Phantom Protocol: AI powered Infiltration and Escalation System For Digital Risk Environments.

Students of IV/IV Bachelor of Technology,
Department of Computer Science and Engineering (Data Science)

Team : Strategic Boosted Algorithms
Sathvik Eppakayala (Y22CD033)
Ankula Shiva Kumar Goud (Y22CD004)
Rishitha Pagadala (Y22CD127)

R.V.R. & J.C. College of Engineering
Chowdavaram, Guntur, Andhra Pradesh, 522019

Problem Statement & Approach

In today's more digital world, law enforcement and intelligence agencies face bigger challenges in detecting, assessing, and responding to real-time scams or threats on unstructured communication platforms like Telegram and other encrypted or semi-open networks.

This Highly makes us:

- Delayed threat identification and response times
- Inability to coordinate across agencies in real time
- Missed signals in decentralized or fast-moving digital environments
- Lack of actionable insight from unstructured data streams

Given the absence of a comprehensive real-time monitoring system for such threats, we developed an automated solution that not only monitors activity continuously but also identifies and reports potential criminal behavior proactively.

Approach

Our Methodology Involves in the following:

- Real Time Monitoring using AI Bot.
- AI Driven Threat Analysis
- Dynamic Risk Scoring using Risk factors
- Smart Escalation Logic
- Reporting & Coordination
- Privacy & Ethical Compliance

All of them will be briefly mentioned in the next slides.

Real Time monitoring using AI Bot

- This could be very useful for the Department of Intelligence to stop Cyber Scam.

This Involves in the following:

❖ Telegram native Integration with Our AI LLM Bot(Most Scams happens on telegram).

❖ Autonomous Data Capture: It will search for suspicious information in the group 24/7 without any manual intervention.

❖ Instant Threat Recognition: If suspicious content is detected, initially it reports the threat. Then starts the investigation without any manual intervention. The Bot will never get caught; it acts as a real Human.

❖ Escalation: If any decoy Agents are found in the group, It messages as the victim persona and tries to retrieve all the details from the Decoy Agent, or the suspect.

❖ This Bot will also, makes immediate actions based on the risk of the suspicious activity found.

AI Driven Threat Analysis

We use the following for Threat Analysis, which calculates the Risk score of each suspect, and the group making such suspicious activity

- Analyze messages of Hate Speech, Threats, misinformation or any other Online fraud.
- We will also use LLM to integrate real time analysis for positive form/negative form of the message.
- We will also try to scan the images, analyse the audios, and Video scanning.
- Behavioural Pattern detection
- Threat Classification & Risk Score Analysis
- For this, we will be using several NLP, ML, Techniques.

Smart Escalation Logic

Multi-Level Response Framework

- Level 1 – Low risk: Logged for analytics
- Level 2 – Moderate risk: Flagged for human review
- Level 3 – High risk: Immediate alert to enforcement channel

Human-in-the-Loop Oversight

- Critical escalations are reviewed by trained analysts
- Ensures ethical validation and false positive control

Adaptive Learning

- Feedback from analysts and outcomes feeds back into the system
- Improves future detection accuracy and escalation precision

Reporting & Coordination

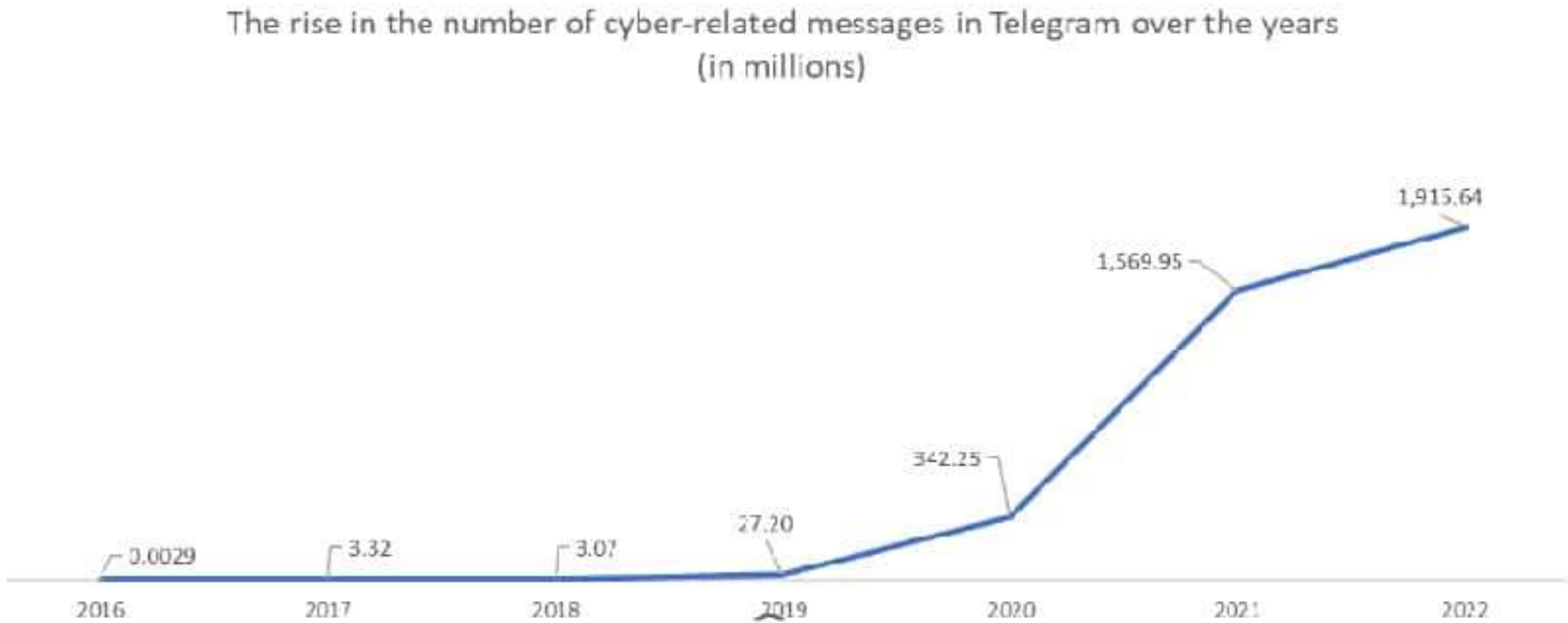
Law Enforcement Integration

- We will try to collaborate with cyber department, and will automate the process using 91crpc.
- Generates Real time reports, and send them via mail to the Bot user. Reporting the Crime in very short period of time.
- Depending on the risk score, it will also send the alerts and call back notices to the user.
- If used by the Department of Police, It would send alerts to the department, when it gets suspicious content in the group.

Advantages of this Approach

1. Real-Time Intelligence
2. AI-Powered Accuracy
3. Automated Escalation
4. Ethical Oversight
5. Seamless Law Enforcement Coordination

The rise in the number of cyber-related messages in Telegram over the years



Cyber Crimes Over Years

Cybercrimes

The Delhi police has investigated financial frauds worth over ₹500 crore between January and July this year

At least **700** people are falling prey to cyber frauds every day

- The cyber helpline number 1930 receives, on average 55,000 to 60,000 calls per month
- 700 to 800 new complaints are registered every day
- Out of these 700 calls, 200-250 pertain to financial frauds
- The rest of the calls pertain to 'sextortion', digital arrest, matrimonial website frauds and cheating on the pretext of offering work from home opportunities

> Police recently investigated a case where a man ended up losing ₹22 crore just because he wanted to double his investment

HEMANT TIWARI
Deputy Commissioner of Police (Cyber Cell)

SOURCE: DCP CYBER CRIME CELL

TELANGANA POLICE
Duty Honour Compassion

పైసలు ఏస్తరు.. అకౌంట్ ఖాళీ చేస్తరు

తక్కువ మొత్తం డిపాజిట్ చేసి ఫోన్‌కు క్రెడిట్ అలర్ట్

అ మెసేజ్ చూసి యూపీఐ బ్యాలెన్స్ చెక్ చేస్తే ఖాతాలోని డబ్బు గాయబ్! డిపాజిట్ చేసిన మొత్తానికి చివర సున్నా చేర్చి అందినకాడికి దోచేస్తరు

మెసేజ్‌ల రూపంలోనూ యూపీఐ లింకులు, క్లిక్ చేస్తే అంతే..!

యూపీఐలో అడ్డగోలుగా పెరుగుతున్న జంప్ డిపాజిట్ స్కామ్స్

హైదరాబాద్, వెలుగు:

సైబర్ నేరగాళ్లు మన అకౌంట్‌లో ఎంతోకొంత డబ్బు డిపాజిట్ చేసి ఉన్నదంతా ఊడ్చేస్తున్నారు. డిపాజిట్ చేసిన మొత్తానికి సున్నా చేర్చి మరిందను వేయగా.. వేలు లక్షలుగా మార్చి కొట్టేస్తున్నారు. రీఫండ్ చేయమనే కాల్ చేసి బెదిరింపులకు పాల్పడుతున్నారు. ఇలా యూపీఐ లద్దాగా సాగుతున్న సైబర్ మోసాలను 'జంప్ డిపాజిట్ స్కామ్'గా దేవనల్ సైబర్ క్రైమ్ పోర్టల్ గుర్తించింది. పేమెంట్ గేట్‌వే, ఈకామర్స్, బ్యాంక్ పోర్టల్స్, టాక్స్ రిఫండ్ తదితర పేర్లతో మోసాలపై అలర్ట్‌గా ఉండాలని ప్రజలకు సూచిస్తోంది. ఇప్పటికే రాష్ట్రాల సైబర్ క్రైమ్ పోలీసులకూ అలర్ట్ జారీ చేసింది. మనకు తెలియకుండానే ఎంతోకొంత డబ్బు డిపాజిట్ అయినట్లు మెసేజ్‌లు రాగానే వెంటనే యూపీఐ పేమెంట్ యాప్‌ను ఓపెన్ చేయొద్దని నిపుణులు సూచిస్తున్నారు.

సున్నా చేర్చి పంపుతారు..

సైబర్ నేరగాళ్లు ఫోన్‌పే, గూగుల్ పేతోపాటు ఇతర పేమెంట్ గేట్‌వేలతో లింకులు ఉండేలా చేస్తున్నారు. రూ.1000 నుంచి రూ.5 వేలదాకా డిపాజిట్ చేస్తున్నారు. మిగతా 2లో

ఇలాంటి మోసాలు ఈ మధ్య ఎక్కువగా జరుగుతున్నాయి. అకౌంట్‌లో డబ్బు డిపాజిట్ చేసిన వెంటనే.. ఫోన్ లేదా పీసీ యాక్టివేట్ అవుతుంది. కాని ఇలాంటి డిపాజిట్ జరిగిన వారం 15 నుంచి 30 నిమిషాల పాటు యూపీఐని వాడొద్దు. మనం ఆ లింకులు ఓపెన్ చేశామంటే స్కామర్లు పీడ్ చేసుకున్న మొత్తం ఇతర ఖాతాదారికి ట్రాన్స్‌ఫర్ అవుతుంది. మ్యూల్ అకౌంట్, కొనుగోలు చేసిన బ్యాంక్ అకౌంట్ల ద్వారా పరిడ్రా చేస్తుంటరు. ఇలాంటి మోసానికి గురైతే వెంటనే 1930 లేదా సైబర్ క్రైమ్ పోలీసులను ఆశ్రయించాలి.

– వక్కలగడ్డ వంశీకృష్ణ, ఎథికల్ హ్యాకర్, ఎసీఐపీఐ సొల్యూషన్స్, హైదరాబాద్

..అకౌంట్ ఖాళీ చేస్తరు

(మొదటి పేజీ తరువాయి)

దీనికి సంబంధించిన క్రెడిట్ అలర్ట్ మెసేజ్ పంపిస్తున్నారు. సాధారణంగా ఇలాంటి మెసేజ్ వచ్చిన వెంటనే ఫోన్‌పేలోనో, జీపేలోనో బ్యాలెన్స్ చెక్ చేస్తుంటాం. దీన్నే సైబర్ నేరగాళ్లు అదునుగా వేసుకున్నారు. క్రెడిట్ అలర్ట్, లింకులు క్రియేట్ చేస్తున్నారు. తాము డిపాజిట్ చేసిన మొత్తానికి చివర 'సున్నా' కలుపుతున్నారు. రూ.పందర్లో పంపిన మొత్తం వేలుగా..వేల్లో డిపాజిట్ చేసిన మొత్తం లక్షలుగా మార్చేస్తున్నారు. బ్యాలెన్స్ చెక్ చేసేందుకు మనం యూపీఐ పిన్ ఎంటర్ చేసిన వెంటనే సైబర్ నేరగాళ్లు అప్పటికే ఎంటర్ చేసుకున్న అమౌంట్ మొత్తం వాళ్ల యూపీఐ ద్వారా వాళ్ల బ్యాంక్ అకౌంట్‌లో డిపాజిట్ అయ్యేలా లింకులు క్రియేట్ చేసి పంపిస్తున్నారు.

రీఫండ్ చేయాలని రిక్వెస్టులు, లేదంటే బెదిరింపులు

యూపీఐని వాడనివాళ్లకు సైబర్ నేరగాళ్లు కాల్స్ చేసి మోసాలకు పాల్పడుతున్నారు. మరొకరి అకౌంట్‌కి పంపాల్సిన డబ్బు పొరపాటున మీకు పంపించామని, రివర్స్ కొట్టండి అంటూ రిక్వెస్ట్ చేస్తారు. అమాయకులైతే బ్యాంక్ బ్యాలెన్స్ చెక్ చేసుకోవాలని సూచిస్తారు. మెసేజ్‌లో ఉన్న లింక్‌ను క్లిక్ చేసి ఫోన్‌పే లేదా జీపేకి రిఫండ్ చేయాలని కోరుతారు. ఇక్కడే అసలు మోసం ఉంటుంది. సైబర్ నేరగాళ్లు పంపించిన మెసేజ్‌లో ఉదాహరణకు రూ.5 వేలు డిపాజిట్ అయినట్లుంటే.. వారు పంపించే లింకులో మాత్రం రూ.50 వేలు తమ అకౌంట్‌కి క్రెడిట్ అయ్యేలా ఫీడ్ చేస్తున్నారు. దీంతో లింక్ ఓపెన్ చేసి యూపీఐ పిన్ ఎంటర్ చేసిన వెంటనే సైబర్ నేరగాళ్ల టార్గెట్ పూర్తవుతుంది. వాళ్లు చెప్పినట్లుగా రీఫండ్ చేయనివాళ్లకు కాల్స్ చేసి బెదిరింపులకు పాల్పడుతున్నారు. పోలీసు మార్కింగ్ చేసి సోషల్‌మీడియాలో పెట్టామని ఫ్రాడ్ మెయిల్ చేస్తున్నారు.

ఈ కామర్స్‌లో ఓవర్ పేమెంట్, జాబ్ రీఫండ్ స్కామ్..

ఓఎల్ఎక్స్, ఫేస్‌బుక్, మ్యాట్రిమోనీ సైట్ లాంటి ఈ కామర్స్ సైట్లలోనూ సైబర్ నేరగాళ్లు చేతివాలం ప్రదర్శిస్తున్నారు. అమ్మకానికి పెట్టిన వస్తువులను కొంటామని నమ్మించి, రేట్లు తగ్గించాలని అడుగుతున్నారు. చివరకు ఓ రేటు ఫిక్స్ చేసుకున్నాక డబ్బులు యూపీఐ ద్వారా చెల్లిస్తామని చెప్పారు ఫిక్స్ అయిన రేటు కంటే ఎక్కువ మొత్తంలో డబ్బులు పంపినట్లు నమ్మిస్తారు. అదనంగా వచ్చిన డబ్బు రీఫండ్ చేయాలని కోరి మోసాలకు పాల్పడతారు. ఈరీలో నిరుద్యోగ యువతలను టార్గెట్ చేస్తున్నారు. రిక్రూటర్లుగా వ్యవహరిస్తూ.. మెసేజ్‌లు పంపిస్తున్నారు. అధిక మొత్తంలో జీతాలంటూ ఆశ పెట్టి, ట్రావ్ చేస్తున్నారు. వెరిఫికేషన్, రిక్రూట్‌మెంట్ ఫీజు పేరుతో హంగామా చేస్తారు. సెలెక్ట్ అయ్యారని నమ్మిస్తారు. అడ్వాన్స్ సాలరీ లేదా జాయినింగ్ బోనస్ పేరుతో బ్యాంకులో చెక్ డిపాజిట్ చేశామని చెప్తారు. ఇవ్వాల్సిన దానికంటే ఎక్కువగా డిపాజిట్ చేశామని, టెక్నికల్ ఇష్యూస్ వల్ల చెక్ క్యాన్సిల్ అయిందని నమ్మిస్తారు. అందుకు సంబంధించి నకిలీ రిసీప్టులను బాధితులకు పంపిస్తారు. ఎక్కువగా డిపాజిట్ చేసిన డబ్బు తిరిగి ఇవ్వాలని సూచిస్తారు. లేదంటే ఉద్యోగం రాకపోగా, రిమార్క్ చేస్తామని బెదిరిస్తారు.

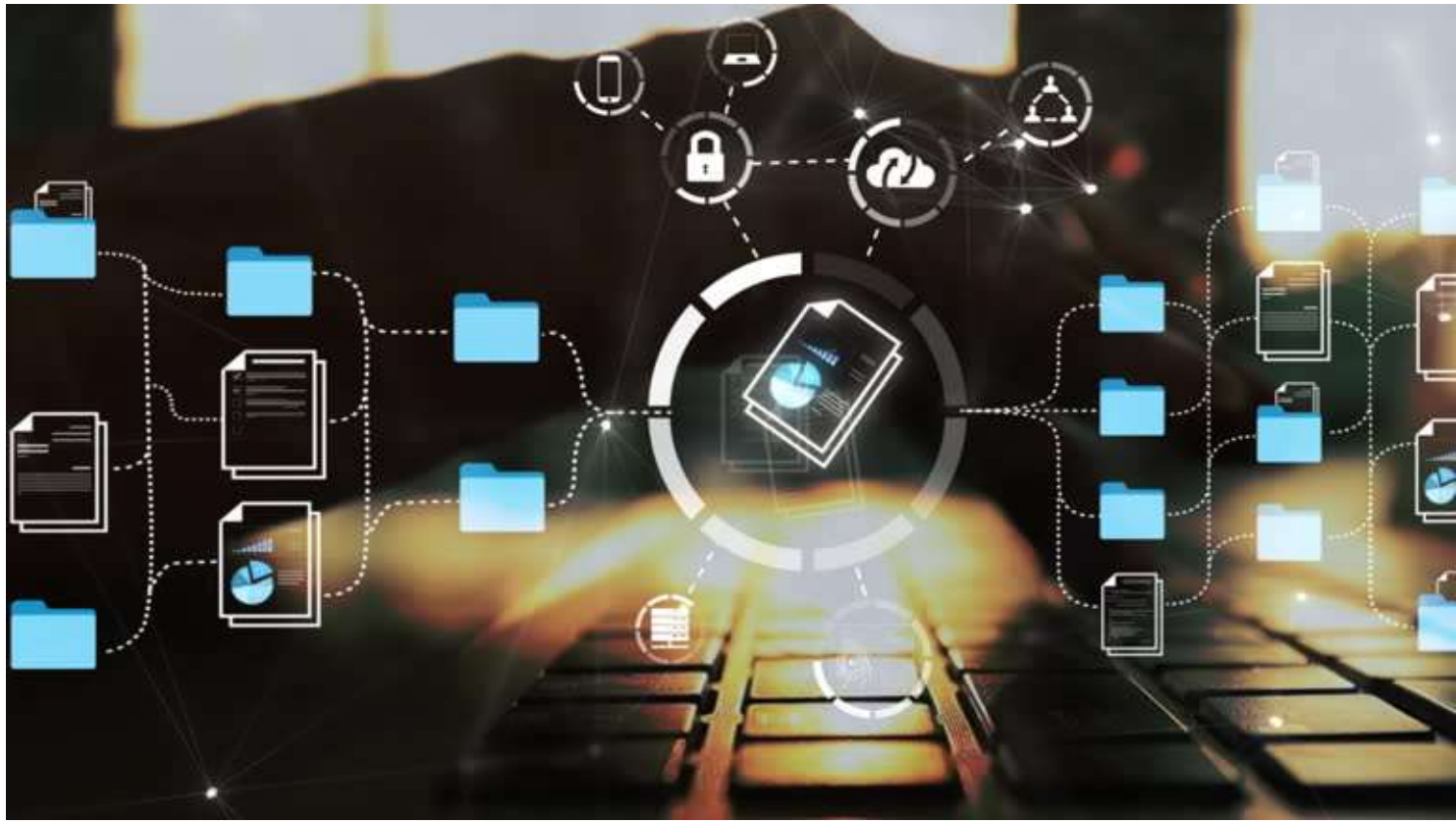
Social Impact

- ❖Enhanced Public Safety
- ❖Faster Crime Detection & Prevention
- ❖Support for Law Enforcement Agencies
- ❖Protection Against Digital Radicalization
- ❖Safeguarding Vulnerable Communities
- ❖Online Promoting
- ❖Ethical AI Use in Security Building
- ❖Trust in Digital Communication Platforms

Real Time Applications

- ❖Monitoring Suspicious Telegram Groups & Channels
- ❖Early Detection of Cyberbullying or Online Harassment
- ❖Tracking Organized Crime & Illicit Trade Networks
- ❖Identifying and Escalating Terror Threats or Radical Content
- ❖Coordinating Digital Evidence Collection for Law Enforcement
- ❖Real-Time Alerts for Fraud, Scams, or Financial Crimes
- ❖Surveillance of Crisis Events (riots, protests, misinformation spread)
- ❖Action Against betting Channels, Betting promoters, and cyber fraud Agents.

Technical Stack



Backend:

- Python (Flask, Fast API)
- MongoDB/ MySQL

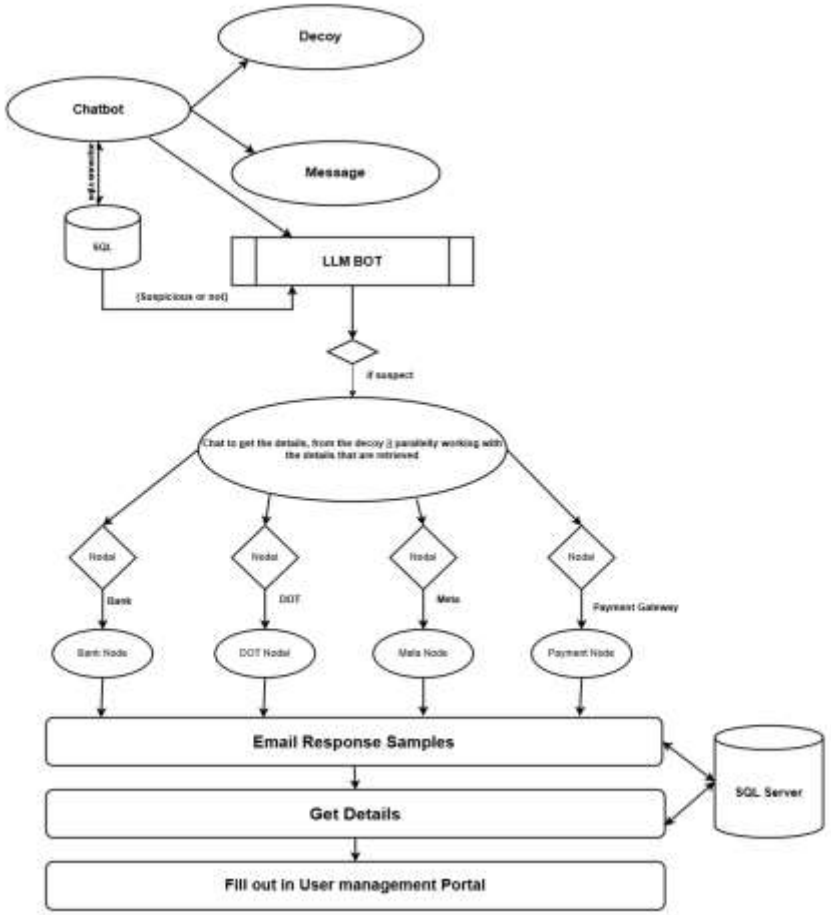
Frontend:

- HTML/CSS
- Java Script

LLMs:

- OpenAI, Gemini, Gemma
- We use only Free access LLM’s and mention them in our documentation too.

Expected System Architecture



22-yr-old kills self after losing ₹5L in online betting in NZB dist

TIMES NEWS NETWORK

Hyderabad: A 22-year-old man died by suicide in Akulakondu village in Nizamabad district after suffering heavy losses in online betting apps, police said on Tuesday.

The deceased, Akash, who worked at a local private company, had reportedly lost ₹5 lakh by placing bets on multiple online betting apps. On the night of March 26, overwhelmed by his losses, he consumed poison on the terrace of his residence in an attempt to end his life. His family members noticed him struggling and rushed him to a local hospital, where he succumbed on Tuesday.

After Akash was admitted to the hospital, doctors alerted the police about the suspected suicide attempt. "We recorded his dying declaration, in which he said that he had become addicted to online betting and lost ₹5 lakh. He felt extreme guilt over losing his hard-earned money," Nizamabad rural police told **TOI**.

Police revealed that Akash had been placing bets for the past six months on two betting apps — Crash and Colour Trading. He had first learned about these platforms through YouTube advertisements, which lured him into gambling.

A case has been registered, and an investigation is underway. Akash is survived by his wife.

బెట్టింగ్‌లో నష్టపోయి గొలుసు చోరీ.. రిమాండ్

కేపీహెచ్‌బీకాలనీ, న్యూస్‌టుడే: ఆన్‌లైన్ బెట్టింగ్‌లో నష్టపోయి బయటపడేందుకు గొలుసు చోరీ చేసిన నిందితుడు కటకటాలపాలయ్యాడు. సీఐ రవికుమార్ వివరాల ప్రకారం. కేపీహెచ్‌బీ పరిధిలోని వసతిగృహంలో ఉంటున్న యువతి బంజారాహిల్స్‌లో ఐటీ ఉద్యోగి. ఈ నెల 12న విధులు ముగించుకొని కేపీహెచ్‌బీ బస్టాప్ వద్ద బస్సు దిగి నడుస్తుండగా గుర్తుతెలియని వ్యక్తి ఆమె మెడలోంచి గొలుసు తెంచుకుని పారిపోయాడు. పోలీసులు సీసీ కెమెరాలు పరిశీలించగా కాలనీ రెండో రోడ్డు వైపు వెళ్లినట్లు గుర్తించారు. శనివారం ఉదయం కాలనీ ఒకటో రోడ్డులో అనుమానాస్పదంగా సంచరిస్తున్న వ్యక్తిని అదుపులోకి తీసుకొని విచారించగా గొలుసు చోరీకి పాల్పడినట్లు అంగీకరించాడు. తిరుపతి జిల్లా వెంకటగిరి పరిధి బొగ్గులమిట్ట గ్రామానికి చెందిన మల్లూరు శ్రీనివాసులుగా గుర్తించారు. కూకట్‌పల్లి పరిధి ఎల్లమ్మబండలో భార్యతో ఉంటూ జేఎన్‌టీయూ రోడ్డులోని ఓ వస్త్ర దుకాణంలో పనిచేస్తుంటాడు. ఆన్‌లైన్ బెట్టింగ్‌లో నష్టపోయి అప్పులపాలయ్యాడు. బయటపడేందుకు గొలుసు చోరీ చేయాలని పథకం వేసి దొరికిపోయాడు. గొలుసు స్వాధీనం చేసుకుని రిమాండ్‌కు తరలించారు.

Betting apps are like organised mafia, says Sajjanar

INTERVIEW

V.C. Sajjanar

Influencers put young lives at risk!

Create negative impact by promoting online betting apps through social media accounts

Recent suicide cases

Thank you

sathvikeppakayala@gmail.com
kumarshiva02877@gmail.com
rishithapagadala0@gmail.com