Department of Financial Services
Ministry of Finance
Government of India

PSBs Hackathon Series-2025

(An initiative of Government of India, Ministry of Finance, Department of Financial Services)

IDEA
INNOVATION | DEVELOPMENT | EXECUTION | ADVANCEMENT

SOMAIYA VIDYAVIHAR UNIVERSITY

Promoting Innovation and Fostering Collaboration

PRESENTED BY

यूनियन बैंक ऑफ इंडिया

Union Bank of India

In association with K J Somaiya School of Engineering, Vidyavihar, Mumbai

SOCH SE SACH TAK
Taking dreams of your journey to a defining reality

Problem Statement and Team Details

Team name (As submitted on portal)	weHaveTime
Domain (FinTech, Cybersecurity, GenAI)	Cybersecurity
Problem Statement Title	Need for Government Agencies Assistance for takedown of Malicious/Phishing domain

	Name	Area of Expertise
Member I (Team Leader)	Ritesh Jha	Cybersecurity
Member II	Dev Baliga	Web-Development
Member III	Shail Shaji	AI-ML
Member IV	Shayaan Amir	Web-Development
Name of College	KJ Somaiya College of Engineering, Vidyavihar	

IDEA TITLE - PhishNet

Proposed Solution (Describe your Idea/Solution/Prototype)

1) Detailed Explanation of the Proposed Solution & How It Addresses the Problem

This solution is a Unified Cybersecurity Framework anchored by a Centralized Takedown Platform. Imagine a system that uses AI, deep-learning models and web scraping tools to spot phishing domains the moment they appear. Cybersecurity experts like Arnav can report threats instantly through a dashboard that auto generates evidence and uses standardized templates to escalate complaints to registrars, hosting providers or CERTs. The platform tracks every takedown request in real time and pushes stubborn cases to higher authorities or diplomatic channels if registrars refuse to cooperate. It partners with global registrars to act faster and even blocks phishing sites in specific regions using geo-fencing. Suspicious domain ownership changes get flagged automatically through WHOIS monitoring while the legal module crafts jurisdiction specific notices to counter state protected threats.

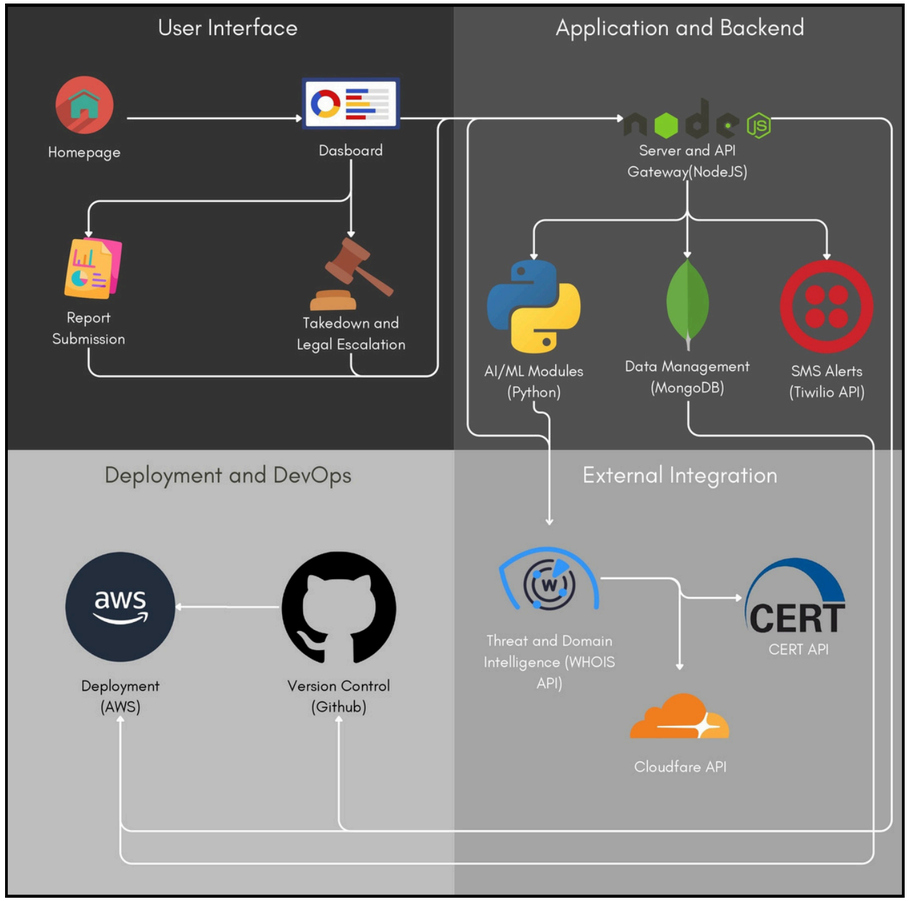
This solution directly addresses the problem by cutting through delays by automating detection and reporting while centralizing coordination to bypass bureaucracy. When registrars drag their feet the platform uses legal escalation and global alliances to force action. Real time tracking keeps everyone accountable and standardized workflows remove confusion. This means customers face fewer scams and public sector banks regain trust through swift transparent responses. This directly reduces customer exposure to scams and strengthens trust in PSBs.

2) Innovation and Uniqueness

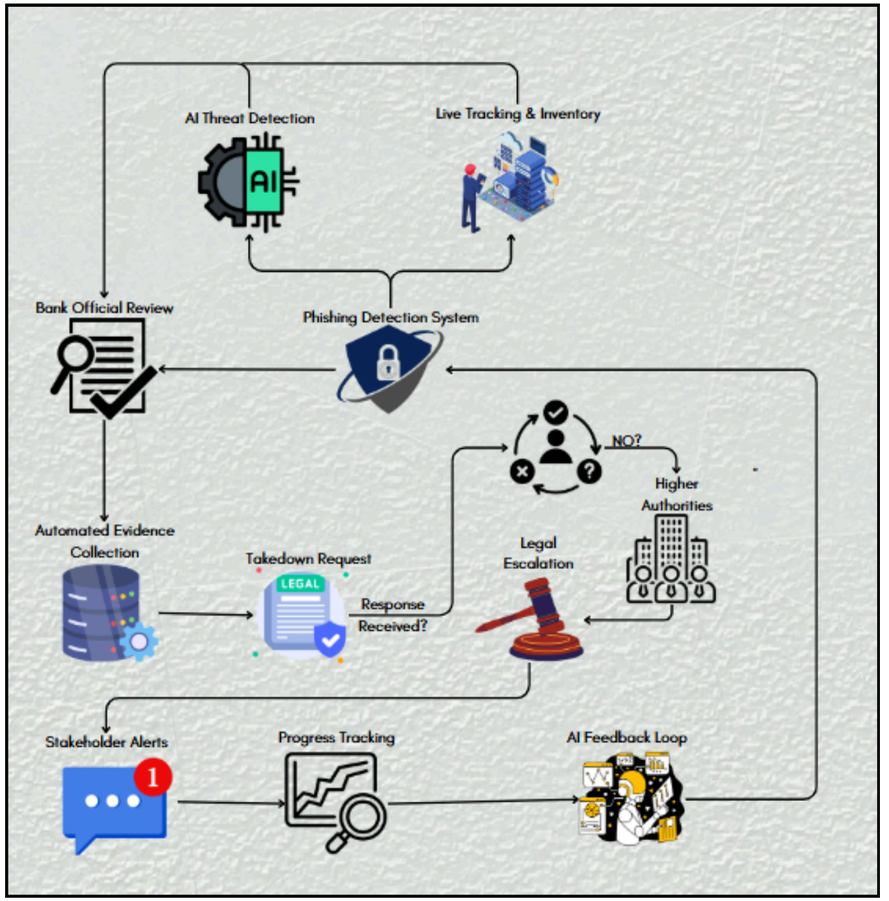
It combines cutting edge AI with diplomatic legal strategies which is unheard of in cybersecurity. The predictive engine stops phishing campaigns before they even launch while geo-fencing contains threats to specific areas. By merging detection, reporting and enforcement into a single platform it fixes both tech gaps and legal loopholes. Proactive features like WHOIS anomaly alerts and preemptive takedowns shift the focus from reacting to threats to stopping them early. Real time customer alerts keep users safe the moment a phishing attack is detected. This isn't just another tool, it's a strategic game changer built for the unique challenges faced by Indian PSBs. It turns fragmented efforts into a unified proactive shield against cybercrime.

TECHNICAL APPROACH

Technologies to be used



Methodology and process for implementation



FEASIBILITY AND VIABILITY

1) Analysis of the feasibility of the idea

This solution is highly feasible because it builds on existing technologies like AI driven threat detection and standardized legal frameworks already used in cybersecurity. Banks and CERT-In have access to threat intelligence feeds and diplomatic channels which can be integrated into the platform. Major registrars like GoDaddy or Cloudflare already collaborate with law enforcement, proving partnerships are possible. The modular design allows phased implementation, starting with automated detection and reporting before scaling to global registrars or legal escalation. Resource wise, India's push for digital sovereignty and cybersecurity startups provide talent and policy support. With PSBs facing rising phishing threats, the urgency to adopt such a system is clear, making funding and stakeholder buy-in achievable.

2) Potential challenges and risks

- Weak laws in some regions may delay takedowns.
- Old banking IT may not integrate with the platform's APIs.
- Too much AI reliance could flag legitimate domains.
- Cybercriminals may exploit fast changing domain registrations to stay ahead.
- Legal action might cause diplomatic friction.
- Keeping global registrar partnerships needs constant negotiation.
- GDPR and other privacy laws may hinder evidence sharing.
- Phishers may evade detection with decentralized hosting or blockchain domains.

3) Strategies for overcoming these challenges

Pre negotiate agreements with top registrars to fast track takedowns, backed by government mandates. Use lightweight APIs and open-source tools to ease legacy system integration. Pair AI with human oversight to validate threats and reduce errors. Build a legal advisory team to navigate cross border laws and avoid diplomatic clashes. Continuously update detection models to counter evolving tactics like blockchain domains. Launch a crowdsourced threat intelligence network with banks and CERTs to share data securely. For data privacy, anonymize customer information in reports. Finally, run pilot programs with cooperative registrars and PSBs to refine the platform before full scale rollout, ensuring adaptability and trust.

IMPACT AND BENEFITS

1) Potential impact on the target audience

Public sector banks and their customers will experience transformative change. Banks like Union Bank of India gain the power to swiftly neutralize phishing threats slashing customer data exposure from weeks to hours. Cybersecurity teams save critical time with automated detection and prebuilt legal templates letting them focus on strategic defense. Customers regain trust knowing their bank actively shields them from scams through real time SMS alerts and security guidance. Over time this reduces financial fraud losses and panic driven account closures. For citizens in rural or digitally naive communities it's a lifeline protecting hard earned savings from sophisticated scams. The platform's centralized coordination will break silos between banks and agencies like CERT-In enabling unified action against cross-border threats reducing phishing success rates the solution indirectly lowers interest rates and fees banks impose to offset fraud losses benefiting every citizen. Finally it creates a culture of cyber awareness where customers become vigilant partners in spotting threats accelerating India's journey toward a fraud resilient economy. PSBs evolve from vulnerable targets to proactive guardians of India's financial safety.

2) Benefits of the solution

Socially it empowers millions to bank online without fear. Economically PSBs save crores spent on fraud mitigation and legal battles while customers avoid crippling losses. Nationally it strengthens India's digital infrastructure against cross-border cybercrime. By unifying banks and regulators on one platform it fosters collaboration over competition. By automating evidence collection it reduces human error in legal processes ensuring higher conviction rates. The solution's predictive capabilities prevent scams before they spread reducing the need for reactive spending. Diplomatic escalations set precedents for global cyber enforcement challenging state-protected threat actors. Environmentally it cuts the carbon footprint linked to prolonged IT investigations. Most importantly it positions Indian PSBs as global cybersecurity pioneers inspiring safer digital ecosystems worldwide.

BUSINESS MODEL

1) Business Model overview

The business model revolves around a subscription based platform tailored for Union Bank of India and other PSBs. Revenue is generated through tiered subscriptions offering basic automated detection and reporting for smaller banks while premium plans include advanced features like predictive phishing engines, legal escalation modules and global registrar partnerships. Union Bank can also monetize by licensing the platform to private banks or fintech companies seeking robust cybersecurity solutions. Additionally, the platform can charge third-party cybersecurity firms for API access to its threat intelligence database. The value proposition lies in offering a unified, proactive and scalable solution that reduces phishing related losses, enhances customer trust and streamlines regulatory compliance. By owning this platform Union Bank can position itself as a cybersecurity leader while generating recurring revenue from subscriptions and licensing fees.

2) Commercialization Potential and Scalability

- The target includes 12 PSBs, 22 private banks, and 10,000+ NBFCs/fintechs in India.
- With 60% of banks still using legacy systems, the platform's modular design ensures scalability.
- Union Bank can first deploy the platform internally to prove its effectiveness.
- Once validated, it can market the solution to PSBs via government initiatives.
- Union Bank can leverage its reputation and government ties to gain early adopters.
- Partnering with CERT-In, which handles 1.3 million cyber incidents yearly, aligns with national priorities.
- Global reach can be expanded through top 10 registrars like GoDaddy and Namecheap, controlling 60% of domains.
- Initial phases focus on detection and reporting, with predictive engines and legal escalation added later.
- Union Bank can white-label the platform for global banks or offer it as SaaS to smaller institutions.
- With 35% of banks resisting tech upgrades, API-based integration enables phased adoption.

RESEARCH AND REFERENCES

Mandatory Submission: Summary

Details/Links of References and Research work

- https://www.giac.org/paper/gsec/4323/phishing-banks-timely-analysis-identity-theft-fraud-financial-sector/107044#:~:text=Some%20of%20the%20more%20simpler,www.legitimatbanking.com).
- https://www.ijstr.org/final-print/oct2019/Detailed-Study-On-Phishing-Site-Detection-For-E-banking-Security-.pdf
- https://www.sciencedirect.com/science/article/pii/S1319157823000034
- https://ieeexplore.ieee.org/ielaam/6287639/8948470/8970564-aam.pdf
- https://www.researchgate.net/publication/365790574_Phishing_URL_detection_using_machine_learning_methods
- https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2024.1428013/full
- https://www.sciencedirect.com/science/article/abs/pii/S0167404824001445
- https://www.researchgate.net/publication/268334916_Security_Issues_on_Banking_Systems
- https://www.iibf.org.in/documents/reseach-report/Tejinder_Final%20.pdf
- https://www.iibf.org.in/documents/BankQuest/Bank-Quest-Jan-Mar-2018-Final-200418.pdf
- https://inspirajournals.com/uploads/Issues/1599392142.pdf