happiest minds
The Mindful IT Company
Born Digital . Born Agile

SECURING THE GOLD RUSH

Generative AI And The Evolving Landscape Of Banking Security

HOW GENERATIVE AI CAN TRANSFORM THE BANKING SECTOR?

Generative AI is rapidly becoming the new gold rush, with its potential to revolutionize industries like banking. In the next five years, Generative AI could fundamentally change financial institutions' risk management by automating, accelerating, and enhancing everything from compliance to climate risk control. As Generative AI transforms the banking sector, security and governance practices are also evolving to ensure responsible development and deployment. This includes measures to mitigate bias in AI models, protect sensitive financial data, and maintain transparency. The banking sector can prioritize these aspects by harnessing the immense potential of Generative AI while safeguarding its customers and the financial system.

WHAT ARE THE BIGGEST CHALLENGES BANKS ARE FACING IN THIS DIGITAL AGE?

Unauthorized Transaction

Promptly detecting unauthorized transactions like fraudulent transfers or account takeovers is crucial for banks.

Phishing Attack

Banks strive to prevent phishing attacks aimed at customers via deceptive emails or websites.

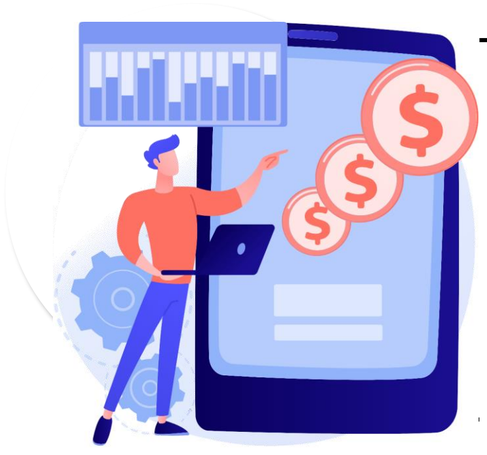
Fraudulent Loan Application

Identifying fraudulent loan applications, often submitted with falsified information or stolen identities, is imperative for banks.

Insider Threat

Banks confront risks from insiders like employees or contractors accessing sensitive data for malicious purposes.

HOW GENERATIVE AI CAN HELP WITH THE CHALLENGES



Real-Time Transactional Analysis

Generative AI leverages real-time data analysis to swiftly detect irregular patterns or deviations in transactions, enabling the rapid identification of potential fraudulent activities.

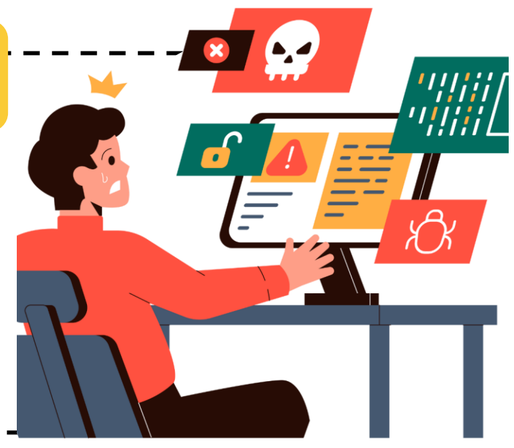
Advanced Phishing Detection

Generative AI analyzes email content, sender behavior, and website characteristics, effectively identifying and preventing phishing attempts before they compromise customer credentials.

Fraudulent Loan Application Detection

With advanced analytics, Generative AI meticulously scrutinizes loan application data to uncover anomalies and inconsistencies, facilitating the detection of fraudulent submissions.

Insider Threat Detection



Generative AI continuously monitors user activity logs and data access patterns, employing machine learning algorithms to pinpoint suspicious behavior indicative of insider threats, such as unauthorized data access or unusual activity, thereby enhancing security measures.

BUSINESS BENEFITS OF IMPLEMENTING GENERATIVE AI

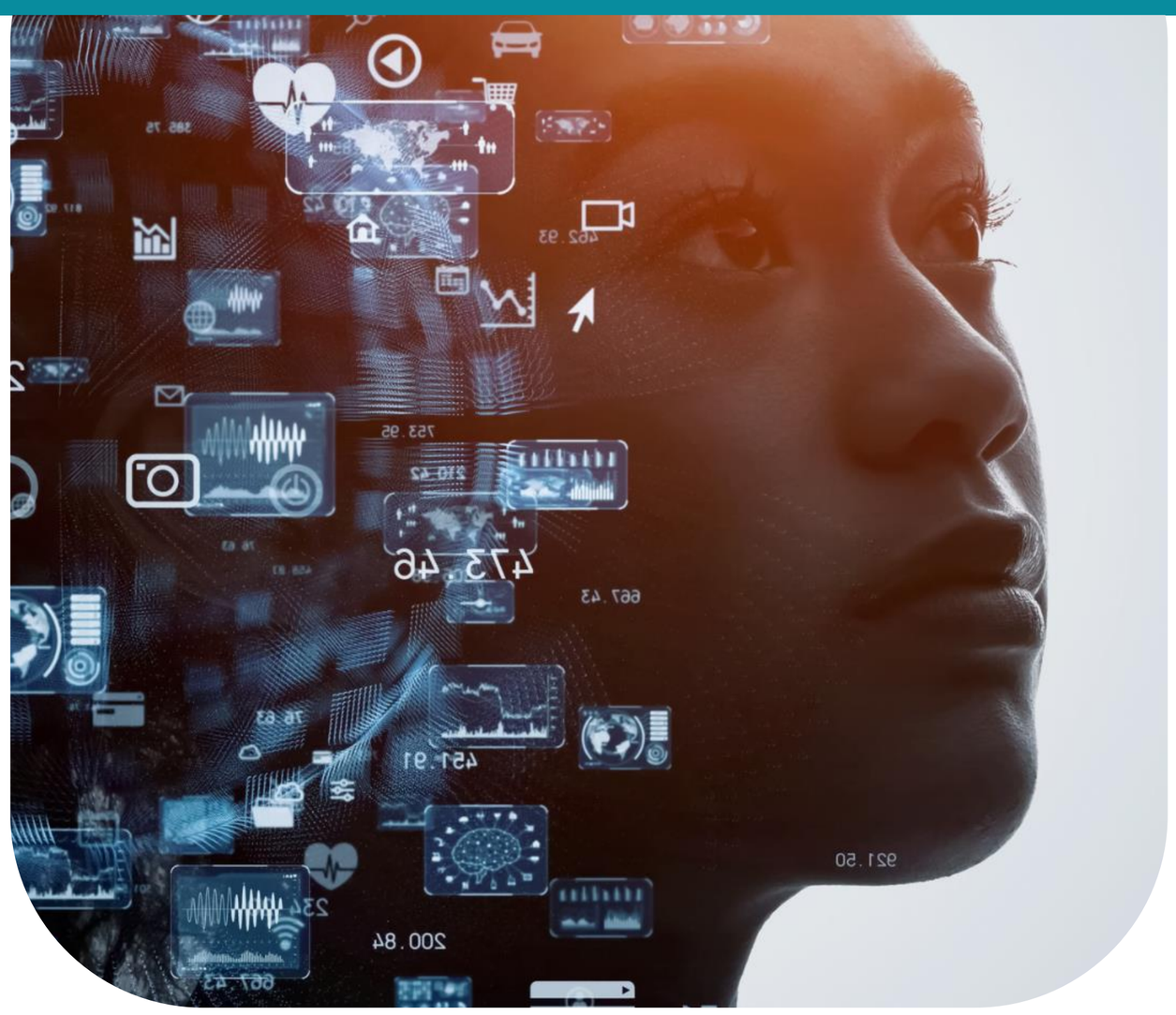
Financial Safeguarding *– Generative AI's swift detection and blocking of unauthorized transactions enable banks to safeguard finances, protect customer assets, and bolster trust in their services.*

Regulatory Compliance *- Proactive detection of insider threats assists banks in averting data breaches, safeguarding confidential information, and ensuring regulatory compliance.*

Risk Mitigation *- Accurate detection of fraudulent loan applications aids banks in mitigating default risks, reducing financial losses stemming from non-performing loans, and elevating the overall quality of their loan portfolios.*

Enhanced Security *- Proactively blocking phishing attempts with Generative AI ensures the prevention of customer account compromises and reduces fraud-related.*

GENERATIVE AI BASED SOLUTIONS



STREAMLINED UNDERWRITING & RISK ASSESSMENT

ChatGPT automates underwriting tasks like data entry and risk assessment, allowing underwriters to focus on innovation. Its neutrality reduces bias, ensuring fair treatment. With transparent decision-making, it integrates seamlessly with industry standards, improving quality and avoiding mistakes. By analyzing vast data, including unstructured sources like social media, ChatGPT tailors' coverages, improves premiums, and boosts customer satisfaction.

1

Structured Data	Unstructured Data
Property data, claims data, weather data, news articles, social media posts, customer reviews	

Integrate & Process Data - Data Lake

2

Decision Trees	Random Forest	Linear Regression	Logistic Regression	Support Vector Machines	Neural Networks
Identify variables that contribute to specific outcome	Multiple decision trees to generate better predictions	Estimate the relationship between variables	Predict binary outcomes	Likelihood of an event based on a set of variables	Handles large datasets. useful in image recognition

Traditional Machine Learning Model on Structured Data

3

GPT model analysis primarily on unstructured data

4

Comprehensive risk analysis report	Recommendations for specific risk mitigation measures	Insights into customer sentiment and concerns	Predictive modeling of future risks

Risk analysis outcome

FRAUD DETECTION

ChatGPT excels at fraud detection by analyzing claims data for patterns like repeated claims for the same damage or location. It spots suspicious behavior in customer interactions, like unusual requests or inconsistent claims. It also calculates claim risk scores using advanced analytics, helping insurers predict claim likelihood and costs, optimize resources, improve customer service, and reduce losses using techniques like regression analysis, decision trees, neural networks, and Bayesian algorithms.

Resolve and Consolidate Data

Create Data Strategy

Collected data includes personal identifiers (name, date of birth, contact info, social security numbers) and asset details (residential/commercial buildings, vehicles, farmland, etc.). It also encompasses policy specifics like coverage limits, deductibles, discounts, and billing arrangements.

Harness Business Rules

Feature Engineering

Insurers leverage various data sources like internal datasets, surveys, public records, and third-party databases to enhance claim risk scores. By blending these sources, they uncover hidden nuances and relationships.

Hybrid Predictive Monitoring for Fraud and Anomaly Detection

Innovative statistical techniques offer a competitive edge in crafting complex claim risk models. With its intricate calculations, machine learning uncovers hidden patterns, detects anomalies, and ranks risks, enhancing model sophistication.

Deploy and Validate Incoming Claims

Incorporate it directly into the claims management process by comparing the incoming claim with its corresponding risk score value.

happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

www.happiestminds.com

About Happiest Minds

Happiest Minds Technologies Limited (NSE: HAPPSTMNDS), a Mindful IT Company, enables digital transformation for enterprises and technology providers by delivering seamless customer experiences, business efficiency and actionable insights. We do this by leveraging a spectrum of disruptive technologies such as: artificial intelligence, blockchain, cloud, digital process automation, internet of things, robotics/drones, security, virtual/ augmented reality, etc. Positioned as 'Born Digital. Born Agile', our capabilities span Product & Digital Engineering Services (PDES), Generative AI Business Services (GBS) and Infrastructure Management & Security Services (IMSS). We deliver these services across industry groups: Industrial, Manufacturing and Energy & Utilities, Healthcare & Life Sciences, Retail, CPG & Logistics, Banking, Financial Services and Insurance (BFSI), Hi-Tech and Media & Entertainment, and EdTech. The company has been recognized for its excellence in Corporate Governance practices by Golden Peacock and ICSI. A Great Place to Work Certified™ company, Happiest Minds is headquartered in Bengaluru, India, with operations in the U.S., UK, Canada, Australia, and the Middle East.

Write to us at business@happiestminds.com