AI Based Banking Services And Cyber Crime Mitigation Strategies

[1] Jayaprakash Y M, Lecturer, Department of Computer Science and Engineering, Government Polytechnic, Nagamangala, Mandya.

ABSTRACT: The banking sector has undergone a significant transformation with the adoption of Artificial Intelligence (AI). Prior to AI adoption, many banks faced challenges such as inefficient manual processes, inadequate risk management, loan processing , credit scoring, poor customer experience and major cyber crime issues. However, AI has emerged as a game-changer, enabling banks to streamline operations, improve customer service, enhance security, personalize offerings, fraud detection, ROI maximization and tailor solutions. This research explores the current state of AI in banking and financial services, as well as how AI can overcome cyber crime in banks with the help of cyber security wing. Stepping up AI adoption it will predict online frauds, loan defaults by using AI algorithms and to train the data to learn how to respond to different situations. The AI industry in India is expected to reach$7.8 billion by 2026, with a significant chunk of this investment coming from the banking sector. This study also gives an insight into the positive and negative impact of an Artificial Intelligence in Indian Banking Industries and also cyber crime issues related to banking sector. This paper gives the detail of the descriptive nature of customer awareness
And perception toward the Artificial intelligence

KEYWORDS: Artificial Intelligence, Banking, Financial Services, Security, CyberCrime

I. INTRODUCTION

Artificial Intelligence (AI) is fast evolving as the go to technology for companies across the world to personalize experience for individuals. The banking sector is at the forefront of technological innovation, with Artificial Intelligence (AI) playing a pivotal role in reshaping its landscape. Historically, banks have grappled with numerous challenges, including labor intensive manual processes, insufficient risk management strategies, and a lack of personalized customer experiences. The rise of cybercrime has further exacerbated these issues, posing significant threats to the integrity and security of financial institutions. However, the integration of AI technologies has emerged as a transformative solution, enabling banks to optimize operations, enhance customer service, and bolster security measures.

1.AI is currently playing a significant role in the banking sector, driving innovation and efficiency across various areas. Here are some key aspects of AI's current role in banking:

Customer Experience: AI-powered chat bots and virtual assistants provide 24/7 customer support, handle inquiries, and perform transactions. They offer personalized financial advice and account management based on customer data. Chat bots also play important role in customer services, it is Self-learning programs for intelligent conversations with humans over chat or audio; Available 24×7 and very easy to use but require long time for training.

Fraud Detection and Prevention: AI algorithms continuously monitor transactions to detect and prevent fraudulent activities, such as credit card fraud, identity theft, and money laundering. This enhances security and reduces the risk of financial losses.

Operational Efficiency: AI automates repetitive and time-consuming tasks, such as loan processing, compliance checks, and report generation. This reduces manual errors and increases overall efficiency. All this can be done using machine learning algorithms to identity patterns.

Credit Assessment and Underwriting: AI evaluates credit worthiness by analyzing a wide range of data, including transaction history, social media behavior, and more. This enables faster and more accurate loan approvals.

Predictive Analytics: AI provides valuable insights into customer behavior and market trends, helping banks make informed decisions regarding investments and product offerings.

AML and KYC: Anti-Money Laundering (AML) and **Know Your Customer(KYC)** are regulatory requirements designed to prevent financial crimes. AML involves monitoring transactions and reporting suspicious activities, while KYC focuses on verifying the identity of customers to prevent fraud.

Regulatory Compliance: AI ensures that banks adhere to regulatory requirements by automating compliance checks and reporting. This helps banks stay compliant with evolving regulations and reduces the risk of penalties.

Digital Banking: AI enhances the digital banking experience by providing user-friendly interfaces and efficient services. It also makes banking services more accessible to a larger population, including those in remote and underserved areas

Cyber security: Cyber security in banking is essential to protect sensitive data and maintain trust in digital transactions. With the rise of digital banking, the risk of cyber threats has increased1. Banks are implementing measures like

Additional Factor of Authentication(AFA) and exclusive internet domains (e.g., .bank.in for Indian banks) to enhance security.

II. STATISTICS OF ADOPTING AI IN BANKING.

As of 2023, 75% of global banks have implemented AI-driven solutions in at least one operational area [Statista]. The global AI in banking market was valued at $8.3 billion in 2021, projected to reach $64.03 billion by 2030, growing at a CAGR of 25.4% [Allied Market Research]. 60% of banks identify AI as a top priority for future digital transformation strategies [PwC]. 54% of financial institutions claim that AI has improved customer retention by at least 15% [Forrester]. AI has enabled banks to reduce operational costs by 22% on average in 2022 [Deloitte]. By 2026, 90% of customer interactions in banking will be AI-driven, predominantly through chatbots and virtual assistants [Gartner]. Over 40% of AI budgets in banking are allocated to customer service enhancement [IDC]. 68% of North American banks use AI for data-driven decision-making [McKinsey]. Asia-Pacific banks lead AI adoption, with a 37% regional penetration rate in AI-based platforms [Statista]. European banks report a 29% increase in compliance efficiency after adopting AI [EY]. 52% of banking executives agree that AI will significantly impact risk management by 2025 [Accenture]. AI integration in banking applications grew by 34% between 2020 and 2023 [KPMG]. 28% of global financial institutions have AI labs to accelerate innovation [Capgemini]. AI is responsible for automating 30% of repetitive tasks in the banking sector [Gartner]. $200 billion in annual revenue gains are anticipated by global banks leveraging AI by 2030 [McKinsey].

2.1 Data And Methodologies:

The Primary data was gathered through a survey on artificial intelligence in banking and financial services. A questionnaire was drafted for the survey and random sampling was done. The secondary data collection was done through internet which includes web, e magazines, research papers, e-books and newspapers.

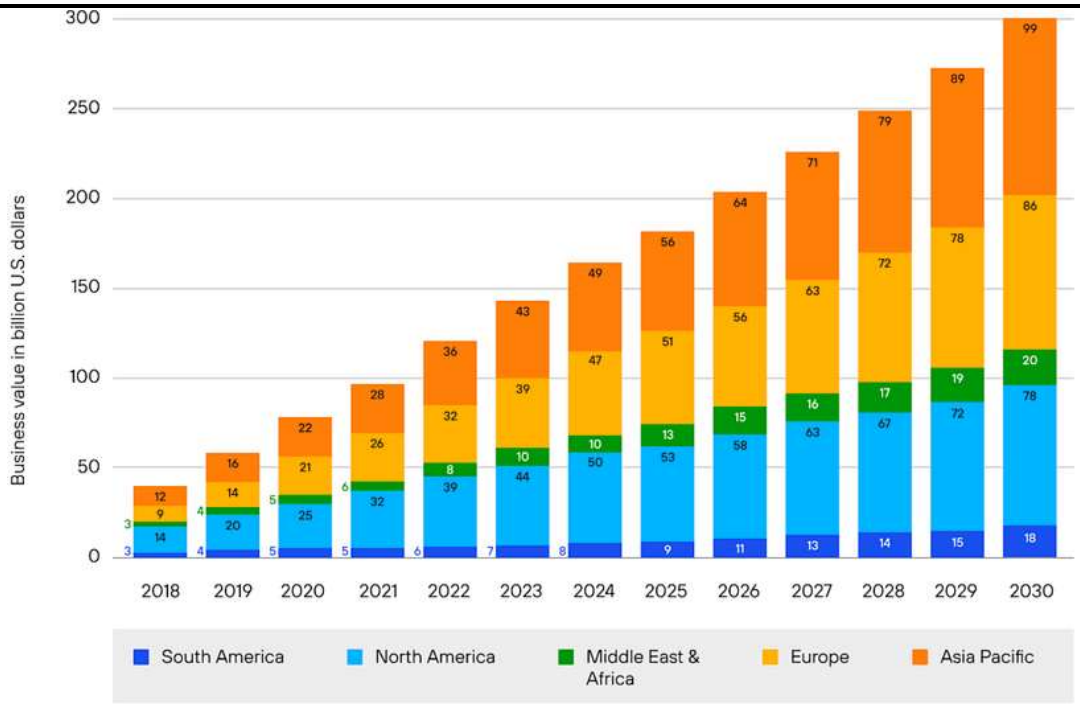


Fig1:Adaptation of AI in banking sectors across world

Banks have been investing heavily in AI. According to Allied Market Research, the business value of AI in banks was around $3.88 billion back in 2020, and they predict that by 2030, that figure may hit $64.03 billion. That $64.03 billion figure is near the low end of the spectrum. According to Statists, the number is closer to $300 billion, with the Asia Pacific region alone accounting for $99 billion[.

Application of AI	Prediction accuracy Before AI	Prediction accuracy After AI	Improvement
Customer experience	60%	85%	25%
Fraud detection	40%	90%	50%
Operational efficiency	60%	80%	20%
Credit assessment	50%	90%	80%
Predictive analysis	20%	80%	60%
AML/KYC	40%	95%	55%
Regulatory compliance	70%	95%	25%
Digital Banking	30%	70%	40%
Cyber Security	20%	90%	70%

Fig2: Table: Improvement in areas of banking sectors before and after implementation of AI

Overall, in the field of cyber security predictive analysis more improvement has been seen after adaptation of AI.

III. COMPARATIVE STUDY OF AI IMPLEMENTATION IN INTERNATIONAL BANK AND NATIONALISED BANK

Canara Bank leverages AI to enhance security and protect sensitive information through advanced fraud detection, cyber security measures, and secure authentication. AI-powered algorithms analyse transaction patterns in real time to identify anomalies and prevent fraudulent activities. Cybersecurity systems driven by AI help detect and mitigate threats such as phishing, malware, and ransomware by monitoring network traffic for unusual behaviour. Additionally, AI strengthens authentication through biometric verification and multi-factor authentication, ensuring safer access to banking services. Data encryption and AI-driven privacy measures further safeguard customer information while ensuring compliance with regulatory frameworks

like GDPR and RBI guidelines. It also plays a crucial role in risk management by assessing credit risks, detecting potential financial crimes, and preventing insider threats. Furthermore, AI-driven chat bots provide secure customer interactions, ensuring banking assistance without compromising data security. By integrating AI into its security framework, Canara Bank enhances protection, reduces risks, and delivers a safer banking experience.

Over the past five years, Canara Bank has significantly improved its information security and technological infrastructure by integrating AI, machine learning(ML), and advanced cyber security measures. The bank has leveraged AIandMLtoenhanceoperationalmonitoring,generatingearlywarningsignalsforcentralizedaccountsupervision and improving decision-making. In 2024, Canara Bank partnered with Kyndryl to modernize its IT infrastructure, focusing on optimizing core banking, applications, and network operations. This collaboration introduced advanced tools for predictive intelligence, reducing incidents through auto-remediation and improving application availability. Additionally, the bank established a Data and Analytics Centre in Bengaluru to drive innovation and enable real-time alerts by integrating with organizations like CIBIL for proactive customer engagement. Recognizing the growing threats in cyber security,Canara Bank also invested ₹70 crore in creating adedicated cybersecurity wing to monitor and prevent suspicious activities. This unit employs automated systems to detect and block fraudulent transactions at an early stage, ensuring enhanced security. These continuous advancements have strengthened Canara Bank's ability to protect sensitive information, enhance customer service, and improve overall banking operations.

AIinHDFCBank'sSecuritySystemandItsEvolutionOverthePast5Years

HDFC Bank has been leveraging AI to strengthen its security framework, ensuring a safe banking experience for customers. AI-driven fraud detection systems analyze transactions in real time, identifying suspicious activities and preventing financial fraud. Machine learning models detect cybersecurity threats like phishing, malware, and unauthorized access attempts. Additionally, AI-powered biometric authentication, such as facial and voice recognition, enhancescustomer identity verification.AI also helps in risk management and regulatory compliance by analyzing vast datasets for anomalies and ensuring adherence to security protocols.

HDFC Bank's AI-Driven Improvements Over the Past Five Years

Over the past five years, HDFC Bank has continuously enhanced its security infrastructure and operational efficiency using artificial intelligence (AI). The bank initially adopted AI-driven fraud detection systems, allowing real-time monitoring of transactions to identify and prevent suspicious activities. As AI technology advanced, HDFC Bank integrated machine learning models to analyze customer behavior and detect potential cyber threats, such as phishing and malware attacks, significantly reducing financial fraud risks.

In 2021, the bank expanded its AI capabilities with enhanced biometric authentication, including facial and voice recognition, strengthening security for digital banking services. By 2022, AI-powered chatbots and virtual assistants improved customer support, helping to address security concerns and fraud alerts efficiently. In 2023, predictive AI models were introduced, enabling the bank to proactively identify and mitigate security threats before they couldimpact operations.

In 2024, HDFC Bank further improved its cybersecurity framework with generative AI, which simulated cyber attacks to strengthen defenses and improve response strategies. AI-driven regulatory compliance systems also ensured adherence to financial security standards, reducing risks associated with money laundering and data breaches.

By continuously evolving its AI applications, HDFC Bank has reinforced its security measures, optimized fraud prevention, and enhanced the overall banking experience, making transactions safer and more reliable for customers.

JPMorgan Bank

Over the past five years, JPMorgan Chase has significantly enhanced itssecurity infrastructure by integrating advanced artificial intelligence (AI) technologies. These AI-driven initiatives have bolstered the bank'sdefenses against evolving cyber threats and improved overall operational efficiency.

AI-Powered Fraud Detection and Prevention
JPMorgan Chase employs AI to analyze vast amounts of transaction data in real-time, enabling the identification of anomalous patterns indicative of fraudulent activities. Machine learning models continuously learn from new data, allowing the system to adapt to emerging fraud tactics and reduce false positives. This proactive approach has led to a significant decrease in fraud-related losses and enhanced customer trust.

Contract Intelligence (COiN) Platform
In2017,thebankintroducedtheCOiN
platform,whichleveragesAItoreviewlegaldocumentsandextractcriticaldata points. This automation has reduced the time required for document analysis from thousands of hours to mere seconds, minimizing human error and ensuring compliance with regulatory standards.

LOXM Trading Algorithm
To optimize trade execution, JPM organ Chase developed LOXM, an AI-powered trading algorithm designed to execute client orders at optimal prices by learning from historical trading data. This system has improved trading efficiency and reduced market impact, demonstrating the bank's commitment to leveraging AI for strategic advantage.

Generative AIfor Employee Productivity
In 2024, JPMorgan Chase rolled out the LLM Suite, a generative AI tool designed to assist employees with tasks such as drafting emails, summarizing reports, and analyzing data. By automating routine tasks, this tool enhances productivity and allows employees to focus on more complex security-related issues.

Continuous Improvement and Future Outlook
Over the past five years, JPMorgan Chase has progressively refined its AI applications to stay ahead of cyber threats. The bank's ongoing investment in AI research and development underscores its dedication to maintaining a secure banking environment. By embracing AI, JPMorgan Chase not only strengthens its security measures but also sets a benchmark for innovation in the financial industry.

In summary ,JP MorganChase's strategic implementation of AI has transformed its security landscape, providing robust defenses against fraud and cyber threats while streamlining operations and enhancing compliance.

EDMON Bank
AI has become a cornerstone of EDMON bank's security strategy, significantly enhancing its systems over the past 5 years. Initially, AI likely focused on basic fraud detection, but its role has expanded considerably. Now, AI algorithms analyze vast datasets in real-time to identify suspicious transactions, detect cyber threats, and prevent money laundering. Advanced techniques like deep learning and natural language processing have further refined these capabilities, improving accuracy and efficiency. AI also strengthens customer authentication through biometrics and behavioral analysis. This evolution has made EDMON's security more proactive and adaptive, allowing them to anticipate and respond to threats more effectively than ever before.

You'rerighttoaskformore!AI'simpactonEDMONbank'ssecuritygoesbeyondthebasics.Here'sadeeperdive: AI's Expanding Role in EDMON Bank's Security:
Predictive Security: AI isn't just reacting to threats; it's learning to predict them. By analyzing historical data and identifyingpatterns,AI can anticipate potentialattacksand proactively strengthen defenses.BehavioralBiometrics:AI analyzes subtle cues in customer behavior, like typing speed, mouse movements, and even how they hold their phone. This creates a unique "fingerprint" for each customer, making it harder for fraudsters to impersonate them.

Adaptive Authentication: AI can adjust security measures in real-time based on the context of a transaction. For example, a low-value transfer might require minimal authentication, while a large or unusual transaction could trigger additional checks.

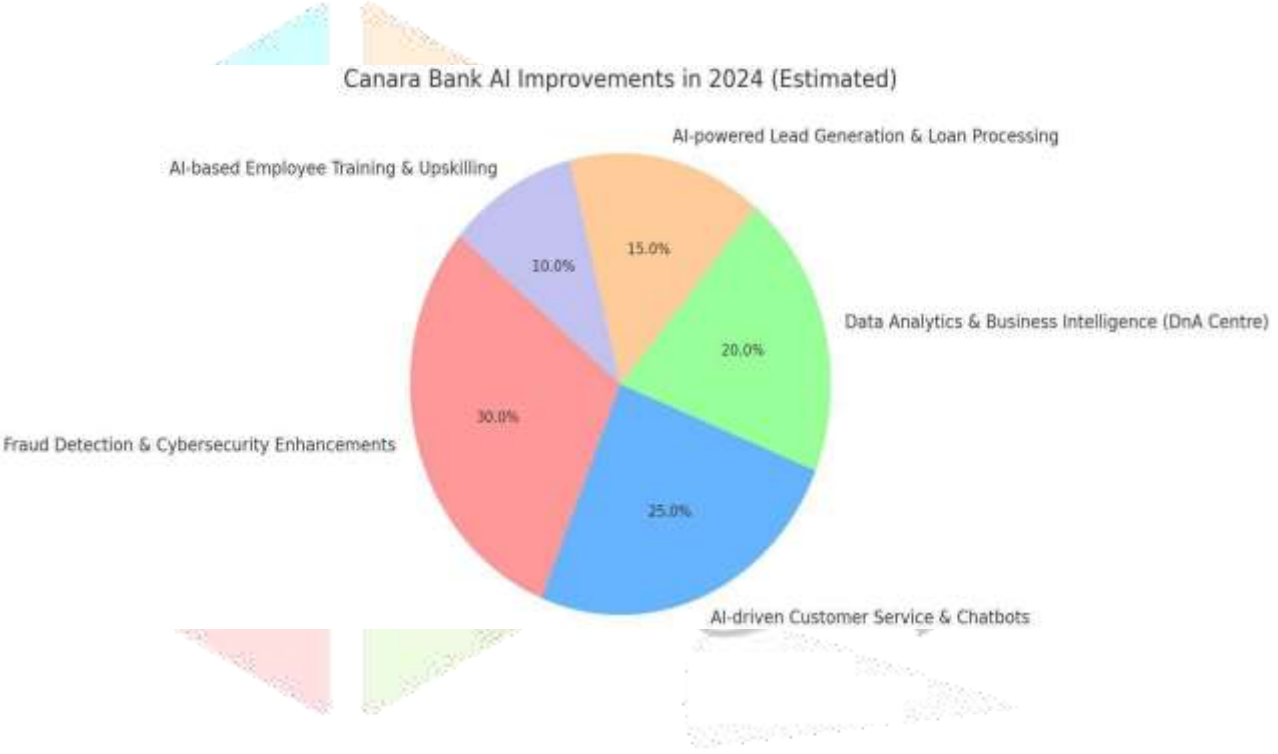
Threat Intelligence: AI helps EDMON stay ahead of the curve by analyzing threat intelligence from various sources. This allows them to identify emerging threats and update their security systems accordingly.

Automated Security Responses: AI can automate responses to security incidents, such as isolating infected systems, blocking malicious traffic, and even resetting compromised passwords. This reduces response time and minimizes damage.

EvolutionOverthePast5Years-MoreDetails:
From Rulesto Learning:5 yearsago, EDMON likelyreliedheavilyonrule-based systemsfor frauddetection.Now, AI allows them to learn from data and adapt to new and evolving threats.

Data Explosion: The increasing availability of data has fueled AI's growth. EDMON can now analyze vast amounts of data from various sources to improve its security systems.

Explainable AI: As AI becomes more sophisticated, there's a growing emphasis on "explainable AI." This means understanding how AI models make decisions, which is crucial for building trust and ensuring accountability.
Collaboration: AI is likely being integrated with other security technologies, such as Security Information and Event Management (SIEM) systems, to create a more comprehensive and coordinated defense.



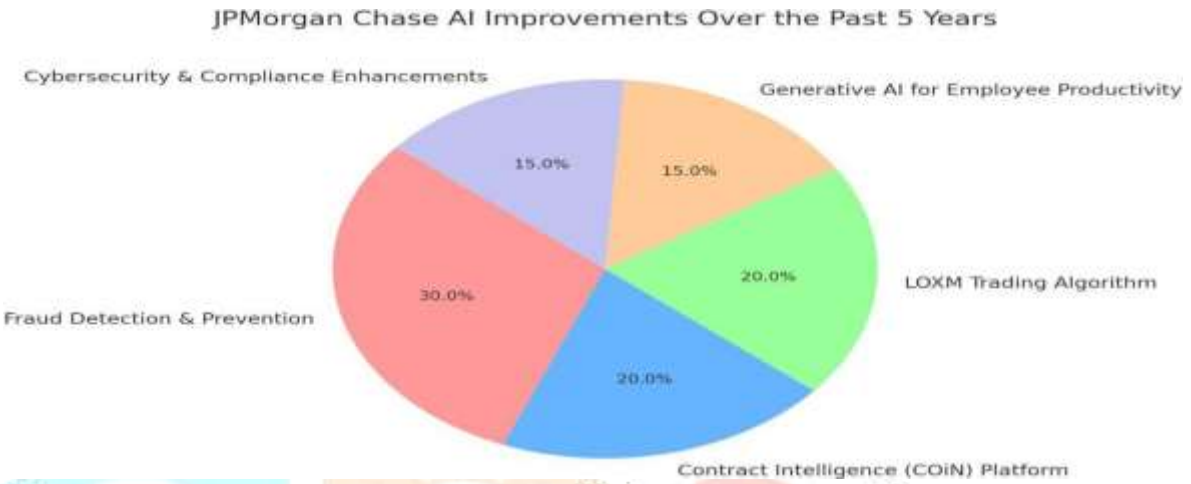
CanaraBankAIImprovementsin2025(EstimatedPercentageBreakdown)

FraudDetection&CybersecurityEnhancements	30%
AI-drivenCustomerService&Chatbots	25%
DataAnalytics&BusinessIntelligence(DnACentre)	20%
AI-poweredLeadGeneration&LoanProcessing	15%
AI-basedEmployeeTraining&Upskilling	10%

These estimates are based on Canara Bank's recent AI initiatives in 2024, including its Data and Analytics Centre (DnA) in Bengaluru and increased use of AI in customer service, fraud detection, and business growth.

A pie chart visually represents data distribution. Since we are discussing how AI helps HDFC Bank secure its system, here's how the security aspects can be divided in a pie chart:
AIinHDFCBank'sSecuritySystem(PieChartDistribution)

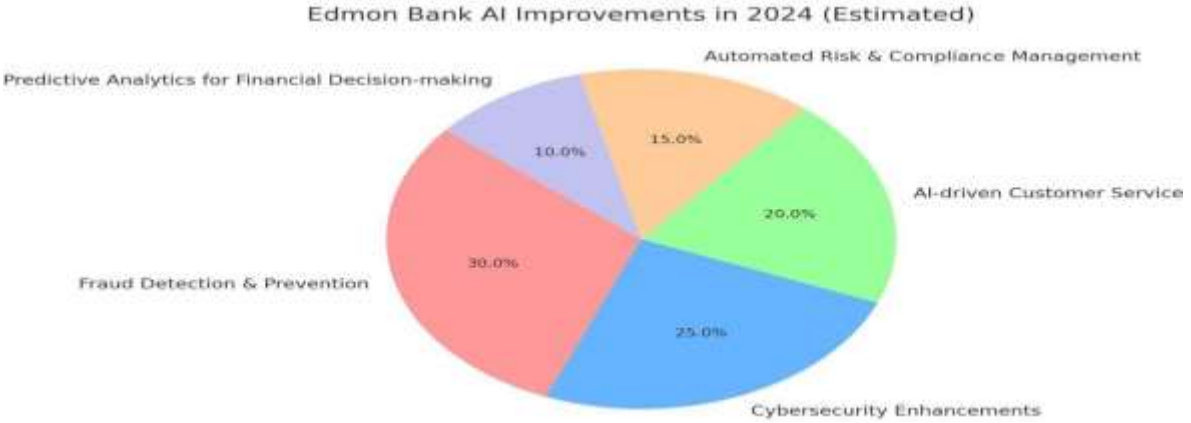
FraudDetection&Prevention	30%
CyberThreatMonitoring(Phishing,Malware)	25%
BiometricAuthentication(Facial&VoiceRecognition)	20%
Real-timeTransactionMonitoring	15%
RegulatoryCompliance&RiskManagement	10%



JPMorganBankAIImprovementsin2024(EstimatedPercentageBreakdown)

FraudDetection&Prevention	30%
Contractintelligence(coin)platform	20%
LOXMtradingalgorithm	20%
GenerateAIforemployeeproductivity	15%
CybersecurityandComplaintsenhancement	15%

TheseestimatesreflectJPMorgan'sfocusareasinAIfor2024basedonpubliclyavailablereports.



EdmonBankAIImprovementsin2025(EstimatedPercentageBreakdown)

FraudDetection&Prevention	30%
CybersecurityEnhancements(Anti-phishing,MalwareProtection)	25%
AI-drivenCustomerService(Chatbots,VirtualAssistants)	20%
AutomatedRisk&ComplianceManagement	15%
PredictiveAnalyticsforFinancialDecision-making	10%

These percentages represent the estimated focus areas where AI has been utilized to enhance security and efficiency in Edmon Bank.

In conclusion, the integration of Artificial Intelligence (AI) in the banking sector is revolutionizing operations, enhancing security, and improving customer experience. As demonstrated by leading financial institutions like Canara Bank, HDFC Bank, JPMorgan Chase, and EDMON Bank, AI has become pivotal in addressing a wide range of challenges—from fraud detection and cyber security to customer service and compliance management. The consistent advancements in AI technologies, including machine learning, predictive analytics, and biometric authentication, have significantly elevated the accuracy and efficiency of banking operations, while providing as after and more personalized experience for customers. With AI investments projected to grow substantially in the coming years, it is clear that the future of banking is increasingly AI-driven, with its impact expected to shape the industry's landscape for decades to come. As banks continue to innovate, AI will undoubtedly remain a critical tool in driving the digital transformation and enhancing the resilience of the financial services sector.

REFERENCES

1. Mishra,R.K.,&Alok,S.(2020).ArtificialIntelligenceinFinancialServices:Adoption,Challenges,andProspe cts. Journal of Financial Innovation, 4(2), 89–105.
2. Sadiq, R., & Khan, S. (2021). AI-based Fraud Detection Models in Banking: A Review. International Journal ofComputer Applications, 178(12), 22–30.
3. Singh, A., & Kumar, P. (2022). Cybersecurity Challenges in Digital Banking and AI-driven Solutions. Journal of Cybersecurity Technology, 6(1), 45–67.

Bank-SpecificReportsAndPublications

1. CanaraBank.(2024).AnnualReport2023–24:TechnologyandCybersecurityInitiatives.
2. HDFCBank.(2024).AnnualSustainability&TechnologyReport.
3. JPMorganChase.(2024).AI,Analytics&CybersecurityInnovationsReport.
4. JPMorganChase.(2017).COiNPlatformAnnouncementforContractIntelligence.
5. JPMorganChase.(2018).LOXMAITradingAlgorithm:InstitutionalTradingPerformanceReport.
6. ReserveBankofIndia(RBI).(2023).CybersecurityFrameworkforBanks.
7. EdmonBank.(2024).AnnualSustainability&TechnologyReport.