Overview of the Problem Statement and its Relevance to Banking/FinTech

Aligned with the theme "Code Against Malware", the proposed Host-based Ransomware Protection System (HBRPS) defends at the device level by detecting abnormal file encryption, suspicious processes, and malicious behaviour patterns. Unlike network-only defences, HBRPS offers granular host visibility, ensuring early detection, business continuity and stronger protection of customer trust and critical infrastructure.

What is Ransomware?

From deceptive tactics like Trojans to today's high-risk, high-impact ransomware attacks, the cybersecurity threat landscape has grown increasingly unpredictable and dangerous. Ransomware is a malicious software that encrypts files or locks systems, demanding ransom, often in cryptocurrency, for restoration. It spreads through clicking on phishing link, malicious downloads, communication with command and control (C&C), privilege escalation or exploiting software vulnerabilities to make the successful encryption of stored data. With banks, and FinTech firms handling sensitive data and real-time transactions, even a single ransomware attack can cause downtime, financial loss, and reputational damage.

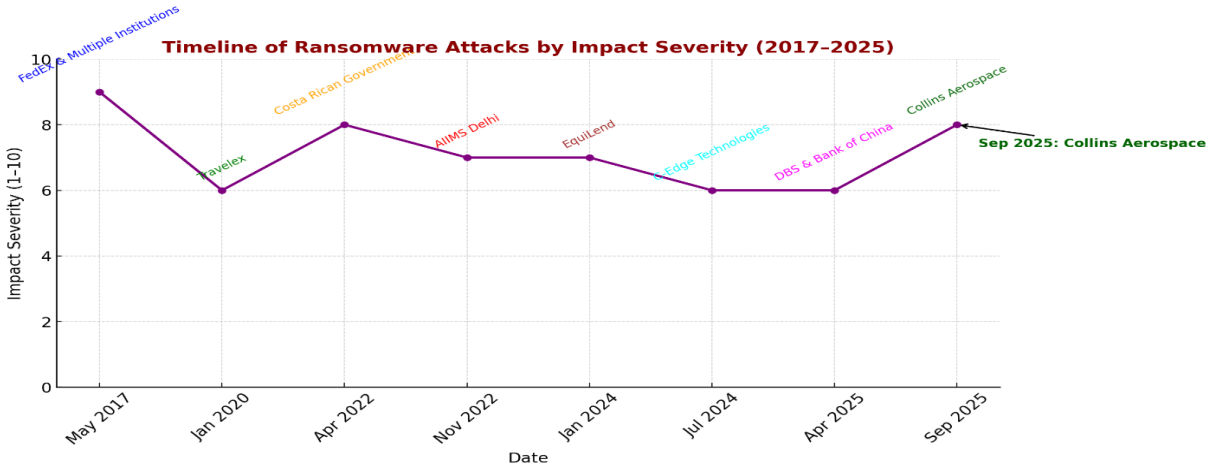
How It Affects Organizations, Especially Banks

Banks are particularly vulnerable to ransomware attacks due to their critical infrastructure and sensitive data. Such attacks can disrupt services, lead to data breaches and cause significant financial and reputational damage.

Operational Disruption	Ransomware can shut down critical systems, making it impossible to perform daily operations like processing transactions or accessing customer data.
Financial Losses	Banks may lose money through ransom payments, downtime, remediation costs and potential regulatory fines.

Reputation Damage	A ransomware attack can erode customer trust, especially if sensitive data is exposed.
Regulatory Impact	Banks operate in highly regulated environments. A breach can lead to investigations, penalties and loss of licenses or certifications.
Data Breach Consequences	Many ransomware variants now also steal data before encryption. This can result in data leakage, identity theft and class-action lawsuits.

Ransomware attacks have increasingly targeted the financial sector, causing significant operational, financial and reputational damage. Below is a timeline highlighting notable ransomware incidents affecting financial/other institutions:



Timeline showcasing major Ransomware attacks on the financial sector

Date	Bank/Institution	Location	Details
May 2017	FedEx & Multiple Institutions (Global)	Global	WannaCry exploited Windows vulnerability, encrypted systems, caused global disruptions including in finance. Increased scrutiny on cybersecurity.
January 2020	Travelex	UK	Ransomware shut down Travelex online services, disrupting FX services for customers and banks.
April 2022	Costa Rican Government (Financial Entities)	Costa Rica	Conti group attacked Costa Rican financial institutions, halted tax collection, $30M/day losses.

Nov 2022	AIIMS (All India Institute of Medical Sciences)	India	A major ransomware attack disrupted AIIMS Delhi's digital systems impacting patient data and lab services forcing manual operations. Involving cryptocurrency ransom demand.
January 2024	EquiLend	USA (Wall Street)	Ransomware attack disabled EquiLend for 2 weeks, disrupting securities lending. Increased risk and capital allocation costs.
July 2024	C-Edge Technologies	India	Affected nearly 300 small banks; NPCI isolated systems.
April 2025	DBS Group & Bank of China	Singapore	Attack on Toppan Next Tech exposed 8,200 DBS and 3,000 Bank of China customer records. Third-party vulnerability.
September 2025	Collins Aerospace (a subsidiary of RTX).	Brussels, London Heathrow, Berlin, and also Dublin	The attack disabled automatic check-in and bag-drop services at several European airports, causing delays, cancellations, and forcing staff to resort to manual check-ins

Description of the Solution Developed

Host-based ransomware protection systems (HBRPS) employs a multi-layered detection engine that combines signature-based and behavioral methods. The system integrates hash-based matching, YARA rule evaluation, and process-level behavioral monitoring to identify malicious activities. Real-time file system monitoring, implemented using Chokidar, enables immediate detection of suspicious modifications, especially ransomware-style encryption attempts.

The architecture is built with open-source technologies to ensure transparency and trust. A lightweight database powered by SQLite3 supports more than one million ransomware/malware signatures while keeping the memory footprint below 100 MB. A cross-platform Electron.js + SvelteKit user interface provides a simple, intuitive experience suitable even for non-technical banking staff, ensuring accessibility across endpoints.

The solution is compatible with both Windows (8/10/11 and Server editions) and Linux distributions, ensuring wide deployment coverage across bank environments.

Highlights of the Team's Journey Through the Hackathon

The initiative generated significant interest, resulting in a total of 84 registrations. From this pool, 15 formal proposals were ultimately submitted. Furthermore, we received six pilot projects for evaluation from leading institutions across the country, including IIT Kanpur, IIT Chennai, IIT Allahabad and C-DAC. Each participating development group was structured with three to four members. evaluated by expert jury members. Among the participants, Team PwnedRaccoons from IIT Kanpur stood out, excelling across detection, prevention, and analysis challenges with a resource-efficient, solution operating under 100 MB. Their collaborative and innovative approach addressed real-world banking needs while ensuring resilience on legacy systems.

Shri M. Nagaraju, Secretary, DFS; Prof. Manindra Agrawal, Director, IIT Kanpur; Shri Atul Kumar Goel, Chief Executive, IBA; Shri Ashok Chandra, MD & CEO, PNB; with the winning team members of IIT Kanpur at the PSBs' Cybersecurity Hackathon Prize Distribution Ceremony.

The journey culminated at the Prize Distribution Ceremony on 19th July 2025 at PNB Corporate Office, Dwarka. New Delhi.

Role of the Bank in Mentoring and Supporting the Team

Punjab National Bank defined the problem statement under the theme "Code Against Malware", focusing on Host-based Ransomware Protection Systems (HBRPS) to tackle sector-specific threats. Bank nurtured the participant to develop anti ransomware system by providing details of ransomware life cycle & its phases, hashes & yara rules, provided sandbox environments for testing, curated datasets, visibility into system requirements, and real-time testing support. Senior officials mentored participants through interactive sessions, offering technical feedback and operational insights. This structured support, along with formal collaboration via MoU with IIT Kanpur, ensured impactful innovation and long-term relevance for the banking sector.

Notable Outcomes, Learnings, and Future Plans

Outcomes

The development of **Host-based ransomware protection systems (HBRPS)** marked a significant outcome of the Hackathon, demonstrating the potential of a scalable and fully indigenous cybersecurity prototype tailored for banking. Bank-ready solutions that align with regulatory and operational requirements.

- → Host-based ransomware protection systems (HBRPS) emerged as a scalable, indigenous cybersecurity prototype for banking systems.
- → It demonstrated how open-source frameworks and AI-powered insights can reduce dependence on costly foreign antivirus vendors.
- → The solution showcased bank-ready adaptability with dual detection modes and data-privacy compliant design.

Learnings

The Hackathon highlighted the need for resource-efficient cyber security solutions that can safeguard legacy banking infrastructure without degrading performance. Most importantly, the collaboration between academia and banks proved that combining research-driven innovation with sectoral expertise can generate practical and scalable cybersecurity solutions.

Future Plans

Looking ahead, the journey of Host-based ransomware protection systems (HBRPS) extends beyond the Hackathon into practical adoption and visibility at larger platforms. The solution is scheduled to be showcased at the Global Fintech Fest 2025, to be held from 7–9 October at the Jio World Centre, Mumbai.

Any Other Notable Points

The team has built a strong foundation with Host-based Ransomware Protection Systems (HBRPS) and plans to extend its capabilities beyond the hackathon. Future enhancements include expanding support to macOS, developing a centralized management system for fleet-wide monitoring, and integrating with enterprise SIEM tools. The solution also aims to leverage deep learning for zero-day detection, strengthen defenses with enhanced datasets and secure cloud updates, and provide advanced visualization dashboards for more granular insights and predictive threat analysis.

----xxx----