Raising Cybersecurity Awareness: Using Gamification and AI Nudging Supported by Cyber Law.

Name of Authors : 1. Piyush A. Gandhi (Author),

2. Asawari P. Shinde (Co-Author).

Year & Department Name : Third Year, Computer Engineering.

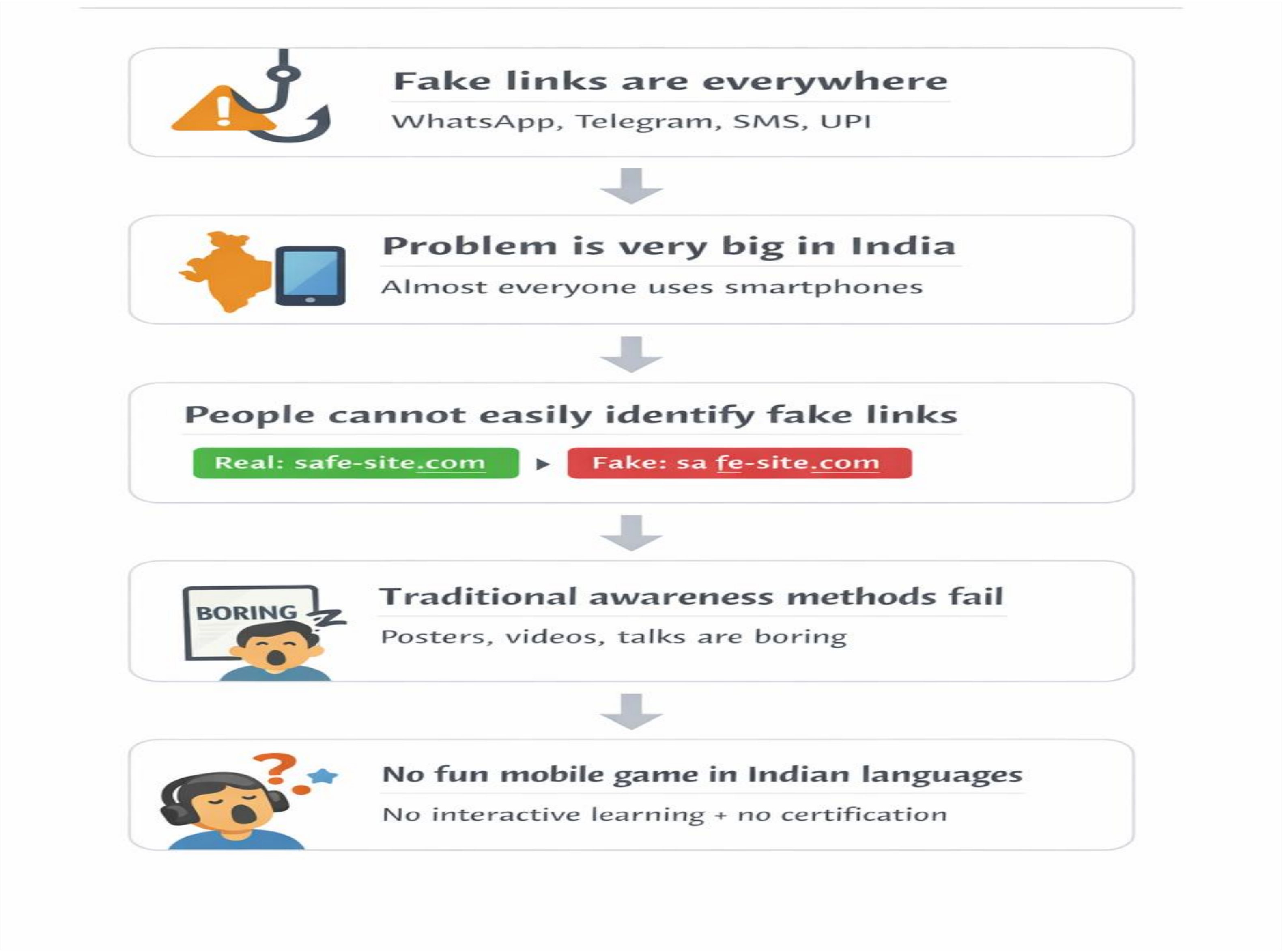
Institute Name : Trinity Polytechnic, Pune (1734) - MSBTE.

Guide Name : Rahul D. Dhongade.

INTRODUCTION

1. Rising Threat: Phishing attacks via malicious links remain one of the top cybercrimes globally and in India (APWG & CERT-In 2024–2025 reports).
2. India Context: High mobile usage + rapid growth in WhatsApp, Telegram, UPI fraud → millions at risk daily.
3. Awareness Gap: Traditional methods (posters, videos, workshops) are passive → low engagement & poor long-term retention.
4. Power of Gamification: Serious games proven to improve knowledge through interaction between system & User.

PROBLEM STATEMENT



Fake links are everywhere

WhatsApp, Telegram, SMS, UPI

Problem is very big in India

Almost everyone uses smartphones

People cannot easily identify fake links

Real: safe-site.com ▸ Fake: sa fe-site.com

Traditional awareness methods fail

Posters, videos, talks are boring

No fun mobile game in Indian languages

No interactive learning + no certification

EXISTING SYSTEM

1. Majority of users fail to detect sophisticated phishing URLs (typosquatting, homoglyphs, fake subdomains, encoded URLs, shortened links).
2. Low cybersecurity literacy among non-technical Indian users.
3. Existing tools are mostly English-only, passive, and lack India-specific context (UPI, regional apps).

PROPOSED SYSTEM

1. 100 levels + 20-question final quiz.
2. 3 lives per level, streak scoring, badges.
3. Rule-based fake link generation. (for ex: grnail.com = m)
4. Multilingual UI (13 Indian languages).
5. Secure quiz mode (anti-exit, anti-screenshot).
6. Digital certificate (PDF/JPG + QR verification).
7. Indian focus: I4C, 1930 helpline, cybercrime.gov.in, CERT-In, regional language support.

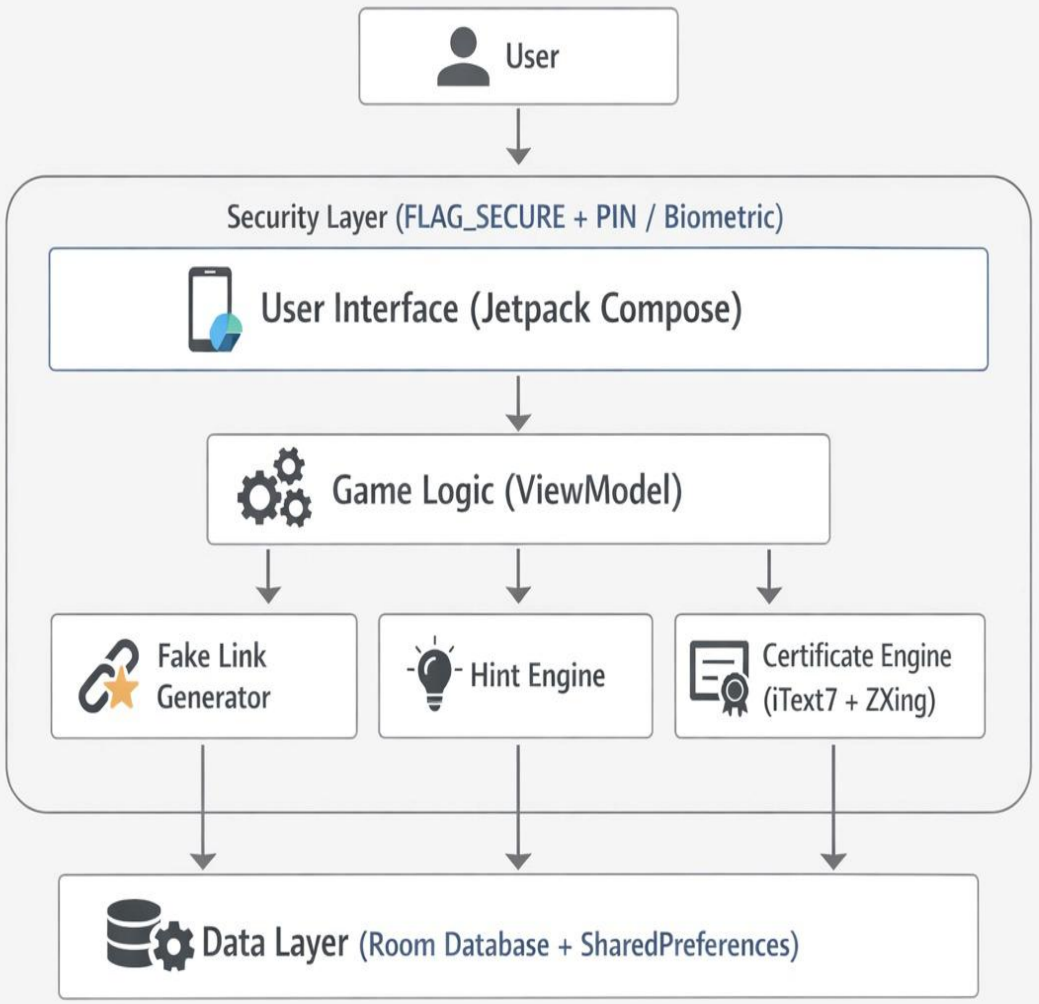
LITERATURE SURVEY

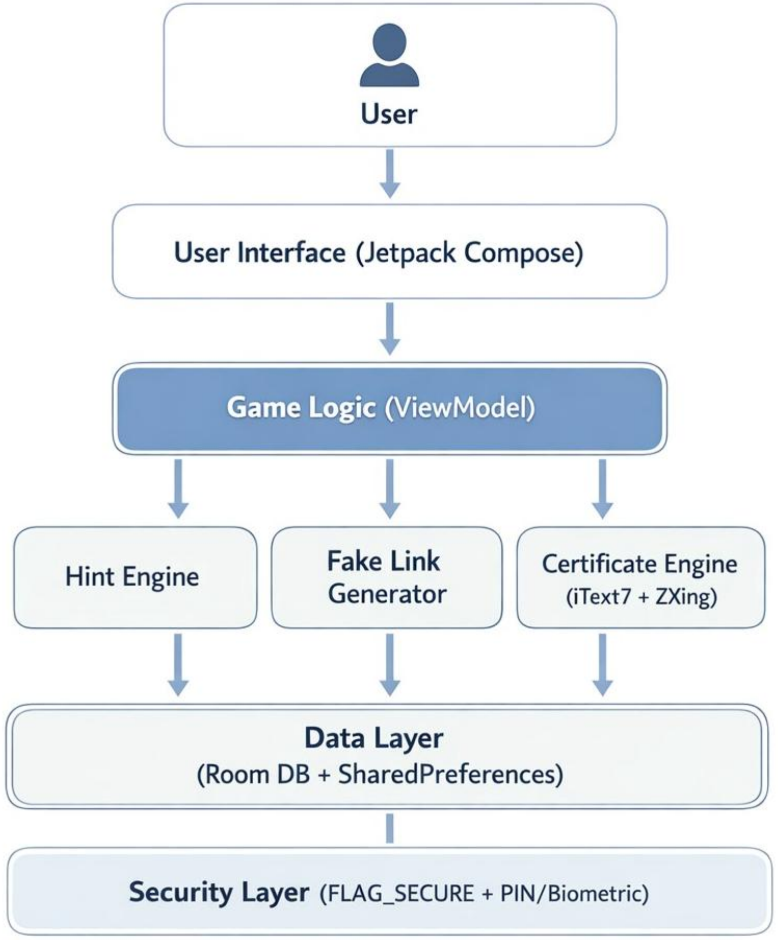
Author (Year)	Domain / Focus	Methodology / Techniques	Key Contributions	Remarks / Limitations
Sheng et al. (2010)	Phishing education via games	Game-based training (Anti-Phishing Phil), user study	First widely cited serious game for phishing; improved recognition rates by ~40% in short term	Web-based prototype, English-only, no mobile version, short-term retention only
Kumaraguru et al. (2007)	Phishing susceptibility & interventions	User studies, training materials, embedded training	Showed that embedded training (in-context warnings) outperforms mass training	Focused on email phishing; no mobile or link-specific focus; dated dataset
Alkhushayni & Lee (2025)	Multilingual / low-resource sentiment analysis	Translation augmentation + SVM / pre-trained models	Improved cross-lingual generalization for low-resource languages (including some Indian languages)	Primarily sentiment analysis (not phishing); e-commerce focus; no gamification
Mao et al. (2024)	General phishing & social engineering survey	Systematic review (PRISMA), 200+ papers	Broad categorization of phishing techniques, datasets, and countermeasures; identifies gaps	Review paper; no original implementation; limited focus on user education games
CERT-In / MeitY (2024–2025)	India-specific cybercrime & phishing trends	Annual reports, helpline data (1930), UPI fraud analysis	Documents massive rise in WhatsApp/Telegram phishing in India; recommends awareness campaigns	Official report; no technical/game-based solution; passive awareness only
Chaithra et al. (2025)	Financial phishing & sentiment in news	Instruction-tuned LLMs + RAG + Reinforcement Learning	Improved detection of financial phishing in news/articles; supports real-time decision making	Finance/news domain only; no user-facing game or training component

OBJECTIVES

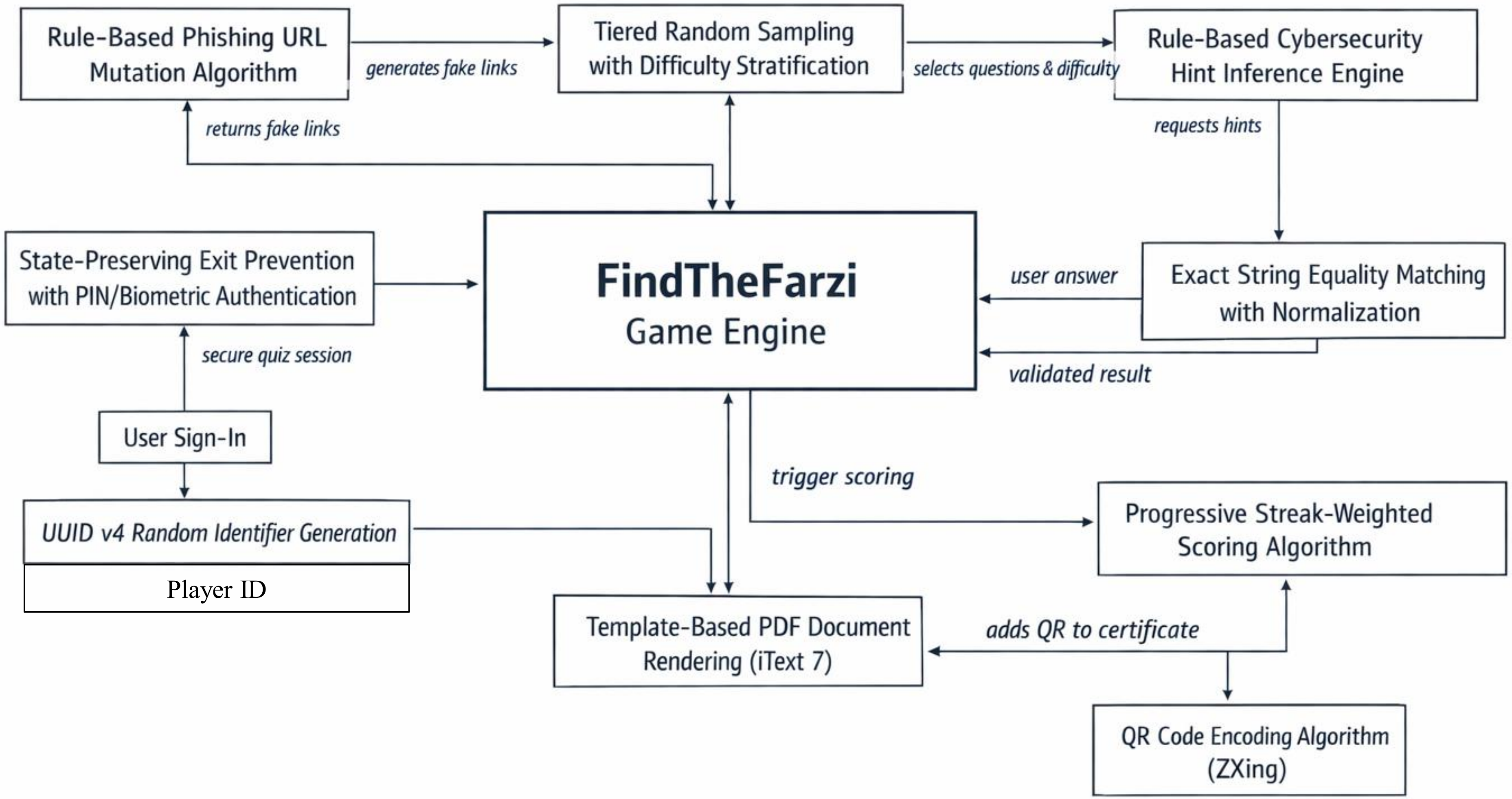
1. To design and develop an interactive mobile game that effectively trains users to detect phishing and malicious links in real-world scenarios.
2. To implement a realistic fake link generation system using a rule-based mutation algorithm tailored for Indian social media and messaging platforms.
3. To prominently promote Indian cyber helplines (e.g., I4C 1930) and resources within the app to encourage immediate action in real incidents.
4. To evaluate the game’s effectiveness in improving phishing detection skills through simulated training and user feedback in an Indian context.

SYSTEM ARCHITECTURE


User
Security Layer (FLAG_SECURE + PIN / Biometric)
User Interface (Jetpack Compose)
Game Logic (ViewModel)
Fake Link Generator
Hint Engine
Certificate Engine (iText7 + ZXing)
Data Layer (Room Database + SharedPreferences)


User
User Interface (Jetpack Compose)
Game Logic (ViewModel)
Hint Engine
Fake Link Generator
Certificate Engine (iText7 + ZXing)
Data Layer
(Room DB + SharedPreferences)
Security Layer (FLAG_SECURE + PIN/Biometric)

METHODOLOGY


Rule-Based Phishing URL Mutation Algorithm
generates fake links
Tiered Random Sampling with Difficulty Stratification
selects questions & difficulty
Rule-Based Cybersecurity Hint Inference Engine
returns fake links
requests hints
State-Preserving Exit Prevention with PIN/Biometric Authentication
FindTheFarzi
Game Engine
user answer
Exact String Equality Matching with Normalization
validated result
secure quiz session
User Sign-In
trigger scoring
UUID v4 Random Identifier Generation
Player ID
Progressive Streak-Weighted Scoring Algorithm
Template-Based PDF Document Rendering (iText 7)
adds QR to certificate
QR Code Encoding Algorithm (ZXing)

FUTURE SCOPE

1. iOS version (SwiftUI / Flutter).
2. Multiplayer / friend challenge mode.
3. On-device ML for real-time link analysis.
4. Integration with CERT-In / I4C threat feeds.
5. AR mode (scan real QR codes).
6. Voice-guided hints in regional languages.
7. Global leaderboard & social sharing.

CONCLUSION

1. Effective Gamification: FindTheFarzi transforms complex phishing detection into an engaging, repeatable mobile game, significantly improving user retention and skill acquisition compared to traditional awareness methods.

2. India-Centric Innovation: With multilingual support (13 languages), realistic rule-based fake link generation, and prominent promotion of I4C 1930 helpline, the app addresses the unique needs of Indian smartphone users.

3. Secure & Verifiable Impact: Strong anti-cheat mechanisms, verifiable digital certification with QR code, and safe simulation environment position FindTheFarzi as a credible tool with potential to reduce phishing vulnerability at scale.

THANK YOU.