TEAM NAME: **StatusC_301**

COLLEGE NAME: **Vidyalankar Institute Of Technology**

TEAM MEMBERS :
1. **Sahil Borhade (24101B2007)**
2. **Ved Thombre(23101A0009)**
3. **Vishant Gawali(23101B0002)**
4. **Keshav Verma (23101B0003)**

PROBLEM STATEMENT

What problem are we solving?

- Students and educational institutions are increasingly exposed to sophisticated phishing attacks that:
- Impersonate scholarship programs and internship portals
- Clone official university login pages
- Create fake hackathon or event registration links
- Trick users into submitting credentials and personal data
- These attacks are highly targeted and difficult to detect manually.

Why is this important?

- Protects student credentials and institutional data
- Reduces large-scale phishing campaigns targeting academia
- Strengthens national cybersecurity posture
- Enables proactive client-side threat prevention

Why Do Existing Systems Fail?

- Phishing domains closely resemble legitimate university domains
- Webpage content appears authentic and contextually correct
- Attackers personalize emails to bypass spam filters

Who Is Affected?

🎓 **Students**

- Targeted through fake scholarships, internships, and hackathon links
- Risk of credential theft (email, LMS, banking details)
- Financial fraud and identity misuse

PROPOSED SOLUTION

Brief Explanation

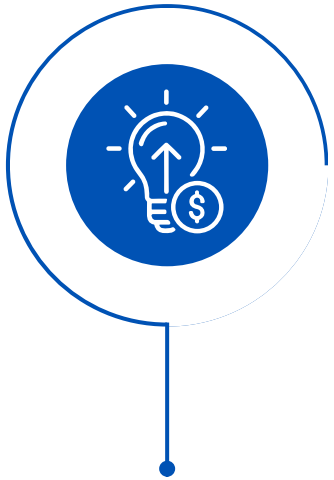
We propose an AI-powered browser extension that acts as a real-time phishing detection layer for students.

The extension:

- Monitors visited URLs in real time
- Extracts structural and lexical URL features
- Analyzes webpage content and login forms

Key Features

- Real-Time URL Analysis
- Machine Learning-Based Risk Scoring
- Webpage Content & DOM Inspection
- Instant Visual Warning Pop-up
- Suspicious Activity Logging



Solving the Problem

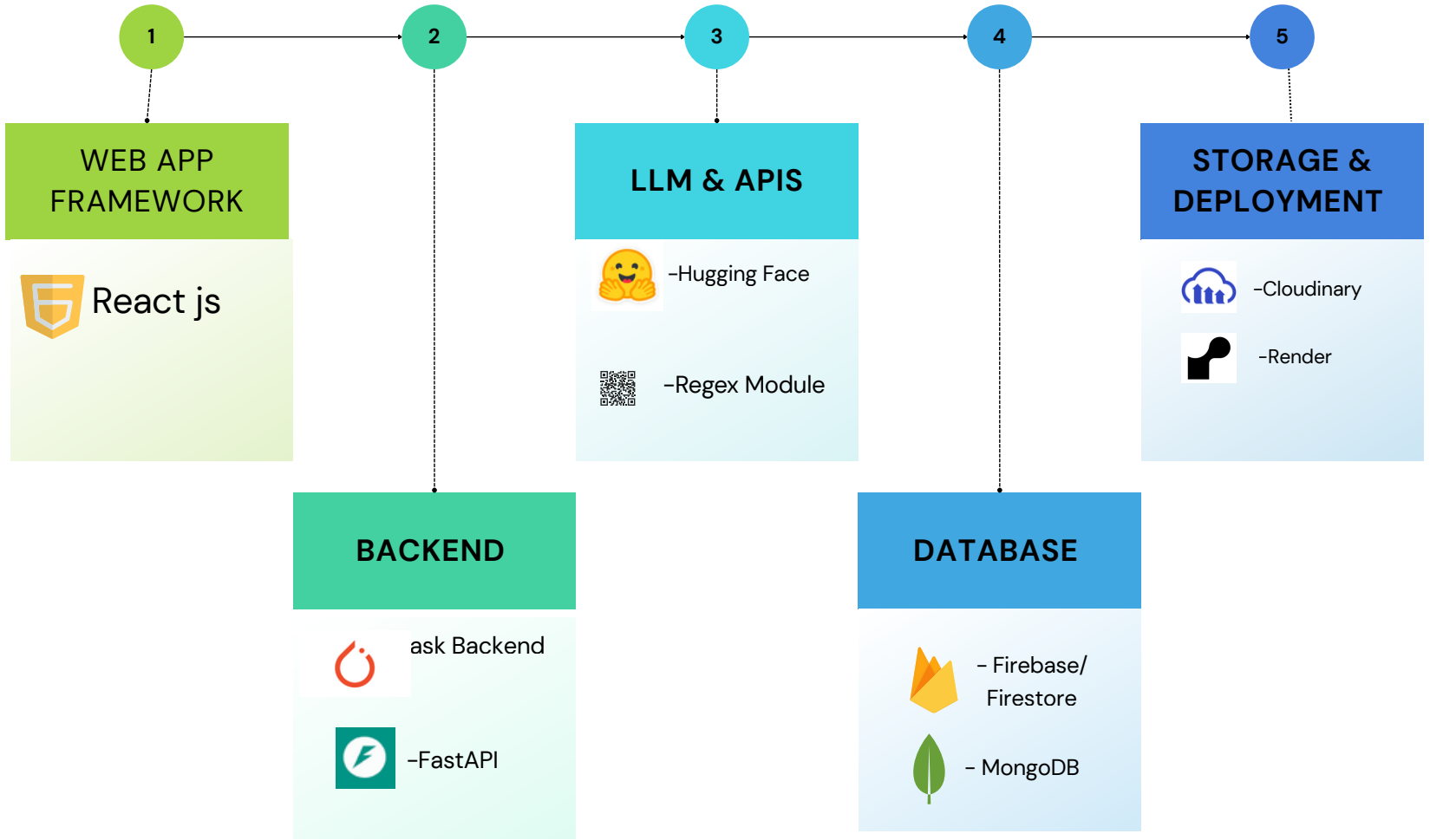
- Prevents credential theft before submission
- Detects cloned university portals
- Identifies malicious scholarship & internship links
- Reduces dependency on traditional spam filters
- Empowers students with proactive security

Innovation & Uniqueness

- Client-side AI detection (No heavy backend required)
- Hybrid detection model (Feature-based + Content-based)
- Risk probability scoring instead of binary classification
- Designed specifically for student phishing scenarios

TECHNICAL APPROACH

TechStack



IMPACT AND BENEFITS

Key Benefits

Security Impact

- **Prevents Credential Theft:** Detects phishing pages before students submit login details.
- **Reduces Financial Fraud:** Stops scams related to scholarships, internships, and exam registrations.
- **Minimizes Data Breaches:** Protects institutional email and portal accounts.

Technological Impact

- **Real-Time Client-Side Detection:** Immediate analysis without server delay.
- **AI-Based Risk Scoring:** Dynamic phishing probability instead of static blacklist checks.
- **Scalable Architecture:** Can be expanded to institutions nationwide.
- **Lightweight Deployment:** Simple browser extension, no complex infrastructure required.

Educational Impact

- **Student Awareness:** Educates users about phishing threats in real time.
- **Safer Digital Learning Environment:** Protects LMS, university portals, and academic platforms.
- **Confidence in Online Opportunities:** Students can safely explore scholarships and internships.

National Cybersecurity Impact

- **Supports CERT-In's Mission:** Strengthens proactive cyber threat detection.
- **Reduces Large-Scale Phishing Campaigns:** Early detection limits spread.
- **Improves Digital Trust in Academic Ecosystem.**

BUSINESS MODEL

Institutional Licensing

- Annual/site-wide licenses for educational institutions
- Volume discounts for district-wide or state-level implementations

Premium Upgrades

- Advanced Threat Analytics Dashboard
- Enhanced Logging & Reporting
- Priority Support (24/7)

Public Sector Support

- Grants and funding from government cybersecurity programs
- Strategic partnerships with CERT-In

Data & Intelligence

- Aggregate anonymized phishing data insights
- Offer research reports to improve national cybersecurity

Freemium Model

- Free basic version for individual students
- Premium features available through a subscription

Existing Solutions Comparison

Feature	KavachX	Enterprise DLP (e.g, Nightfall)	Banning AI
Cost	✔ Free / Low Cost	Very High ($$$)	✘ Free (but costly in productivity)
User Experience	✔ Seamless (In-Browser)	✘ Friction (Separate Apps)	✘ N/A (Cannot use AI)
Detection Type	✔ Hybrid (Regex + AI)	✘ Mostly Regex/Rules	✘ N/A
Privacy	✔ Local Processing	✘ Cloud Processing	✘ Maximum
Setup Time	✔ < 1 Minute	✘ Weeks of Integration	✘ Instant

Privacy	✔ Local Processing	✘ Cloud Processing	✘ Maximum
Setup Time	✔ < 1 Minute	✘ Weeks of Integration	✘ Instant