CYBERHACK 2025

PROBLEM STATEMENT : 02

Saving accounts and current accounts are taken on rent, and cybercrime gangs use these accounts for committing financial frauds at a very large scale. What technical solution can be adopted by banks to avoid the use of such rented accounts ?

PRESENTED BY (TEAM) :

CAFFEINE & CODE

TABLE OF CONTENT

CYBERHACK 2025

THEME

Combating Cyber Crime

MODE

Virtual (Preliminary Round)

Overview

Cybercriminals rent savings and current accounts from individuals or businesses to conduct large-scale financial frauds. These rented accounts are used as intermediaries to transfer or launder illicit money, making it difficult for law enforcement to track the actual perpetrators.

How the Fraud Works ?

1. **Recruitment of Account Holders :** Criminals offer individuals money to "rent" their bank accounts, which are then used for fraudulent transactions.

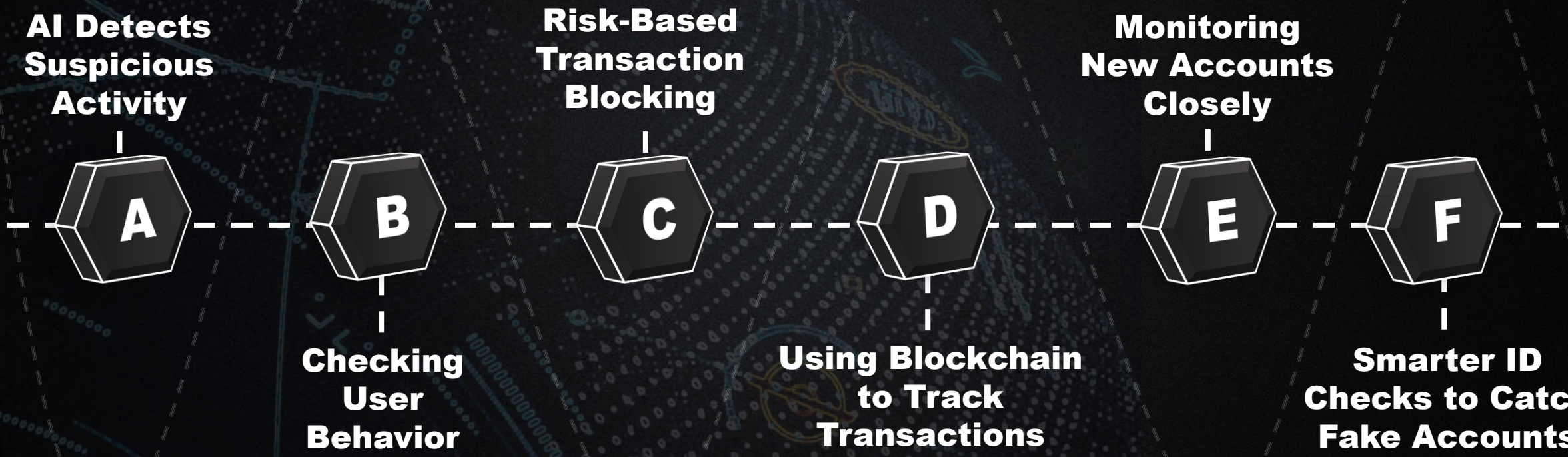
2. **Money Laundering** – These accounts serve as temporary repositories for illegally obtained funds before they are transferred to offshore accounts or withdrawn in cash

3. **Fraudulent Transactions** – Cybercriminals use these accounts for phishing, online scams, fake investment schemes, and unauthorized transfers.

CYBERHACK 2025

Proposed Solution

"SatyaShield : A Context based Detection System to Prevent Rented Account Scams !"



Proposed Solution Explanation

Intelligence Detects Suspicious Activity :

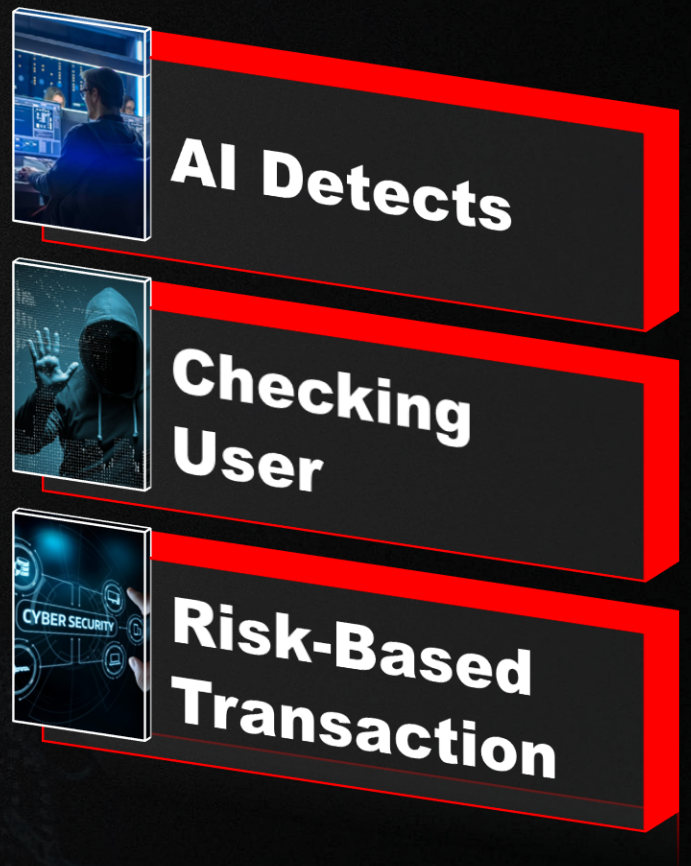
- A new account suddenly receives ₹10 lakh and transfers it to 5 different accounts within minutes.
- AI notices this is not normal behavior (because most people don't do such transactions).
- The bank flags the account for review and temporarily stops transactions.

Checking User Behavior :

- Fraudsters use the rented accounts from different devices, locations, and IP addresses.
- The bank notices that the account was logged in from Mumbai in the morning, Delhi in the afternoon, and Dubai at night—which is highly unusual!
- The system locks the account and asks for identity verification.

Risk-Based Transaction Blocking :

- If a person usually transfers ₹5,000 per month, but suddenly tries to send ₹5 lakh to multiple accounts, the system assigns a high-risk score.
- The bank halts the transaction and asks the user to verify with biometric authentication (face scan or fingerprint).
- If the person fails, the transaction is blocked.



Proposed Solution Explanation

Using Blockchain to Track Transactions :

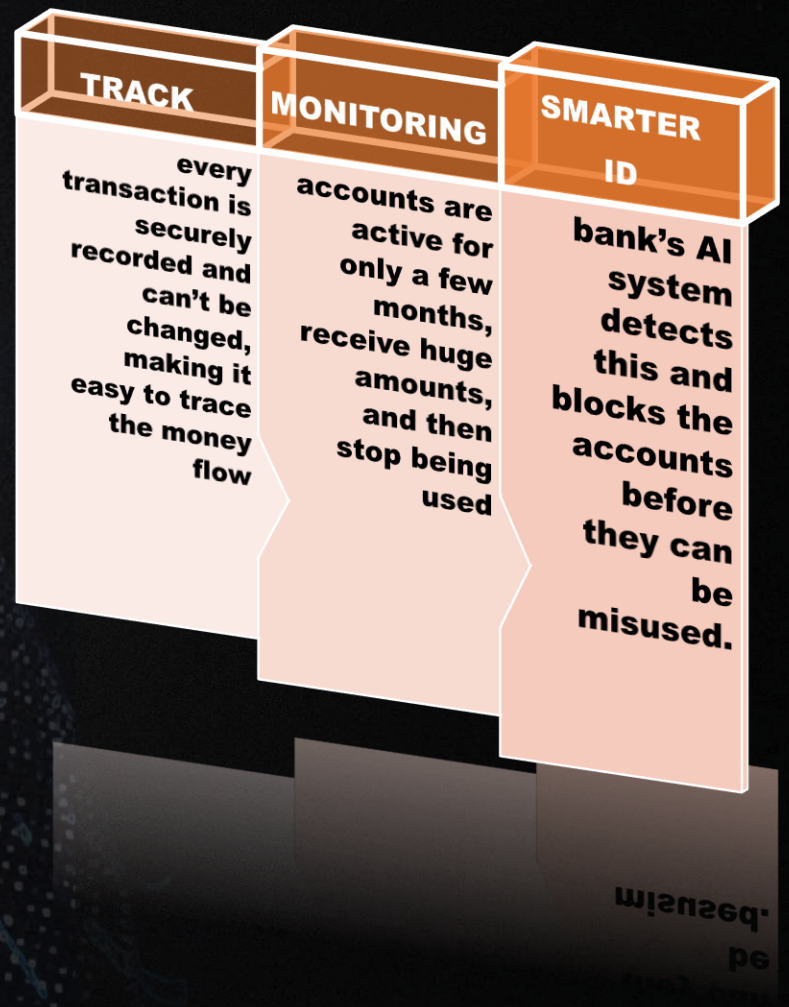
- Fraudsters move stolen money across multiple accounts to hide their tracks.
- With blockchain, every transaction is securely recorded and can't be changed, making it easy to trace the money flow.
- The bank quickly detects that the same few accounts are always involved in fraud and blacklists them.

Monitoring New Accounts Closely :

- Banks notice that some accounts are active for only a few months, receive huge amounts, and then stop being used.
- Such accounts get flagged for closer monitoring.

Smarter ID Checks to Catch Fake Accounts :

- A fraudster tries to open multiple accounts with different names but uses the same phone number, email, or fingerprint.
- The bank's AI system detects this and blocks the accounts before they can be misused.



CYBERHACK 2025

Technical Approach

1 Intelligent Fraud Detection System

- Uses Machine Learning
- Identifies suspicious patterns
- Assigns a risk score
- Auto-blocks

2 Intelligent User Behavior Analysis

- Monitors login activity, device usage, and IP tracking.
- multiple locations/devices in a short time.
- Triggers biometric re-authentication

3 Blockchain-Based Transaction Tracking

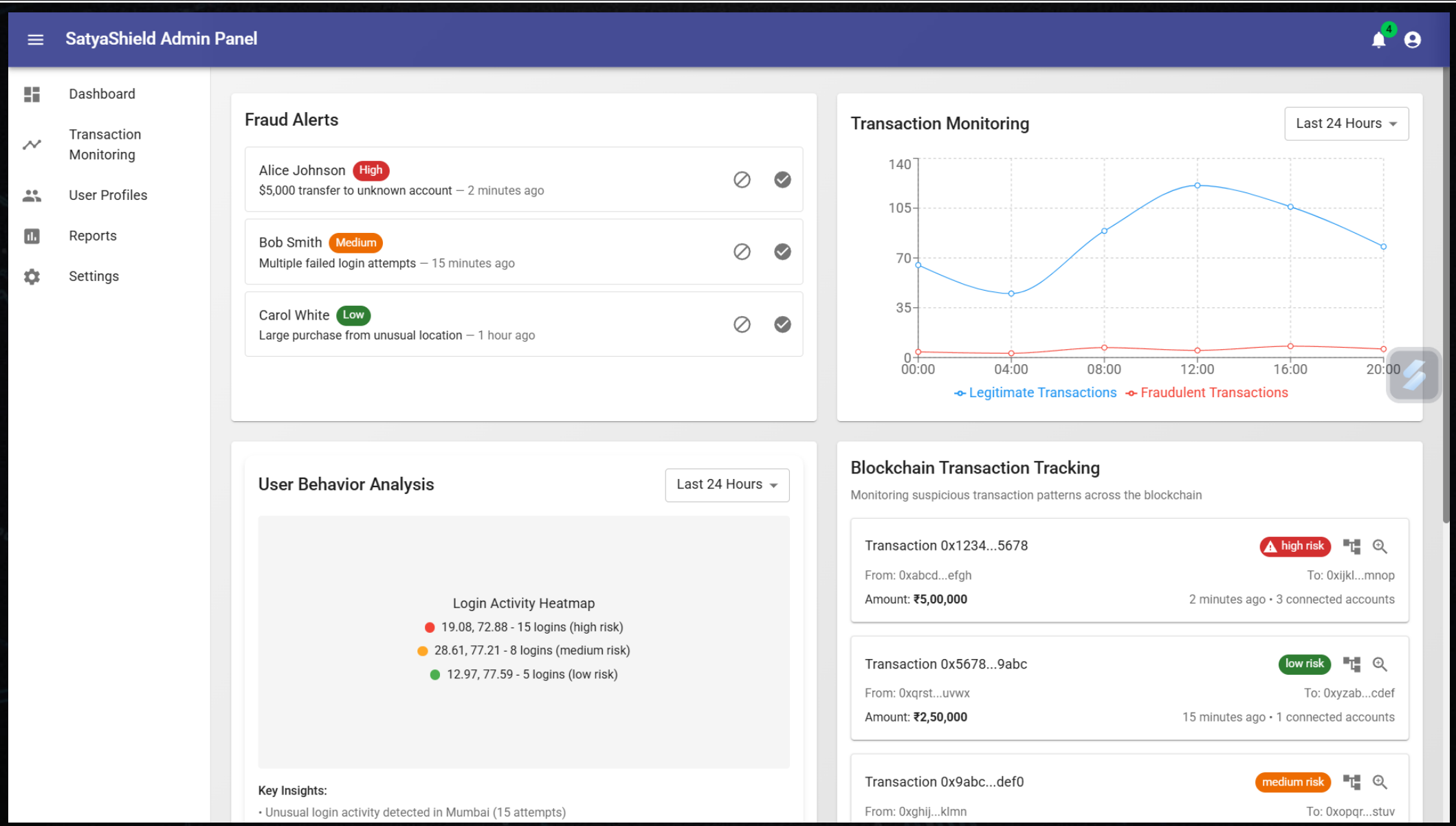
- Implements a blockchain ledger
- Prevents erasing transaction.
- Smart Contracts

4 Enhanced ID Verification & Account Monitoring

- Prevents fraud account creation
- liveness detection in Video KYC
- AI-based face recognition

SatyaShield Admin Panel

CYBERHACK 2025



SatyaShield Admin Panel

CYBERHACK 2025

SatyaShield Admin Panel

4

- Dashboard
- Transaction Monitoring
- User Profiles
- Reports
- Settings

From: 0xqrst...uvwx To: 0xyzab...cdef

Amount: **₹2,50,000** 15 minutes ago • 1 connected accounts

Transaction 0x9abc...def0 medium risk

From: 0xghij...klmn To: 0xopqr...stuv

Amount: **₹10,00,000** 1 hour ago • 2 connected accounts

Key Insights:

- Unusual login activity detected in Mumbai (15 attempts)
- Multiple failed login attempts from Delhi
- Normal activity patterns in Bangalore

Network Analysis

- 2 high-risk transaction patterns detected
- 3 new suspicious wallet addresses identified
- 5 connected transactions under investigation

Case Management

CREATE NEW CASE

Case ID	Customer	Type	Status	Priority	Assigned To	Last Updated	Actions
CASE-001	Amit Patel	Unauthorized Transaction	Open	High	Deepa Verma	10 minutes ago	
CASE-002	Sneha Reddy	Account Takeover Attempt	In Progress	Medium	Arjun Mehta	1 hour ago	
CASE-003	Karthik Iyer	Suspicious Login	Pending Review	Low	Priya Sharma	2 hours ago	

Feasibility & Viability

FEASIBLITY	VIABLITY
Technological Fit: Seamlessly integrates with existing banking infrastructure and fraud detection systems, ensuring high detection accuracy and minimal false positives.	**Cost Savings:** Helps reduce fraud-related financial losses by improving early fraud detection, enhancing return on investment.
Operational Efficiency: AI-driven fraud prevention reduces manual verification time by 40%, enhancing response speed and efficiency.	**Enhanced Customer Trust:** Strengthens account security, increasing customer confidence and satisfaction.
Scalable Solution: Deployable across multiple banks with minimal infrastructure upgrades, ensuring widespread implementation.	**Improved Fraud Detection:** AI-powered algorithms enhance fraud detection accuracy, minimizing false positives and fraudulent transactions.
Compliance Ready: Fully adheres to KYC, AML, and RBI financial security regulations, ensuring legal protection and industry compliance.	**Sustainable Growth:** AI continuously adapts to emerging fraud patterns, evolving with real-time threat intelligence to improve fraud prevention.

Impact & Benefits

POTENTIAL IMPACT	BENEFITS OF SOLUTION
Bank Customers: Ensures safer transactions, reduces fraud risks, and enhances user confidence in digital banking.	**Social:** Protects customers from financial fraud, enhancing digital banking trust.
Banking & Cybersecurity Teams: Automates fraud detection, reducing workload and improving accuracy.	**Economic:** Saves banks millions in fraud-related losses, boosting profitability and efficiency.
Bank Administrators & Decision Makers: Saves costs, improves risk management efficiency, and enhances compliance.	**Technological:** Advances AI-driven fraud detection, setting new industry security standards.
Financial System & Government: Strengthens financial security, reduces cybercrime impact, and improves trust in digital banking.	**Regulatory:** Ensures compliance with financial laws, reducing legal risks and penalties.

THANK YOU !