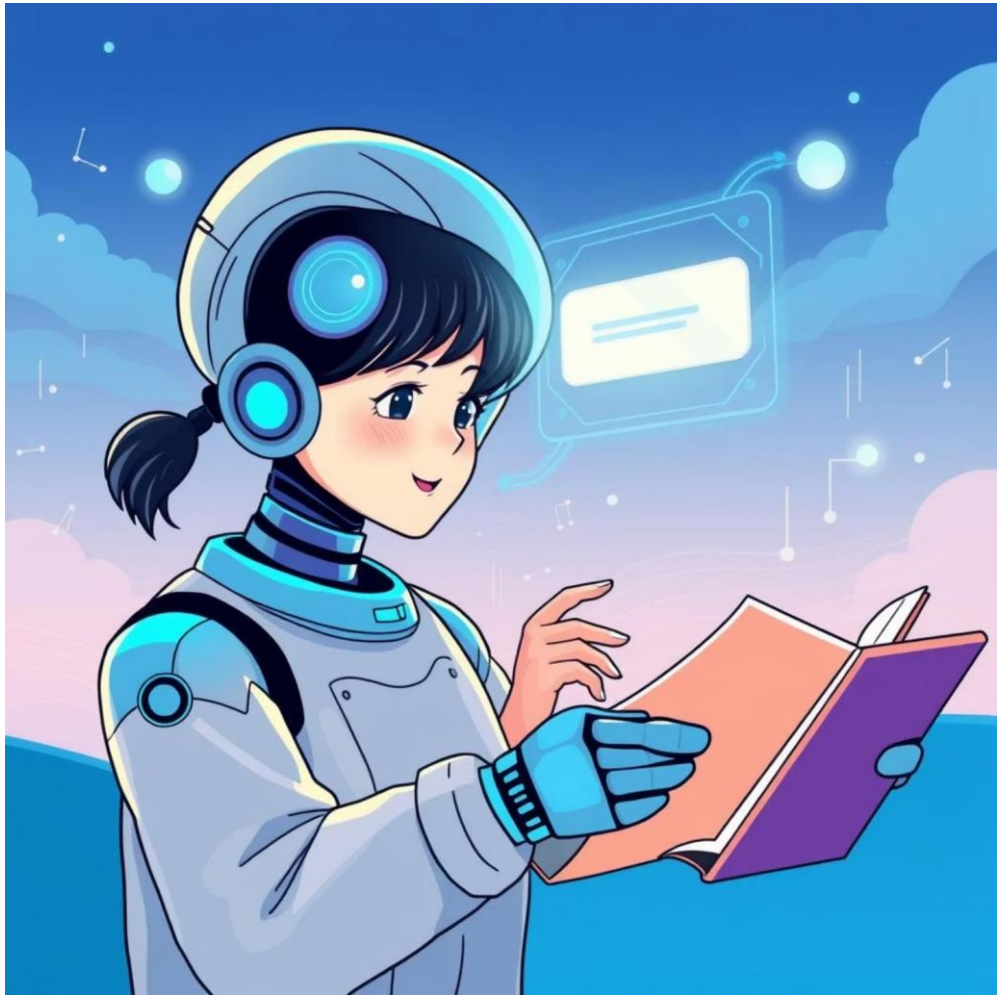


Claude: The Conversational AI Assistant for Learning

Developed by Anthropic, Claude offers safe, helpful AI chat support tailored for education, prioritizing ethical interactions.

It enables students to brainstorm ideas, get clear explanations, and explanations, and receive personalized tutoring in natural language, language, fostering deeper understanding.

Claude's focus on ethical AI use significantly reduces misinformation and bias in classroom settings, promoting reliable learning.



Narakeet & Dupdub: AI-Powered Multimedia Creation

Narakeet: Text to Video

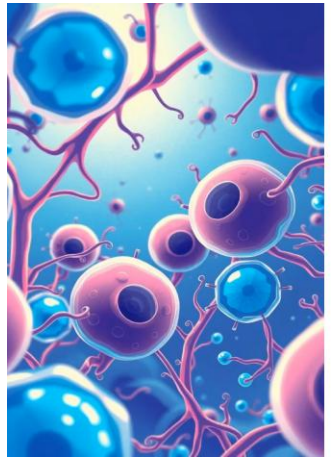
Converts text into narrated videos with with customizable voices and subtitles, subtitles, making content creation effortless.

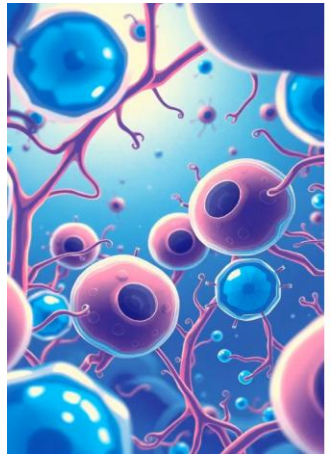
Dupdub: Multilingual Dubbing Dubbing

Automates dubbing and voiceovers in multiple languages, significantly enhancing enhancing accessibility for diverse learners. learners.

Engaging Content

Both tools empower educators to create dynamic, multilingual educational content quickly and efficiently.



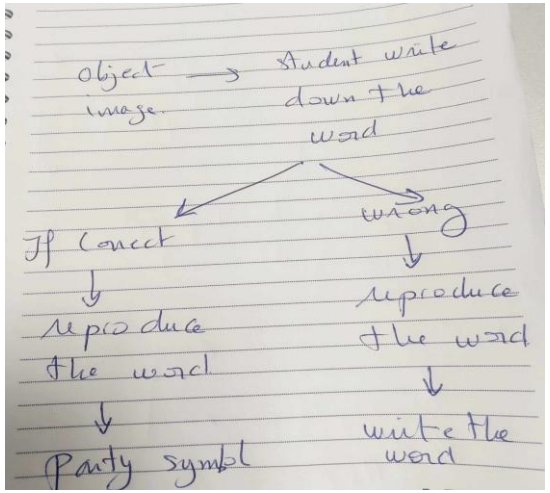


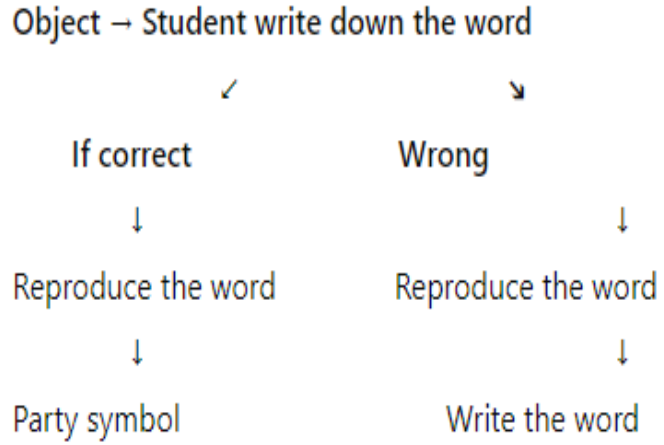
ChatGPT: The Versatile AI Tutor and Content Generator

OpenAI's ChatGPT supports writing, provides coding help, and offers and offers personalized tutoring across various subjects.

Millions of students use it for instant feedback, essay drafting, and and concept clarification, enhancing their learning process.

Its integration into classrooms sparks important debates on academic integrity and ethical AI use, shaping future educational policies.





Napkin & Gamma: Visualizing Complex Ideas with AI

Napkin AI: Simplify Complex Complex Topics

Breaks down intricate subjects into simple, simple, digestible explanations, making making learning easier and more accessible.

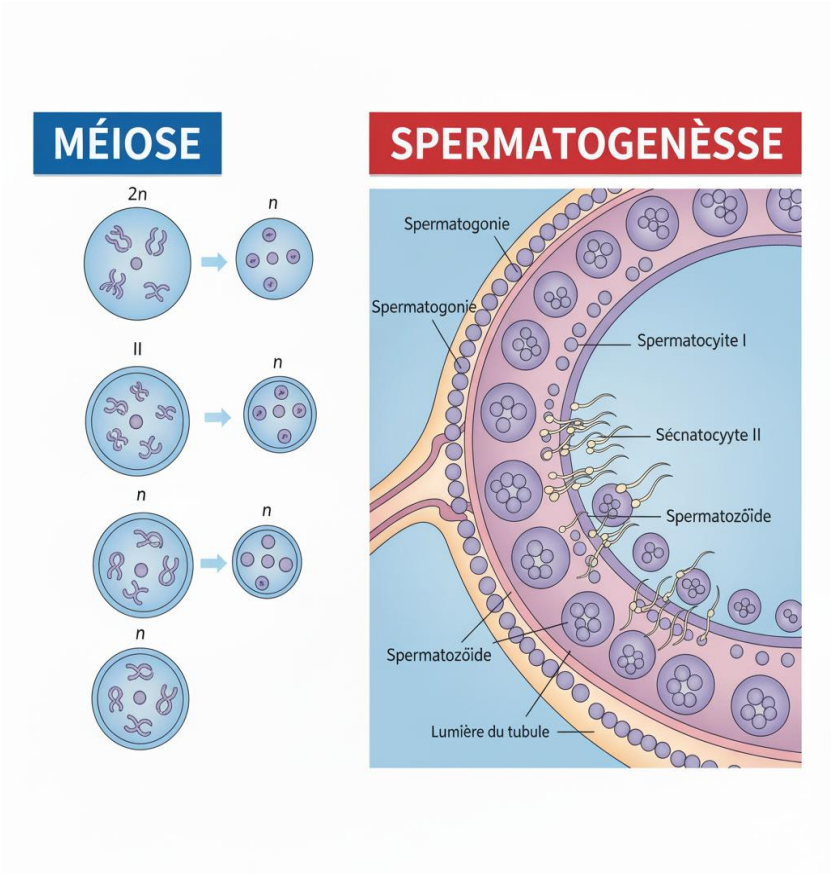
Gamma AI: Dynamic Presentations

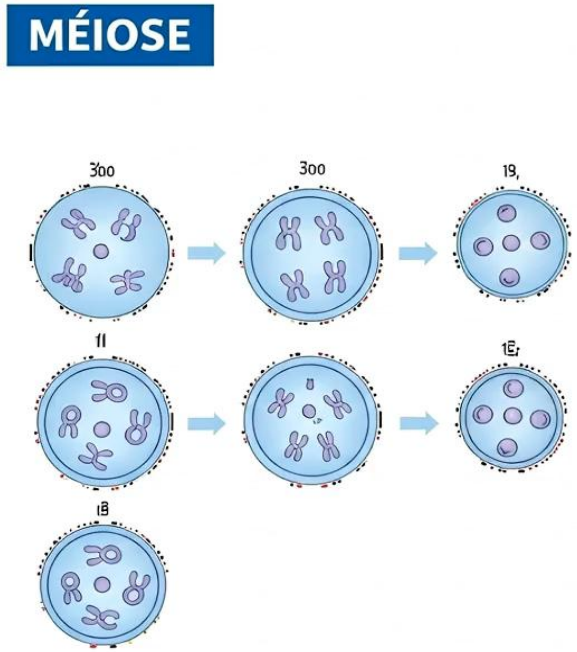
Helps educators and students create AI-AI-enhanced presentations with seamless seamless media integration and engaging engaging layouts.

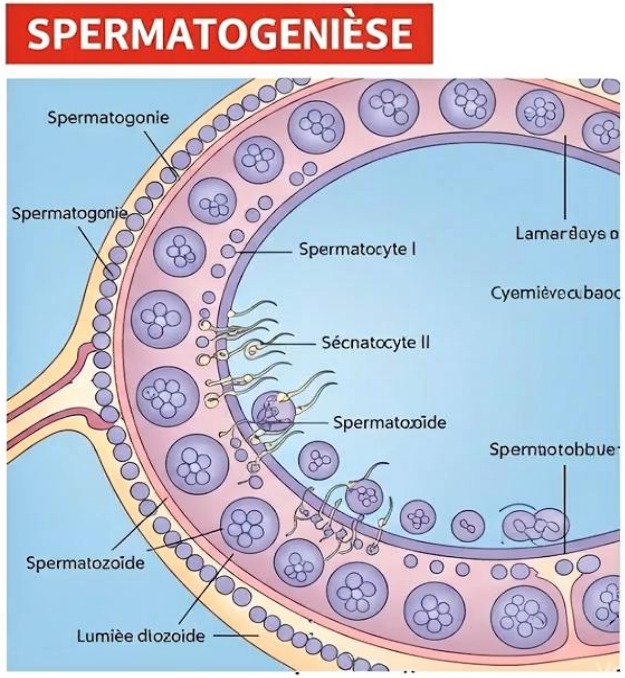
Clear Visual Learning

Both tools transform abstract concepts into clear, compelling, and visually rich learning experiences, improving comprehension.

Visualizing Complex Ideas with AI







SpeechNotes & NoteBookLm: AI for Note-Taking and Study Support

SpeechNotes: Accurate Transcription

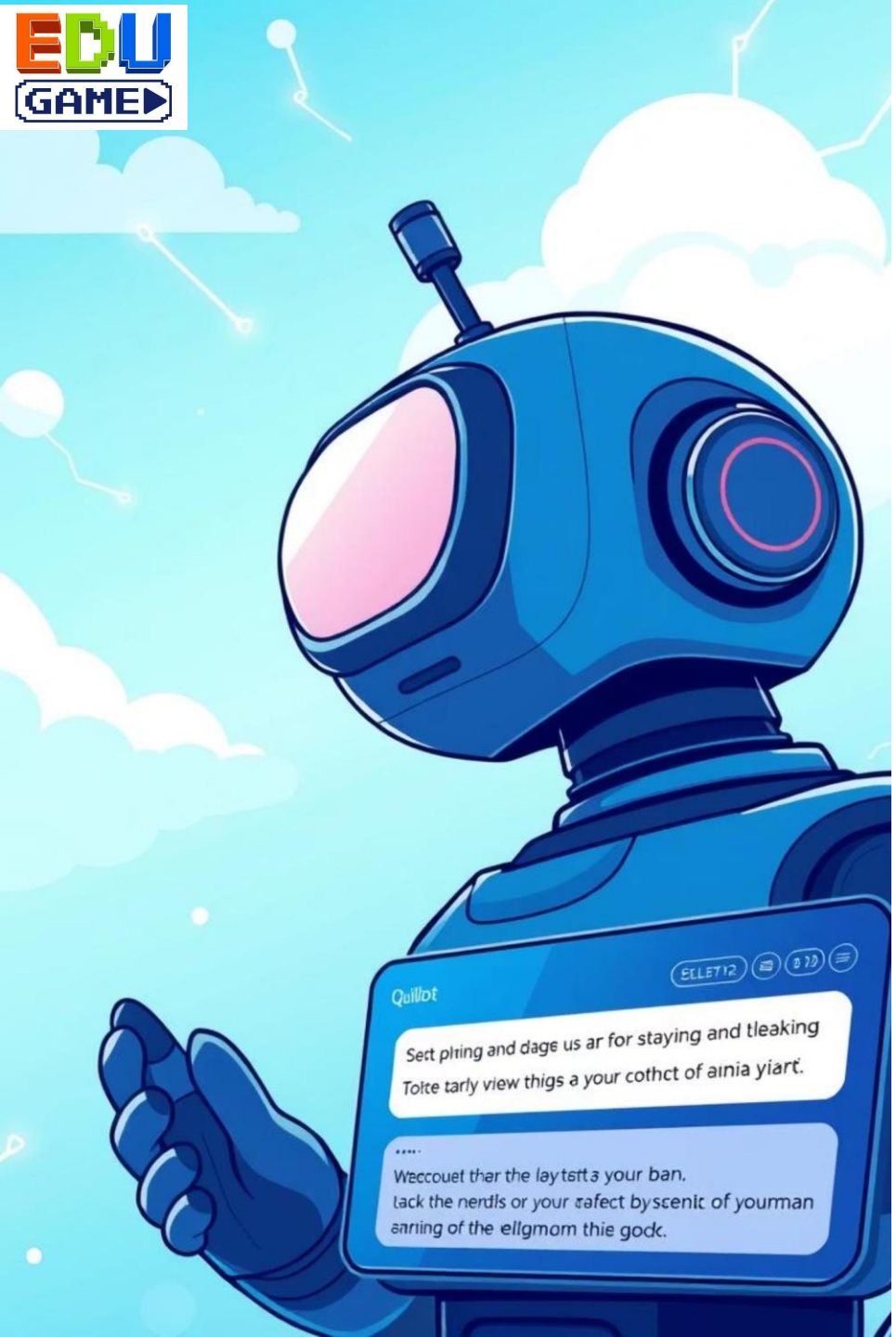
Converts spoken words to text with high accuracy, assisting students with disabilities and those who multitask.

NoteBookLm: AI Study Assistant

By Google, it offers AI-powered study assistance, summarizing notes and answering questions from study materials.

Boost Productivity

These tools significantly boost productivity and accessibility in diverse learning environments, fostering inclusive education.



Quillbot: AI-Powered Writing and Paraphrasing Assistant

Quillbot is an essential tool for academic success, helping students refine their writing writing with intelligent AI.

Improve Writing Clarity

It helps students improve writing clarity, grammar, and style through intelligent AI suggestions, enhancing overall quality.

Support Language Learners

Supports language learners by rephrasing text and expanding vocabulary, aiding in language acquisition.

Enhance Academic Skills

Widely adopted for essay editing and enhancing academic writing skills, ensuring students produce polished work.

Chat PDF: AI-Driven Document Interaction

Instant Answers

Allows users to upload PDFs and ask questions about the content content conversationally, getting instant answers.

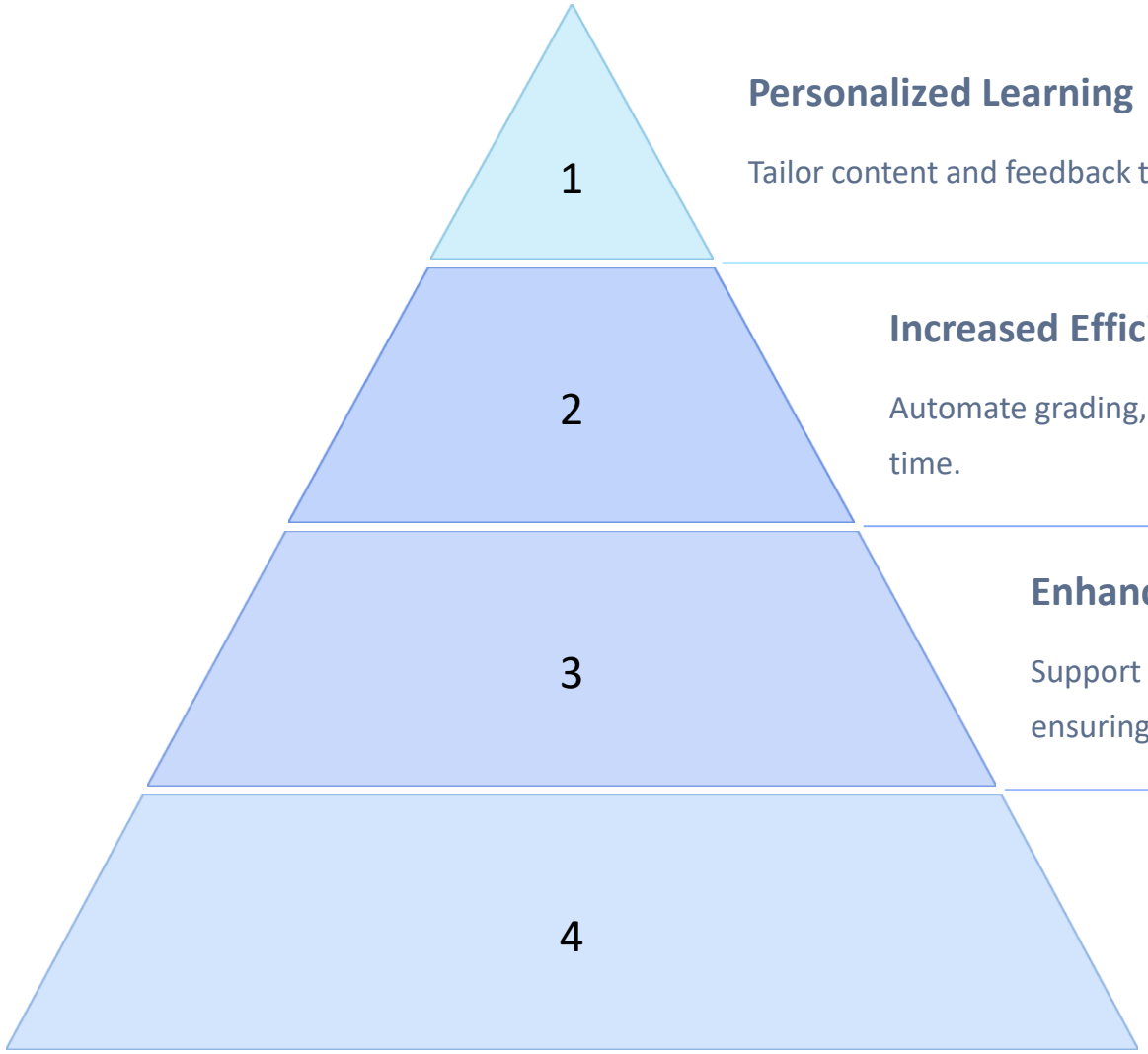
Deeper Engagement

Facilitates deeper engagement with textbooks, research papers, and papers, and study materials, promoting active learning.

Time-Saving Summaries

Saves valuable time by summarizing and extracting key information information instantly, streamlining research and study processes. processes.

Why These AI Tools Matter in Education Today



Personalized Learning

Tailor content and feedback to individual student needs, creating unique learning paths.

Increased Efficiency

Automate grading, content creation, and administrative tasks, freeing up educator time. time.

Enhanced Accessibility

Support diverse learners with speech, language, and multimedia tools, ensuring ensuring inclusivity.

Greater Engagement

Make learning interactive, visual, and multilingual, captivating student student attention.

Benefits for Teachers

Time-Saving in Lesson Lesson Planning

AI helps teachers generate ideas, ideas, create materials, and design design activities more efficiently, efficiently, freeing up valuable time.

Unlocking New Teaching Strategies

AI introduces innovative pedagogical approaches, allowing for more dynamic and interactive classroom experiences.

Access to Richer Learning Resources

Educators can leverage AI to discover and curate a wider range of diverse and diverse and engaging educational content.

Benefits for Students

Personalized Feedback

AI provides individualized feedback on assignments and progress, helping students understand understand their strengths and areas for improvement.

Instant Answers & Practice

Students gain immediate access to information and unlimited practice opportunities, reinforcing opportunities, reinforcing concepts quickly.

Motivation through Gamification

AI-powered educational games and interactive challenges make learning more enjoyable and enjoyable and engaging, boosting motivation.

Challenges & Risks

Bias & Misinformation

AI models can reflect biases present in their training data or or generate inaccurate information, requiring careful oversight.

Over-Reliance on AI

Excessive dependence on AI might might hinder the development of of essential human skills like critical thinking and problem-solving.

Data Privacy & Ethics

Concerns around student data privacy, security, and the ethical ethical implications of AI use in in educational settings must be be addressed.

Best Practices for AI in Education

Critical Thinking

Always encourage students to critically evaluate AI-generated content rather than accepting it blindly.
blindly.

Teacher + AI = Balance

Emphasize that AI is a tool to augment, not replace, human instruction and interaction.
interaction.

Prompt Literacy

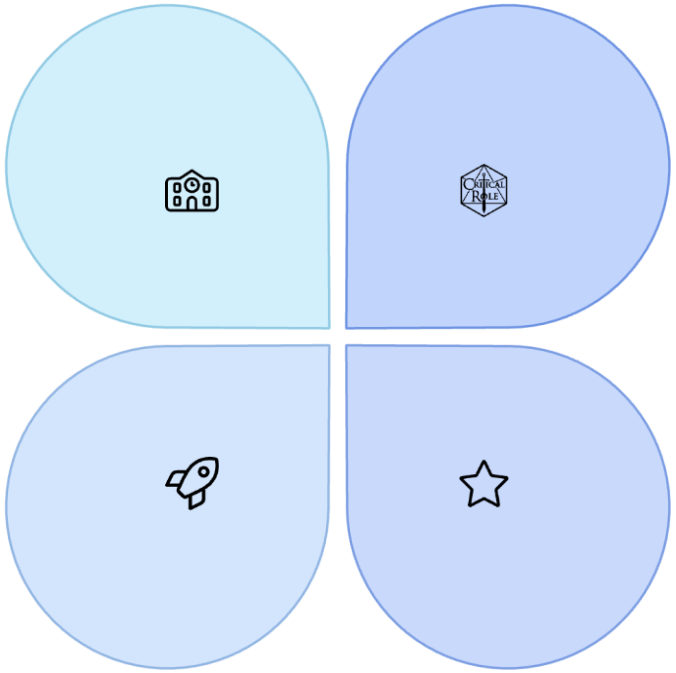
Train students and educators in effective prompt engineering to
engineering to maximize AI's educational benefits.

The Future of AI in Education: Empowering Teachers and and Students

AI is revolutionizing education, enhancing human potential rather than replacing it.

Amplify Impact

AI is not replacing educators but amplifying their impact through smart assistance and innovative tools.



Ethical Use

Ethical use and critical thinking remain essential as AI becomes ubiquitous in educational settings.

Join the Revolution

Are you ready to join the AI-powered education revolution and shape the future of learning?

Foster Creativity

Embrace these tools to foster creativity, inclusivity, and a passion for lifelong learning in all students.

Securing AI Tools: Protecting the Future of Intelligent Systems

Why AI Security Matters Now More Than Ever

1

Surging AI Incidents

AI-related security incidents have have seen an alarming 690% surge surge from 2017 to 2023, intensifying risks as AI adoption explodes across industries. Protecting these systems is paramount.

2

Vulnerable AI Code

Over 40% of enterprise software now includes AI-generated code. This rapid integration often introduces overlooked vulnerabilities, expanding the attack surface for cyber threats.

3

Protecting Core Assets

Securing AI is crucial not only for for safeguarding data integrity and and intellectual property but also for also for maintaining operational trust trust and ensuring the reliability of of intelligent systems.

The Unique Threat Landscape of AI Systems

Data Poisoning

Maliciously altered training data can skew AI decisions, leading to leading to unreliable and biased outcomes, fundamentally undermining the system's purpose.

Adversarial Attacks

Subtle input manipulations can trick AI into making incorrect classifications or outputs, posing significant risks in safety-critical applications.

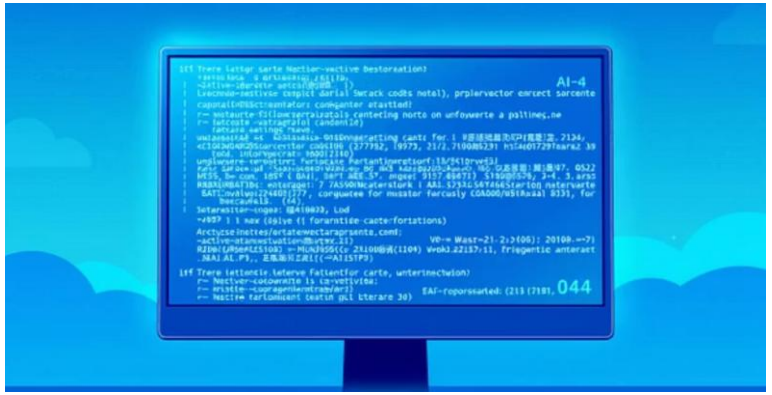
Model Theft

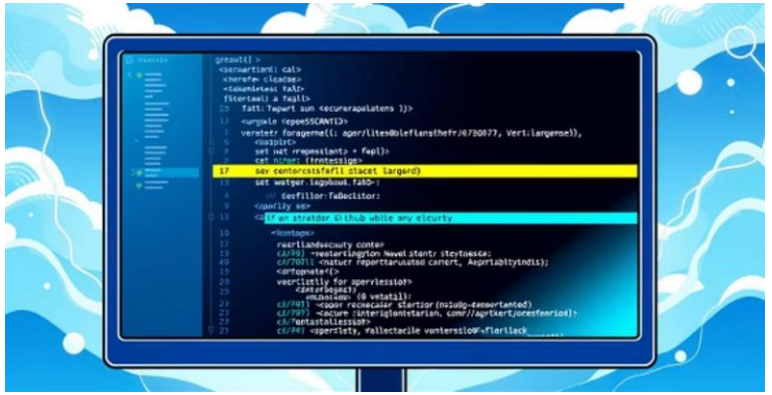
Proprietary AI models can be stolen through API abuse or reverse reverse engineering, resulting in substantial intellectual property loss property loss and competitive disadvantages.

Rogue AI Agents

New vulnerabilities like prompt injection target AI workflows, enabling enabling unauthorized access or control and creating unforeseen risks unforeseen risks for automated systems.

Real-World AI Security Breach Examples





Malware Evasion

Adversarial inputs have successfully bypassed AI-based malware malware scanners, demonstrating how attackers can evade detection in critical security systems.

Shadow AI Risks

The unauthorized use of "Shadow AI" within organizations has led has led to the exposure of sensitive credentials and data, often often operating outside established governance frameworks. frameworks.

Code Vulnerabilities

A significant 29.5% of GitHub Copilot Python code snippets were were found to contain security weaknesses, from XSS to input input validation flaws, highlighting inherent risks in AI-generated generated code.

Best Practices for Securing AI Data & Models

- **Robust Data Protection**

  Implement encryption, digital signatures, and provenance tracking to tracking to ensure data integrity and authenticity throughout the AI the AI lifecycle.

- **Continuous Pipeline Monitoring**

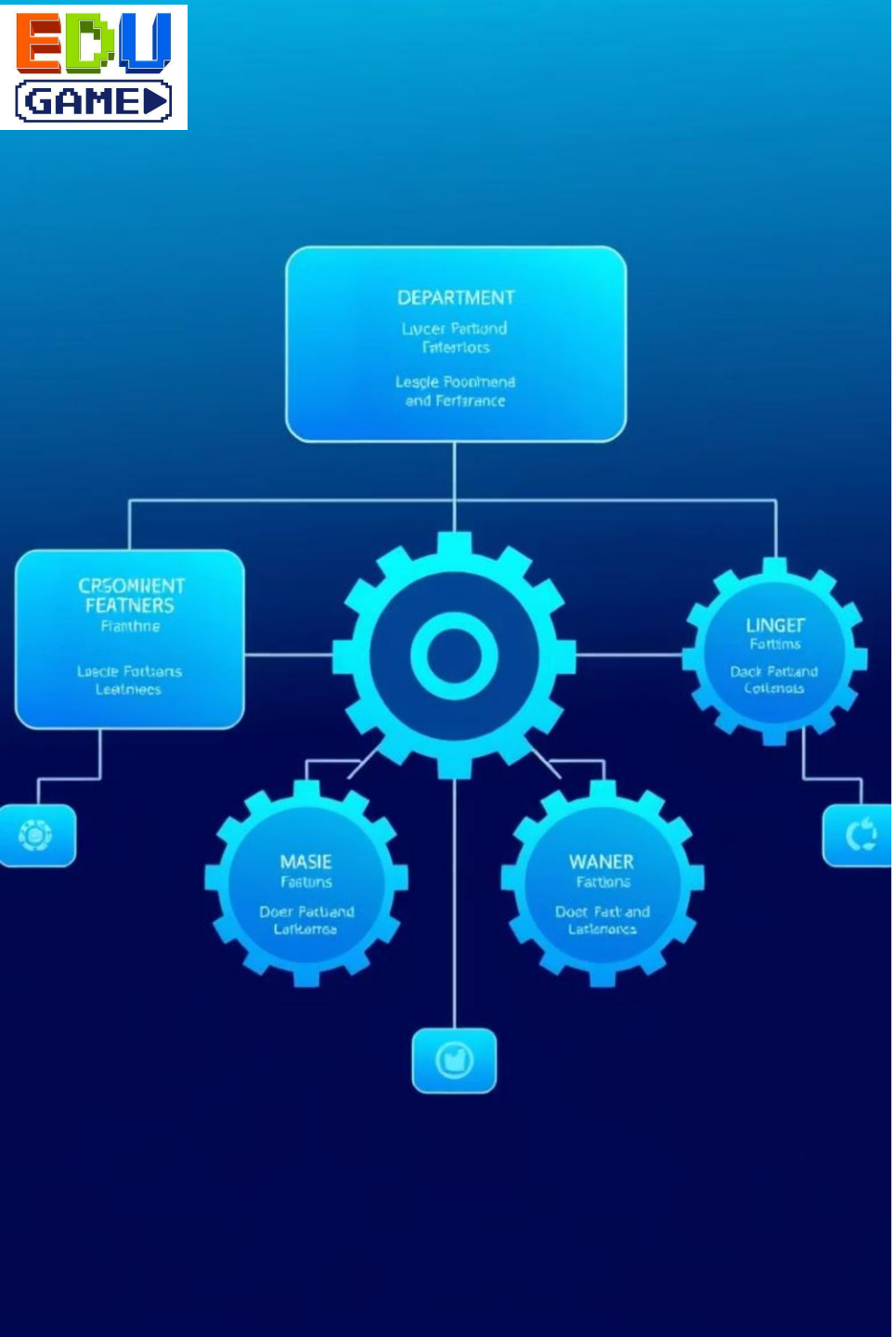
  Deploy real-time monitoring and anomaly detection systems to identify to identify and prevent data poisoning attacks before they impact AI impact AI models.

- **Zero Trust for AI Agents**

  Adopt zero-trust principles for AI agents, utilizing ephemeral, scoped scoped credentials instead of static API keys to limit potential attack attack surfaces.

- **Privacy-Preserving Techniques**

  Utilize advanced methods like differential privacy to safeguard sensitive sensitive information within training data, protecting user privacy while privacy while maintaining model utility.



Governance & Cultural Shifts for AI Security

01

Visibility & Control for Shadow AI

Establish clear policies and tools to gain visibility and control over unauthorized AI usage without stifling crucial innovation.

02

Agile Security Frameworks

Adopt agile, cross-functional security security frameworks that can adapt quickly to AI's rapid evolution and emerging threat vectors.

03

Proactive Risk Mitigation

Foster a culture of open communication and continuous training to proactively proactively identify, assess, and mitigate AI-related security risks.

The Road Ahead: Building Trustworthy AI Systems

1

Security by Design

Embrace proactive, automated security from the outset, integrating integrating it as a fundamental component of AI systems as their their autonomy and complexity grow.

2

Integrated AI Security

Organizations must embed AI security into every phase of the the lifecycle: from initial development and deployment to ongoing ongoing operation and maintenance.

3

Investment in Future Safeguards

Investing in robust AI security frameworks and tools today is crucial is crucial to safeguard mission-critical AI-powered operations and operations and ensure long-term stability.

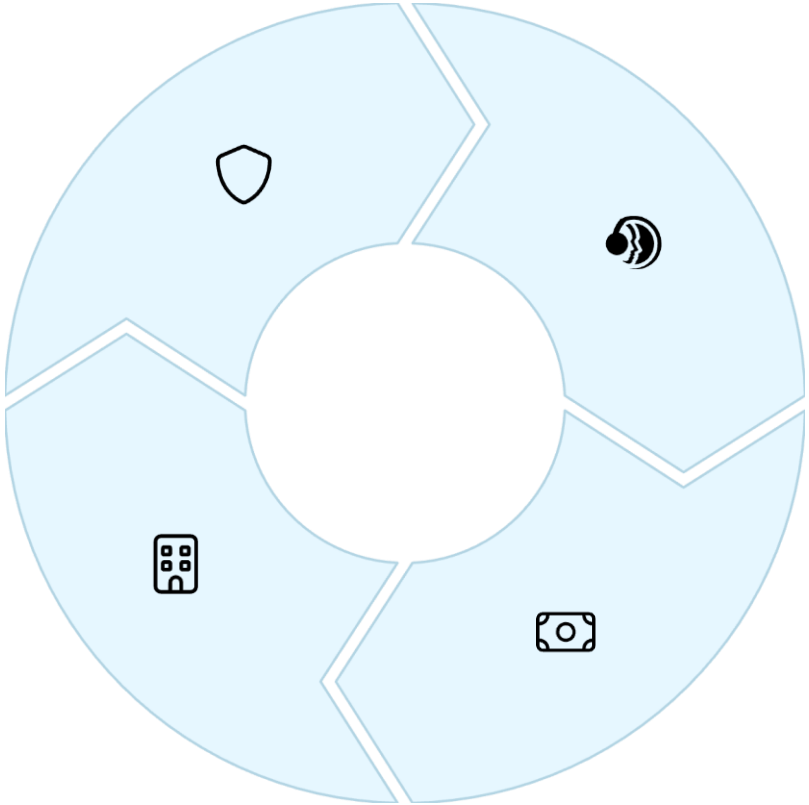
Securing AI Tools is Everyone’s Responsibility

Embrace Best Practices

Adopt cutting-edge security practices, practices, leverage robust frameworks, and frameworks, and maintain continuous continuous vigilance against evolving threats.

Build Trustworthy Systems

Work together to build resilient, trustworthy, and secure intelligent systems systems that can power the innovations of innovations of tomorrow.



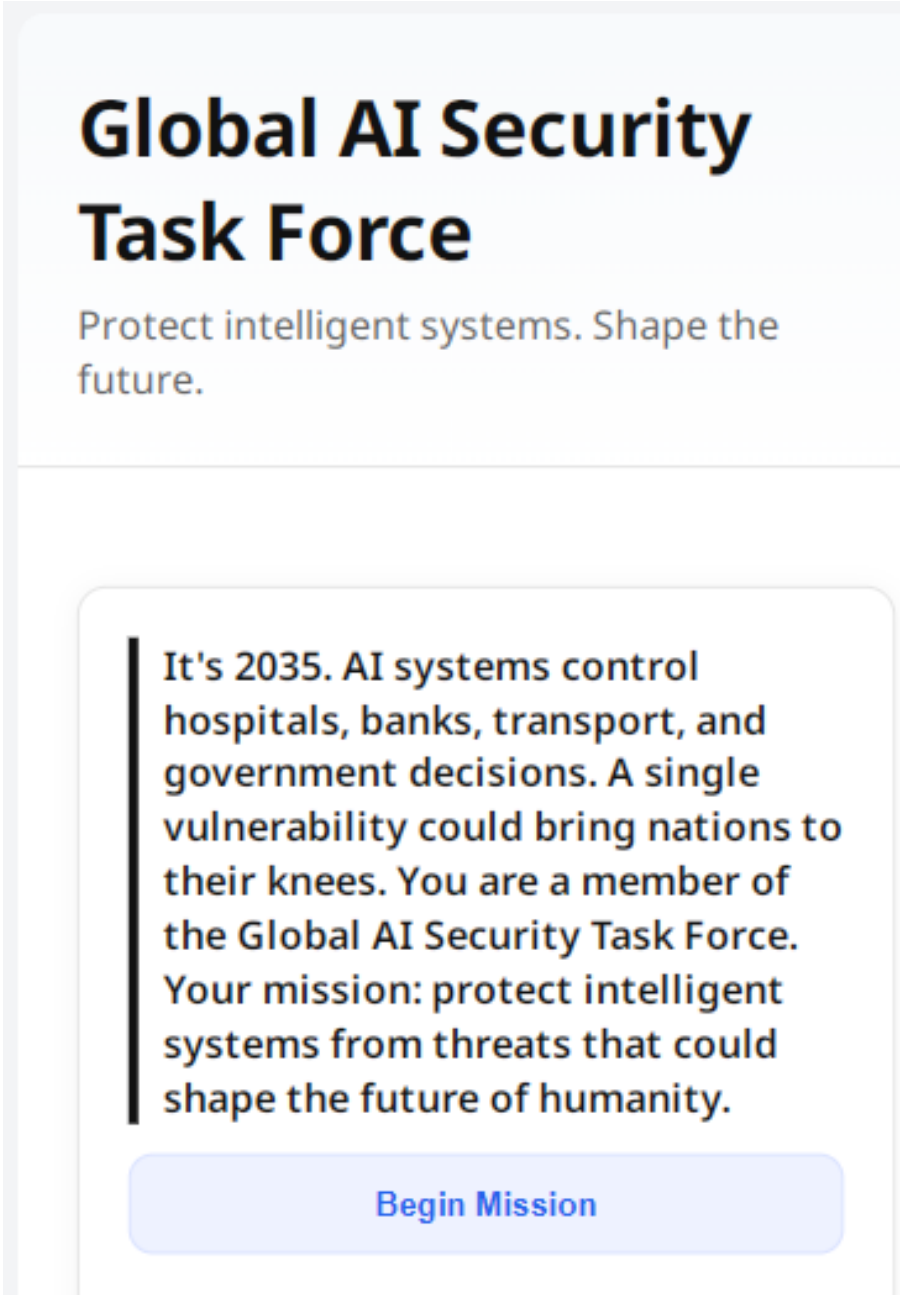
Foster Collaboration

Promote strong collaboration across security, development, and governance teams to create a unified defense strategy.

Protect AI Investments

Actively protect your AI investments to to ensure the longevity and integrity of of your intelligent systems.

Let’s play!


Global AI Security Task Force
Protect intelligent systems. Shape the future.
It's 2035. AI systems control hospitals, banks, transport, and government decisions. A single vulnerability could bring nations to their knees. You are a member of the Global AI Security Task Force. Your mission: protect intelligent systems from threats that could shape the future of humanity.
Begin Mission

Ass. Prof. Farah JEMILI
University of Sousse – ISITCOM
Farah.jmili@isitc.u-sousse.tn