Vision Coders

CONCEPT PROJECTS FOR INHERITANCE

Vision Coders

INTRODUCTION TO THE TEAM

Yash Deshmukh - 241070018 (SY BTech CE)
Vivek Kamath - 241070033 (SY BTech CE)
Shreyansh Modijira - 241070045 (SY BTech CE)
Paarth Maharshi - 241070050 (SY BTech CE)

Vision Coders

PROJECT 1

Vision Coders

SMART AI ASSISTANT

DOMAIN: ARTIFICIAL INTELLIGENCE

An intelligent virtual assistant that interacts with users through voice and text commands.

WHAT IS SMART AI ASSISTANT?

The Smart AI Assistant is an intelligent virtual assistant designed to understand and execute user commands through voice and text interaction. It aims to simplify daily computer tasks by automating actions such as opening applications, performing web searches, and providing information.

Example: Imagine a gamer in important online match and gets a call

In short, our Smart AI Assistant acts as a personal digital helper that enhances user productivity, reduces manual effort, and offers an intelligent, hands-free computing experience.

FEATURES

Intelligent Intent Recognition

Uses NLP to understand complex, natural language, not just fixed commands.

Contextual Awareness

Remembers past actions and current environment to handle multi-step, sophisticated requests.

Cross-Application Automation

Executes tasks that bridge multiple programs (e.g., launching an app, retrieving data, and sending a message).

Seamless Voice Interaction

Provides hands-free control via accurate speech recognition and natural text-to-speech responses.

Task Automation

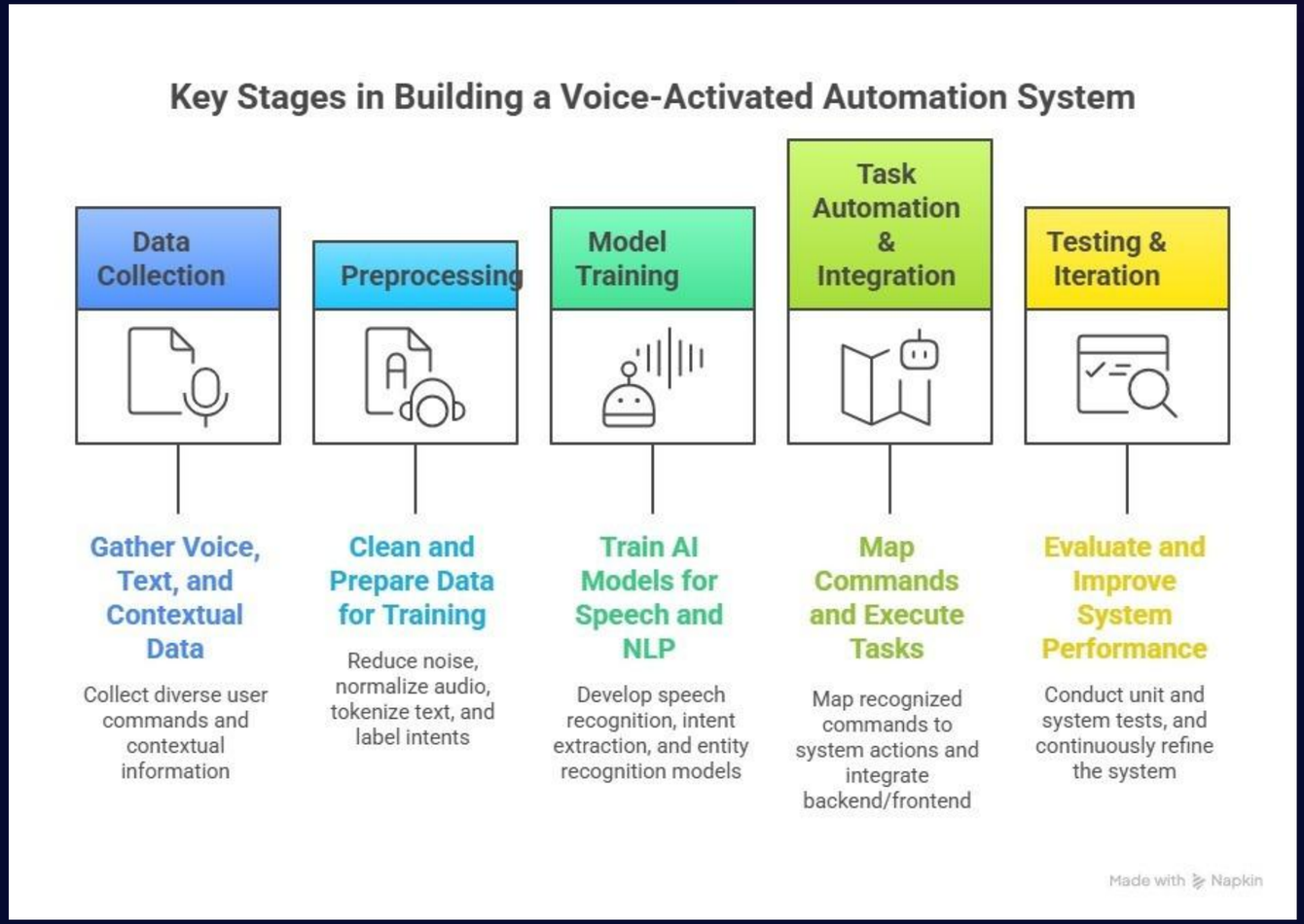
Simplifies daily routines by automatically opening apps, performing web searches, and managing scheduling.

Machine Learning (ML)

Learns user habits and preferences over time for continuous, personalized improvement.

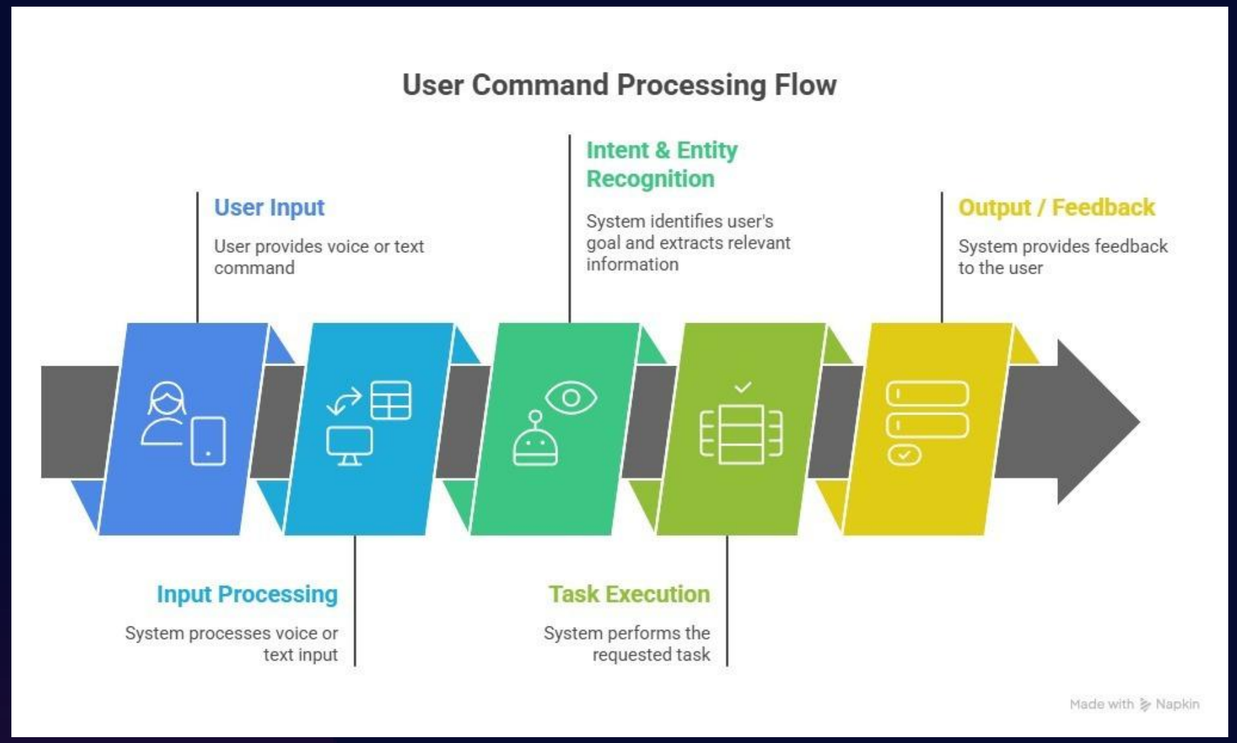
Vision Coders

APPROACH / METHODOLOGY FOR IMPLEMENTING SMART AI ASSISTANT



Vision Coders

FEATURES & HOW THEY WORK +



01

Voice & Text Commands

- How it works: Accepts user input through microphone or text box.
- Technology: Python (speech_recognition), HTML, CSS, JavaScript.

02

Understanding User Intent

- How it works: Uses NLP to analyze input and determine user's request.
- Technology: spaCy, NLTK, ML models (SVM, BERT).

03

Remembering Context

- How it works: Stores frequently used commands and preferences for smarter responses.
- Technology: JSON files or SQLite database.

04

Task Automation

- How it works: Executes tasks such as opening apps, searching the web, or sending messages.
- Technology: Python modules – os, webbrowser, pyautogui.

Vision Coders

FEATURES & HOW THEY WORK +

05

Cross-App Tasks

- How it works: Performs multi-step operations across different apps (e.g., Excel → Email).
- Technology: pyautogui, smtplib.

06

Voice Responses

- How it works: Gives spoken feedback for a hands-free experience.
- Technology: pyttsx3, gTTS.

07

Personalization

- How it works: Learns user habits to improve suggestions and performance.
- Technology: ML models – SVM, Random Forest, LSTM, BERT.

08

Real-Time Execution

- How it works: Handles commands instantly with parallel processing.
- Technology: Python threading, asyncio.

09

User Interface

- How it works: Interactive frontend for commands; backend executes logic.
- Technology: Frontend – HTML/CSS/JS | Backend – Python Flask.

10

Internet & Knowledge Access

- How it works: Retrieves real-time data and answers from the web.
- Technology: APIs (Wikipedia, WolframAlpha), requests, BeautifulSoup.

Vision Coders

RESEACH FOR SMART AI ASSISTANT

Study of Existing Systems

- Analyzed Google Assistant, Siri, and Mycroft.
- Found most rely on internet connectivity with limited offline customization.
- Identified potential for a lightweight, context-aware, semi-offline assistant.

NLP & Voice Technology Research

- **Explored NLP tools: spaCy, NLTK, BERT for intent detection.**
- **Studied speech recognition: speech_recognition, Vosk, Google Speech API.**
- **Reviewed text-to-speech: pyttsx3, gTTS for natural responses.**

Dataset Exploration

- **Examined LibriSpeech, Common Voice, and Snips datasets.**
- **Planned to build a custom dataset tailored to assistant use cases.**

Dataset Exploration

- **Existing systems are data-heavy and cloud-dependent.**
- **There is scope for a privacy-friendly, offline-capable assistant that ensures balance between performance and automation.**

CONCLUSION

The Smart AI Assistant project aims to revolutionize daily computer interactions, making them seamless and intuitive. We understand the challenge of juggling multiple tasks and the constant demand for efficiency in a fast-paced digital world. Therefore, we are developing a personalized, voice-activated assistant to simplify your digital life, freeing you from repetitive manual efforts.

Through the sophisticated use of Artificial Intelligence and Natural Language Processing, the Smart AI Assistant will provide instant task automation. Whether you are managing your schedule, sending quick messages while busy, or simply seeking information, our assistant will be there to empower you.

The Smart AI Assistant will continuously learn from your commands and preferences, adapting to your evolving needs. Our objective is to empower you to make informed decisions, enhance your productivity, and enjoy a truly intelligent, hands-free computing experience.

Vision Coders

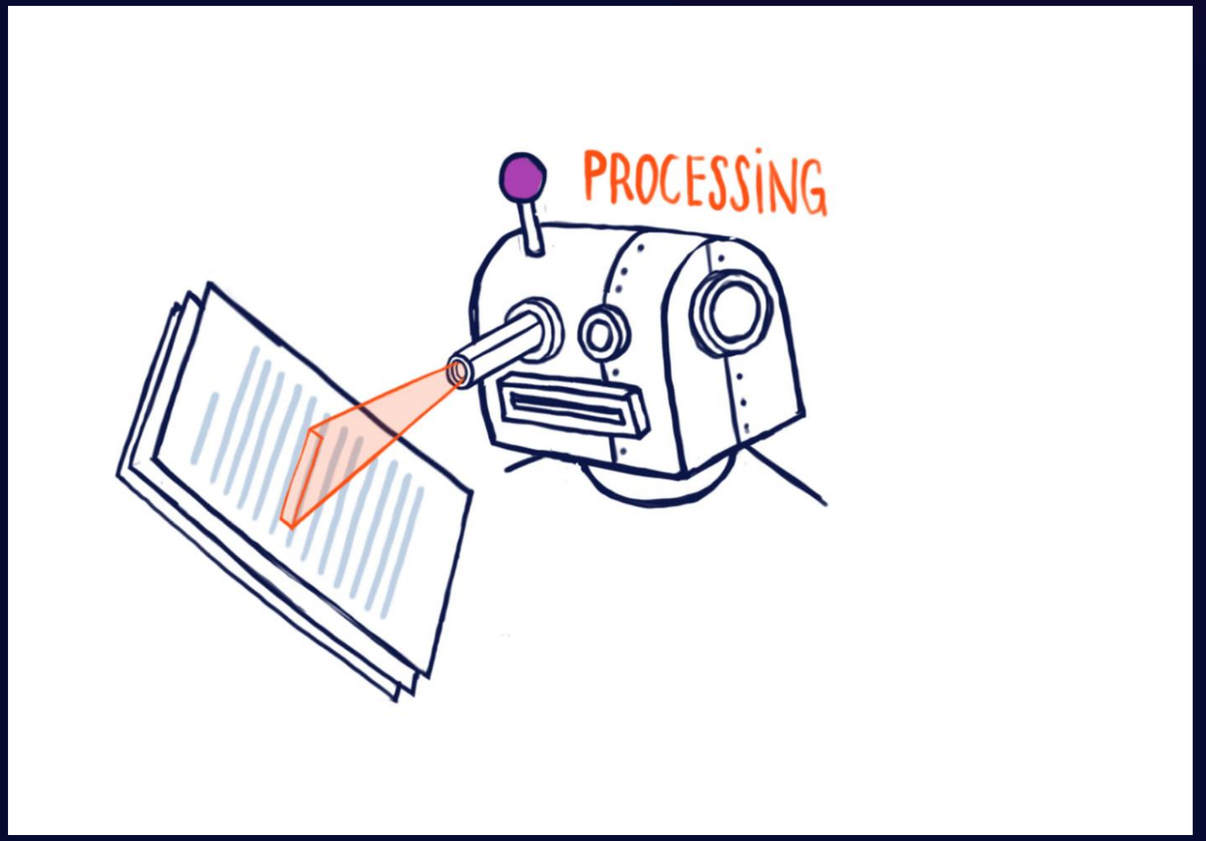
PROJECT 2

Vision Coders

AI TEXT DETECTOR

DOMAIN: ARTIFICIAL INTELLIGENCE & CYBERSECURITY

An AI-based system designed to detect whether a given text is written by a human or generated by an AI model.



Vision Coders

RISE OF AI-WRITTEN CONTENT CHALLENGES CONTENT AUTHENTICITY.

- AI-generated content is rapidly increasing across the internet.
- It’s becoming hard to distinguish between human-written and AI-written text.
- This creates issues in academics, journalism, and online authenticity.
- There is a need for a reliable detection tool to ensure content originality and trust.

AI: A force for social empowerment

India is committed to using AI for common good, while addressing privacy, ethical concerns

AI will replace certain existing job roles but also create several new job profiles. The world needs to manage this transition effectively so that it does not aggravate societal disparities SHUTTERSTOCK

Ravi Shankar Prasad

The success of Digital India has set a new global benchmark for leveraging digital technologies for inclusive growth, good governance and empowerment. The benefits of digital technologies have now become accessible for everyone. Rapidly-changing technology requires continuous evolution of systems, faster regulatory responses and building capacities. The advent of Artificial Intelligence (AI) is not just an incremental change, but a paradigm shift which must be harnessed for humanity's well-being.

Data is the basic building block for any AI system. India, with over 700 million internet subscribers, 1.21 billion phone-users and 1.26 billion Aadhaar users generates massive amounts of data daily. It has the largest user-base for some of the major global internet companies; it also offers the most affordable internet services in the world; and the information technology (IT) sector ensures the availability of competent human resources. These, coupled with the leadership of Prime Minister (PM) Narendra Modi, a champion of technology as a way to improve people's lives, puts India at the cusp of the AI revolution.

In 2018, the National AI Strategy was published by the government. Since then, there have been several initiatives to develop a strong AI ecosystem. The Centre of Excellence in Data Analytics (CEDA) has been established to provide expert data analytics services to government departments. In collaboration with the IT industry, Centres of Excellence have been set up in Bengaluru, Gandhinagar, Gurugram and Visakhapatnam where, so far, 113 start-ups have been incubated, 29 Intellectual Properties have been generated, and 56 sectoral solutions have been developed. The Future Skills Prime online capacity-building platform has been launched to skill and reskill professionals in emerging technologies and in new job roles.

The National AI Portal has been launched as a one-stop digital platform for collaboration and knowledge-sharing in AI. Soon, the ministry of electronics and IT (MEITY) will launch the National Programme on AI.

Learning from public digital platforms such as Aadhaar, Unified Payments Interface, Goods and Services Tax Network and Government e-Marketplace, the government has decided to encourage the setting up of several public digital platforms in health, agriculture, education, logistics and language translations. With the announcement of the National Digital Health Mission, work on a public digital platform for health has begun. MEITY is developing an AI-based Natural Language Translation Mission in collaboration with academic institutions, research institutions, industry and start-ups which will pave the way for a voice-enabled internet in Indian languages. Several ministries in collaboration with industry, academia and start-ups are in different stages of finalising sectoral public digital platforms. These will offer AI-based services while addressing the data security and privacy concerns of users.

Developments in technology also raise concerns. When large-scale computerisation was undertaken, there were concerns about mass unemployment. But eventually, computers and IT became one of the biggest job creators. In the same way, AI will replace certain existing job roles but also create several new job profiles. The world needs to manage this transition effectively so that it does not aggravate societal disparities. Through initiatives such as Future Skills Prime, India has already started work on reskilling its workforce for future job roles in IT. India's approach towards responsible AI for social empowerment seeks to leverage AI for inclusive growth and empowerment while addressing concerns over exclusion and job redundancy. The vision to use AI in health care, agriculture, education, logistics and languages is inspired by our commitment to leverage AI for social empowerment.

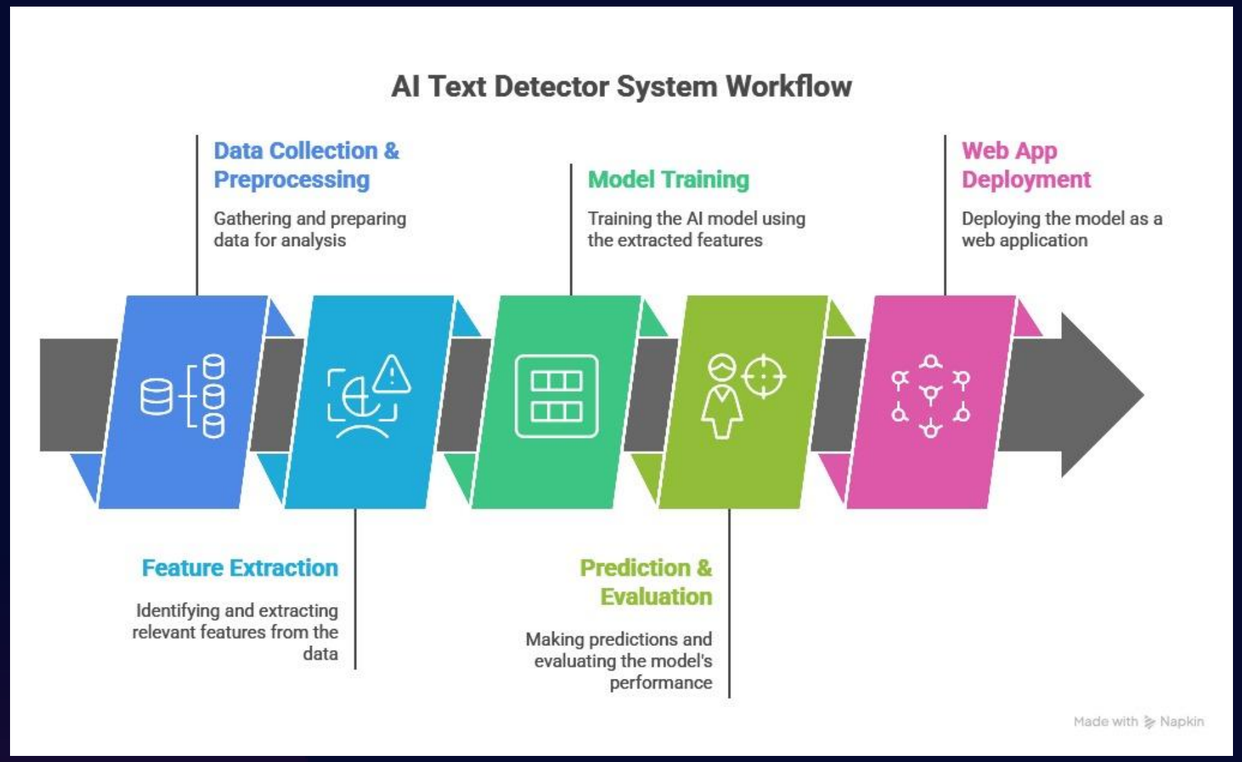
Data resources are going to play a vital role in AI's development, but concerns regarding the misuse of data and breach of privacy of users must be addressed by AI systems. The government has already introduced a robust Personal Data Protection Bill in Parliament, which seeks to protect the privacy of users in the digital age while facilitating the development of a strong data economy. Any attempt to create a monopoly in the digital space by misusing the data of citizens will invite a strong response from the government. The action taken against certain mobile apps recently clearly indicates that the Modi government is committed to protect the data privacy of Indian citizens and India's data sovereignty.

AI also generates other ethical and legal concerns that must be addressed. Algorithms that define the set of rules to operate AI systems must be free of any biases and prejudices. For example, face recognition systems must not display any racial or ethnic biases and news and social media systems must not be biased towards any particular political ideology. Conventional laws based on the basic premise of jurisdictions are being challenged by transnational technologies. Rogue elements situated in any part of the world can disrupt peace in other societies. We saw this in the recent Citizenship (Amendment) Act agitations and the Delhi riots. The world needs to collectively address these concerns.

India is one of the founding-members of the Global Partnership on Artificial Intelligence — a multilateral collective to develop responsible AI, and is also working with several countries bilaterally to develop AI ecosystems. India's biggest AI summit RAISE 2020, which begins on Monday, seeks global collaboration for the development of an AI ecosystem that is responsible towards humanity and committed to social empowerment.

Ravi Shankar Prasad is Union minister for electronics and information technology, communications and law & justice
The views expressed are personal

WORKFLOW



01

Data Collection & Preprocessing

- Gather AI-generated and human-written text datasets.
- Clean and tokenize text for model training.

02

Feature Extraction

- Apply TF-IDF or word embeddings to convert text into numerical form.

03

Model Training

- Train ML models (e.g., Logistic Regression, BERT) on labeled data.

04

Prediction & Evaluation

- Predict class (AI/Human) for new text.
- Evaluate using accuracy, precision, recall, and F1-score.

Vision Coders

RESEARCH FOR AI TEXT DETECTOR

Study of Existing Systems

- Analyzed tools like OpenAI AI Classifier and GPTZero.
- Found challenges in detecting short texts and AI content that mimics human writing.

Dataset Analysis

- Used public AI-generated and human-written datasets.
- Planned to make a balanced dataset for training, validation, and testing.

NLP & Feature Extraction

- Explored TF-IDF, Word2Vec, GloVe, and Transformer embeddings (BERT, RoBERTa).
- Aim: Capture semantic and stylistic differences between human and AI text.

Evaluation Metrics

- Metrics: Accuracy, Precision, Recall, F1-score, ROC-AUC, Confusion Matrix.

ML & DL Models

- Classical models: Logistic Regression, Random Forest, SVM.
- Deep learning: LSTM, GRU, and BERT for text classification.

Key Findings

- Combining classical features with transformer embeddings yields high accuracy.
- A robust approach for authenticity verification of digital text.

Vision Coders

EXPECTED OUTCOME

Accurate classification of AI vs. human text.

Supports content verification for educators, journalists, and platforms.

Improves transparency in digital communication.

Future Scope:

- Identify which AI model (GPT-3, GPT-4, etc.) wrote the text.
- Integrate as browser extension or API for real-time detection.

Vision Coders

PROJECT 3

Vision Coders

PHISHGUARD

DOMAIN: ARTIFICIAL INTELLIGENCE & CYBERSECURITY

An AI-powered phishing detection system designed to protect users from malicious emails and fraudulent websites.

WHY WE CHOSE THIS

In the modern digital era, cyber threats are becoming increasingly sophisticated, putting individuals and organizations at constant risk. Among these threats, phishing emails and malicious websites are some of the most common methods used by attackers to steal sensitive information, such as login credentials, banking details, and personal data.

PhishGuard is an intelligent system developed to combat these threats by using Artificial Intelligence (AI) and machine learning techniques. The system analyzes URLs and emails to detect patterns, anomalies, and risk indicators associated with phishing attempts. By identifying potentially harmful content before users interact with it, PhishGuard enhances cybersecurity awareness, helps prevent data breaches, and provides a safer online experience for everyone.

Crime thrives online, little action on ground

LOW CONVICTIONS Experts blame lack of manpower, poor training

Vijay Kumar Yadav & Jayprakash S Naidu

MUMBAI: The state government in April this year, approved the setting up of four new police stations dedicated to tackling the rising cases of cyber crime in Mumbai. It also sanctioned creating 186 new posts, most of them to be filled by assistant police inspectors.

These units are yet to start work, but meanwhile, cases of cyber crime—which range from data theft to credit and debit card frauds and vishing—have steadily risen over the past three years. Convictions, however, have remained disproportionately low. According to the National Crime Records Bureau's (NCRB) 2016 report on crime, Mumbai ranked first in the country for cyber crime cases. From 2015, up until May 2018, 10,275 cyber crime cases were filed in Maharashtra. While 3,689 of these were solved by the police, just 93 of these cases went to trial. In all, since 2015, there have been convictions only in 28 cases.

"The detection (solving) rate depends on several factors," said Balsing Rajput, the superintendent of police (cyber).

"It is difficult to extract information in cyber crime cases. There are many agencies involved, such as the internet service provider, the ones who provide media content online, intermediaries like the banks and technology service providers. There is also the issue of international jurisdictions."

Rajput pointed out how in many cases, the fraudsters use SIM cards that they got after providing false information.

"The bank accounts of an illiterate person is used, after these fraudsters promise them a commission.".

Former Maharashtra director general of police and cyber crime expert, D Sivanandhan, said one of the main reasons for low detection and conviction rates was the lack of manpower and poorly trained police officers.

CONTINUED ON P10
RELATED REPORTS, P2

CASES RISE, CONVICTIONS FALL

4,035 Cyber crime cases registered in 2017, nearly double the number of cases (2,195) since 2015

16.6% Was the conviction rate in 2017, down from 40.7% in 2015

12 Cases went to trial and were concluded in 2017, much lower than 2015's 54 cases

0 Convictions in 2018, despite all 10 registered cases going to trial, (ended in acquittals)

25.7 was the detection rate (an avg of cases solved) in 2017, down from 35.3 in 2015.

	Cases	Detection	Trials completed	Convictions
2015	777	2,195	54	22
2016	791	2,380	17	4
2017	1,001	4,035	12	2
2018 May	445	1,665	10	0

(Source : Maharashtra Police)

Crime thrives...

"Further, the law permits only officers from the rank of police inspectors and above to register and investigate the cyber crimes," he said, and added that the since cyber criminals operate online, many times from another state, it becomes difficult for the police to arrest them. "For this, we need a good inter-state and international network of officers, and improved coordination among investigative agencies."

At the trial stage, prosecutors and the judges also need to be updated about the growing incidents cyber crimes and the technology that is being used to cheat people. "This may help them better examine evidence, trials will be done faster, and conviction rates will improve. This is the missing link," Sivanandhan said. Special inspector general of police (cyber crime) Brijesh Singh also stressed on the need to better training and improved technology. "In the near future, we will have a centre for excellence where special training and information pertaining to cyber crimes and its investigations are provided to police, prosecutors and the judiciary. We will also have 44 cyber police units that have state-of-the-art technology."

Vision Coders

FEATURES

Phishing Detection

Accurately identifies phishing URLs and scam emails using AI and machine learning models.

Risk Scoring System

Assigns a risk score to each link or email to indicate the level of threat.

Explanations for Threats

Provides clear reasons why a URL or email is flagged, helping users understand potential risks.

User-Friendly Interface

Simple and intuitive web interface built with Flask, HTML, and CSS for easy input and result viewing.

Real-Time Analysis

Detects threats quickly, providing instant feedback to users before they interact with suspicious content.

Data-Driven Insights

Analyzes patterns in phishing attempts to improve detection accuracy over time.

Machine Learning Powered

Uses models like Random Forest, Logistic Regression, and Gradient Boosting for intelligent threat detection.

Safe Browsing Promotion

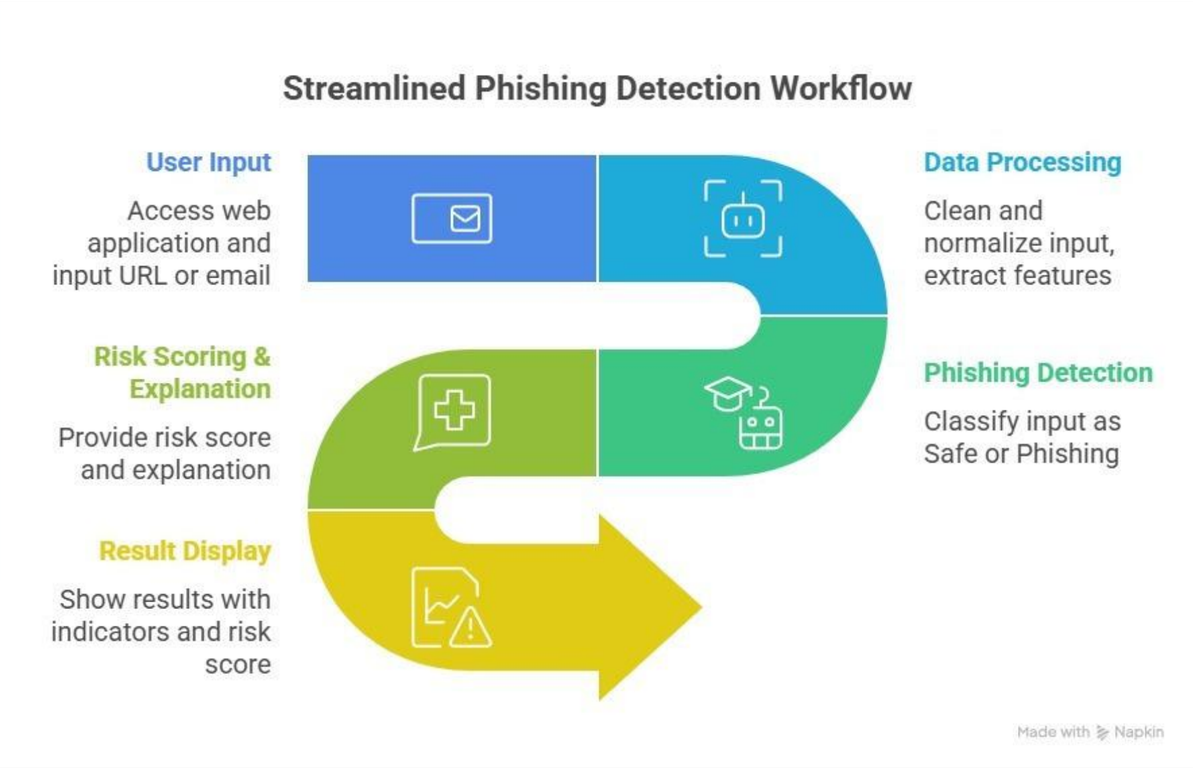
Educates users on cybersecurity best practices and increases awareness of online threats.

Vision Coders

APPROACH / METHODOLOGY FOR IMPLEMENTING PISHGUARD

Vision Coders

FEATURES & HOW THEY WORK +



01

Core Development Language

Python

- Extensive libraries for AI & ML development.
- Enables rapid prototyping and integration with ML frameworks.

02

Machine Learning Frameworks

Scikit-learn, TensorFlow, PyTorch

- Train and deploy models to detect phishing patterns in URLs and emails.
- Supports classification algorithms for accurate predictions.

03

Natural Language Processing (NLP) Libraries

NLTK, spaCy, BERT (optional)

- Analyze email and website text content.
- Understand context, extract features, and detect suspicious language.

04

Data Collection & Parsing

requests, BeautifulSoup

- Retrieve web pages and emails efficiently.
- Extract relevant content for feature engineering and model training.

05

Deployment / Web Frameworks

Flask / Django

- Provides a web interface for users to submit emails/URLs.
- Delivers real-time phishing detection results in an accessible format.

Vision Coders

RESEACH FOR PHISHGUARD

Study of Existing Systems

- Existing Tools: Traditional blacklist-based and rule-based systems, plus basic ML detectors.
- Problem: Fail to detect zero-day phishing attacks; cloud-dependent and slow.
- Focus: Develop a fast, real-time detector that works locally (e.g., browser extension).

AI Model & Data Research

- AI Models: Explored Ensemble Models and lightweight Deep Learning (e.g., MobileBERT).
- Features: Focused on URL structure, HTML code, and metadata to detect hidden threats.
- Goal: Achieve millisecond-level prediction for instant protection.

Dataset Exploration

- Sources: Public datasets (e.g., UCI Phishing Dataset).
- Preprocessing: Balanced data using techniques like SMOTE to avoid bias.
- Future Plan: Continuous updates with new phishing samples for evolving threats.

Key Findings

- Best Detection: Ensemble Models give superior accuracy for new phishing types.
- Ideal Design: A lightweight, real-time, and offline-capable system provides the most effective protection.

CONCLUSION

In a world demanding more digital trust, PhishGuard delivers. We've shown how our intelligent system, powered by advanced AI and Machine Learning, actively analyzes and anticipates threats, turning the tide against cyber adversaries. Our team is incredibly proud to contribute to a safer internet, offering a proactive defense that empowers both individuals and organizations. We are delighted to usher in an era where intelligence fights threat, fostering a more secure and trustworthy digital ecosystem for all.

WE APPRECIATE YOUR TIME!