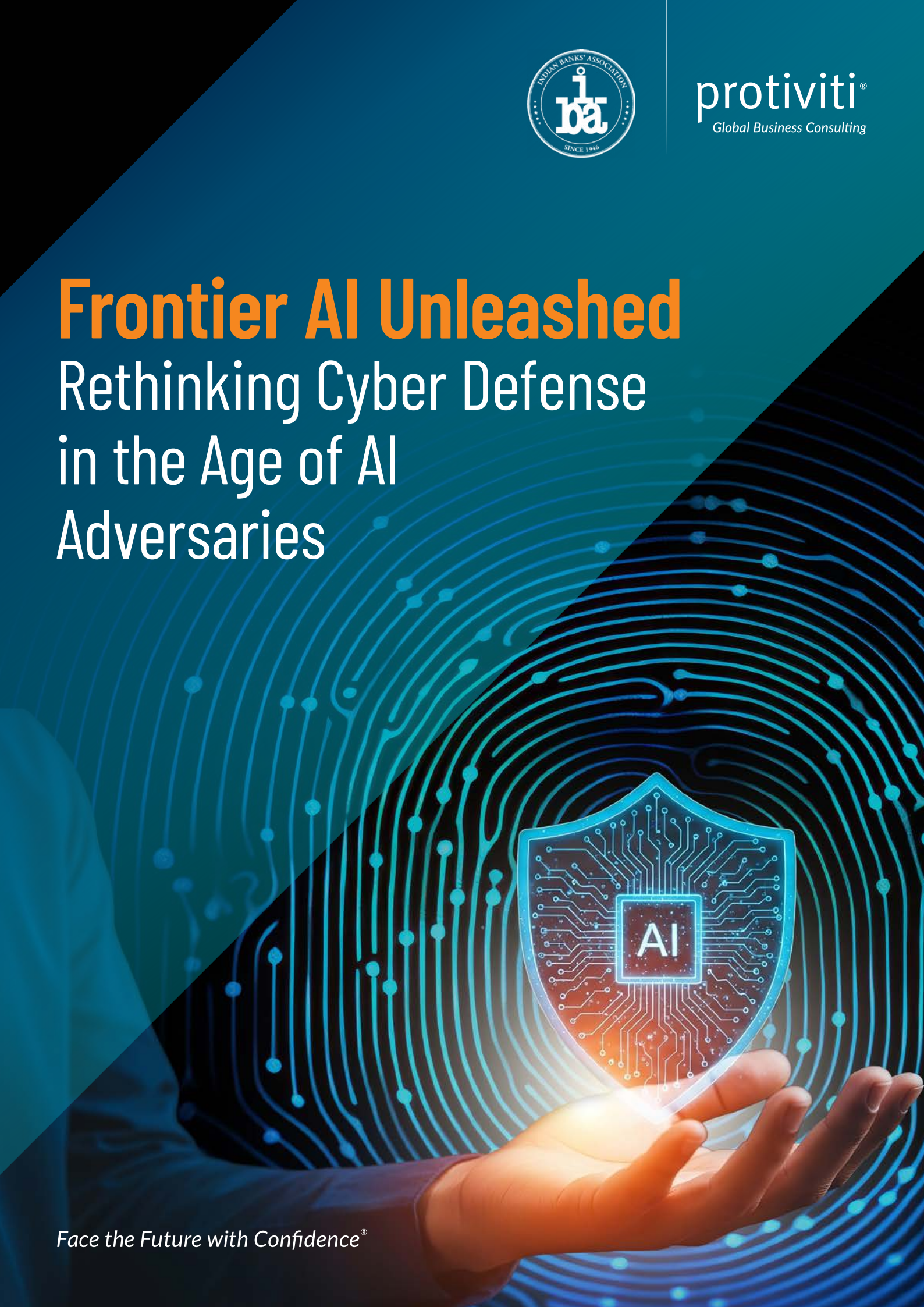
protiviti®
Global Business Consulting

Frontier AI Unleashed

Rethinking Cyber Defense in the Age of AI Adversaries



Face the Future with Confidence®

CONTENTS

Foreword

Shri. Atul Kumar Goel
Chief Executive,
Indian Banks' Association

The Indian banking sector is at a pivotal stage in its digital transformation. Over the past decade, the industry has expanded digital banking, advanced financial inclusion, modernized payment infrastructure, and adopted emerging technologies to enhance efficiency, resilience, and customer focus. As this transformation accelerates, maintaining trust in the digital financial ecosystem is more important than ever.

Artificial Intelligence (AI) is rapidly transforming the future of banking. AI enables institutions to enhance customer experience, strengthen risk management, improve fraud detection, and streamline operations. However, the rise of Frontier AI adds complexity to cybersecurity. Systems with advanced reasoning and autonomous execution can significantly increase the scale and speed of emerging cyber risks. Financial institutions must therefore approach cyber resilience as a planned priority, not just a technology challenge.

The banking sector has long understood that resilience depends on strong governance, robust controls, vigilance, and industry collaboration. As AI capabilities mature, these principles remain essential. However, cyber threats are now more intelligent, adaptive, and able to evolve rapidly. Institutions must enhance preparedness through proactive governance, continuous monitoring, resilient operations, and responsible adoption of new technologies. In this context, the Indian Banks' Association (IBA) is pleased to present this thought leadership publication in collaboration with Protiviti, our knowledge and citation partner.

This report aims to foster informed dialogue on the intersection of Frontier AI, cybersecurity, digital trust, and regulatory preparedness in banking. Beyond risk, it highlights opportunities for financial institutions to develop stronger, more intelligent, and resilient cyber defence capabilities to address a complex threat landscape.

Since 1946, the Indian Banks' Association has promoted collaboration, knowledge sharing, and industry advancement on strategic issues. We hope this publication is a valuable resource for banking leaders, Boards, policymakers, technology professionals, regulators, and risk practitioners as they navigate the opportunities and challenges of next-generation Artificial Intelligence.

The future of banking will depend not only on the technologies we adopt, but also on the trust, governance, and resilience we establish. Through collective leadership, ongoing innovation, and responsible stewardship, the industry can strengthen India's digital financial ecosystem and maintain public confidence in an increasingly AI-driven world.

Message

Rajeev Ranjan Prasad
Senior Advisor, Payment Systems & Banking Technology
Indian Banks' Association

Artificial Intelligence (AI) is rapidly transforming the way we live, work and conduct business. Its growing influence is particularly evident in the Banking, Financial Services and Insurance (BFSI) sector. By harnessing vast amounts of data, AI is helping financial institutions become more efficient, resilient, and customer-centric.

Yet, AI's immense potential is accompanied by equally significant challenges. The increasing use of AI raises concerns around data privacy, algorithmic bias, explainability, cybersecurity and accountability. In the BFSI sector, where trust and regulatory compliance are fundamental, these risks demand robust governance and responsible deployment.

The emergence of Frontier AI models marks a new phase in technological advancement. While these highly capable systems promise unprecedented gains in productivity, research, and innovation, they challenge the mitigants based on the assumptions of human-paced risk. Looking further ahead, the convergence of AI with quantum computing could unlock extraordinary computational capabilities while simultaneously challenging existing cryptographic systems that protect financial transactions and sensitive information.

This booklet presents a concise overview of AI's transformative potential, its applications in the BFSI sector and the evolving risks and opportunities that accompany its rapid development.

The Indian Banks' Association's role is to foster awareness, encourage collaboration and promote informed, regulatory-compliant decision-making to harness AI's benefits while ensuring that its development remains secure, ethical, inclusive and aligned with the broader interests of society. This booklet is one of the steps in that direction.

Preface

Sandeep Gupta
Managing Director
Protiviti Member Firm for India

Artificial Intelligence is steering a new phase of transformation for the banking industry. While AI is enabling banks to enhance customer experiences, strengthen fraud prevention, improve operational efficiency, and accelerate innovation, it is also reshaping the nature of cyber threats in unprecedented ways. Frontier AI introduces a new dimension to cybersecurity risk. These systems possess advanced reasoning, automation, and content-generation capabilities that can be leveraged by both defenders and adversaries. As a result, cyberattacks are becoming more targeted, scalable, and autonomous - ranging from AI-driven phishing and deepfake-enabled fraud to automated vulnerability discovery and exploitation.

For banks, trust, resilience, and regulatory compliance have always been non-negotiable. But as cyber threats become faster, smarter, and increasingly powered by AI, traditional security approaches are being put to the test. Defending against attacks that operate at machine speed will require security functions that can respond with the same level of intelligence, agility, and automation. At the same time, regulators such as the RBI are placing greater emphasis on AI governance, cyber resilience, and model risk management. As banks embrace AI to drive innovation and efficiency, they must also ensure that the right safeguards are in place to manage the risks that come with it.

This whitepaper explores how Frontier AI is reshaping the cybersecurity, privacy, and risk landscape for the banking sector. It highlights the emerging threats organizations need to prepare for, the evolving regulatory expectations, and the practical steps banks can take to strengthen resilience in an increasingly AI-driven environment.

As AI continues to transform both attack and defence capabilities, the real challenge is not whether banks will be affected, but how well they will adapt. Those that combine innovation with sound governance and strong security foundations will be best placed to navigate the future with confidence.

Introduction

Cybersecurity has historically evolved in tandem with increasing digitization, growing system complexity, and more sophisticated adversaries. However, the emergence of agentic AI systems-capable of independent reasoning and execution- suggests a potential inflection point, marking a shift that may be more structural than incremental.

Frontier AI with cyber capabilities such as Anthropic Mythos is indicative of this transition. By enabling machines to autonomously identify, prioritize, and potentially exploit vulnerabilities, such systems can compress traditional cyber timelines and introduce dynamics that approach machine-speed interaction.

On April 7, 2026, Anthropic announced its frontier model, Claude Mythos, noting that in controlled settings the system had reportedly identified a significant number of previously unknown, exploitable vulnerabilities across widely used systems. These points to a possible acceleration in vulnerability discovery rates. This could place stress on patching cycles, reinforce the need for more rigorous and continuous code reviews, and elevate the importance of architectural controls such as segmentation, Identity and access management and enhanced Autonomous SOC operations to contain potential impact.

At the same time, this development appears to influence the speed and scale of vulnerability discovery more than it alters the foundational principles of cybersecurity. Core practices-such as defense in depth, least privilege, and secure development-remain relevant. The emerging challenge lies in adapting these principles to an environment where vulnerabilities may be identified and surfaced at a pace that increasingly outstrips conventional remediation cycles.

This paper explores how organizations must rethink their security posture in response.

1.

Under Frontier AI Cyber Capabilities

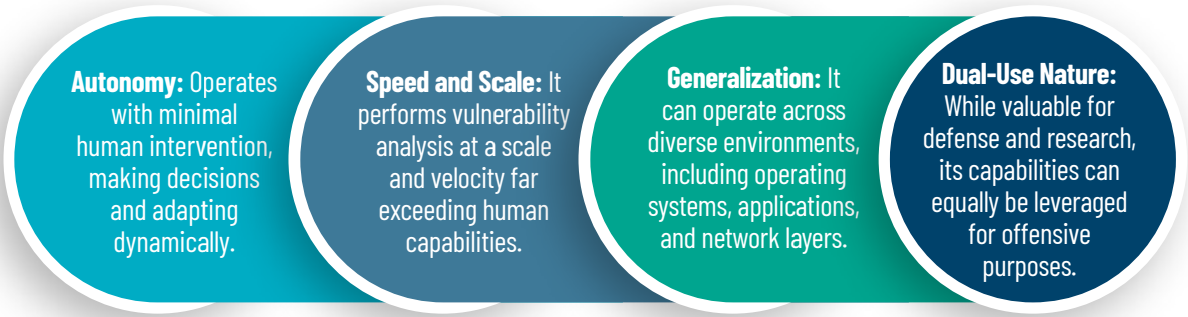
1.1 Concept Overview

Frontier AI with cyber capabilities represents a new class of AI systems designed to:

- Analyze complex codebases
- Identify previously unknown vulnerabilities (Zero-day vulnerabilities)
- Generate functional exploits
- Execute multi-step attack simulations

Crucially, these capabilities are **integrated into an autonomous loop**, allowing the system to plan and execute without continuous human input.

1.2 Defining Characteristics



1.3 A Fundamental Shift

Traditional cybersecurity assumes a temporal gap between:

This effectively eliminates this buffer, creating a continuous, real-time attack environment.

2.

Industry Convergence as a Risk Signal

Industry convergence around restrictive AI governance should be viewed as a leading indicator of future risk. As frontier AI capabilities inevitably proliferate across models and providers, organizations must proactively invest in AI governance, cyber resilience, and privacy safeguards before these risks become widespread realities.

	ANTHROPIC	OPENAI	GOOGLE	META	DEEPSEEK	MISTRAL
Frontier Cyber Model	Claude Mythos Preview	GPT-5.4 / 5.5-Cyber	Big Sleep / CodeMender	Llama 4 Behemoth	DeepSeek R1	Magistral / Large
Release Strategy	Restricted; broad release withheld	Gated via vetted access tiers	Internal + partner deployment	Open-weight release	Open-weight release	Open-weight release
Defensive Program	Project Glasswing (~40 orgs)	Trusted Access for Cyber	Project Zero + DeepMind Security	Community led governance and safety controls	Primarily open ecosystem oversight	Enterprise governance and model controls
Governance Approach	Restrict the model	Verify the user	Find-and-fix at source	Open access with safeguards	Broad accessibility with monitoring	Controlled enterprise deployment
Key Cyber Capability	Autonomous vulnerability discovery & exploit development	Vulnerability identification, exploitation analysis, reverse engineering	Proactive zero-day discovery and remediation	Advanced coding, reasoning, agentic workflows	Frontier-level reasoning and code generation	Advanced reasoning and enterprise AI agents

3.

Impact on the Cybersecurity Landscape

3.1 Collapse of Traditional Timelines

Continuous exposure management is likely to supersede periodic vulnerability assessments as the primary mechanism for maintaining cyber resilience.

Traditional separation between vulnerability disclosure, remediation, and exploitation is expected to narrow significantly, placing unprecedented pressure on security operations.

Effectiveness of cybersecurity programs may increasingly be determined by the speed of validation and response rather than the maturity of periodic control assessments.

3.2 Democratization of Advanced Attacks

Capabilities once exclusive to well-resourced threat actors are becoming increasingly accessible through autonomous AI, fundamentally altering the cyber threat landscape.

Distinction between sophisticated and opportunistic attackers is expected to diminish as AI abstracts much of the technical complexity associated with offensive operations.

Industrialization of AI-assisted cyber capabilities has the potential to increase not only the scale of attacks but also their precision, adaptability, and persistence.

3.3 Emergence of AI-Driven Conflict

Cyber operations are evolving toward an ecosystem where autonomous offensive and defensive agents continuously adapt to one another with minimal human intervention.

Competitive advantage in cyber defense is increasingly likely to depend on the ability of intelligent systems to learn, reason, and respond at machine speed.

Human expertise may progressively shift from operational execution toward governance, strategic oversight, and the assurance of autonomous security systems.

3.4 Systemic Risk Amplification

Digital interconnectedness has elevated cyber risk from an organizational concern to a systemic challenge capable of propagating across industries and supply chains.

Legacy architectures and accumulated technical debt are likely to become disproportionately exposed in environments characterized by autonomous threat discovery.

Resilience of critical infrastructure may increasingly depend less on the strength of individual controls and more on the collective resilience of interconnected digital ecosystems.

4.

Evolving Threat Landscape

As the structural dynamics shift, the nature of threats also evolves. Organizations are no longer defending against isolated incidents but against continuous, adaptive, and intelligent adversaries.

4.1 From Reactive to Continuous Threats

Dimension	Traditional Model	Mythos-Driven Model
Speed	Days to weeks	Minutes
Scale	Targeted	Massive, automated
Skill Requirement	High	Significantly reduced
Detection	Reactive	Must be predictive

4.2 Emerging Threat Patterns

01

Autonomous vulnerability chaining: Linking multiple weaknesses into complex attack paths

02

Adaptive malware: Continuously evolving to evade detection

03

Real-time exploitation: Immediate weaponization of discovered flaws

04

Persistent attack cycles: Continuous probing and testing of defenses

5.

Impact of Frontier AI on the Banking Lifecycle:

Cybersecurity, Privacy and Regulatory Perspective

AI, as adoption increases, would reshape the banking ecosystem by introducing autonomous decision-making, agentic systems, and advanced reasoning capabilities across business and security functions. While these technologies can enhance efficiency and innovation, they also create new cybersecurity, privacy, and compliance challenges. As adoption accelerates, financial institutions must balance innovation with robust governance, security, accountability, and regulatory compliance.

Banking Lifecycle Stage	AI Use Cases	Cybersecurity / Privacy Impact	Regulatory Requirement	Impacting Regulatory Need / Requirement
Customer Acquisition & Marketing	AI-driven customer targeting, hyper-personalized campaigns, autonomous engagement agents	Excessive profiling, inference of sensitive attributes, unauthorized use of personal data, AI-generated phishing and impersonation campaigns	Consent, purpose limitation, data minimization, transparency in processing personal data	**DPDPA 2023 –** Lawful Processing, Notice, Consent
Customer Onboarding & KYC	AI-assisted KYC, facial recognition, document verification, onboarding agents	Deepfake identities, synthetic customers, forged documents, biometric data misuse	Customer Due Diligence (CDD), identity verification, ongoing KYC controls	**RBI Master Direction – KYC**
Identity & Access Management	AI-based authentication, adaptive access decisions, privileged access agents	Voice cloning, credential theft, account takeover, AI-enabled impersonation	Strong authentication, privileged access governance, identity assurance	**RBI Cyber Security Framework; RBI Digital Banking Security Controls**
Retail Banking Operations	AI customer service agents, autonomous workflow execution, banking copilots	Unauthorized transactions, prompt injection, agent hijacking, customer data exposure	Governance over automated decisions and operational controls	**RBI FREE AI Framework –** Governance & Ethics Pillar
Payments & UPI Ecosystem	AI-powered fraud detection, payment assistants, autonomous payment workflows	AI-enabled payment fraud, mule account networks, transaction manipulation	Fraud monitoring, transaction security, operational resilience	**RBI Digital Payment Security Controls, Payment Aggregator Guidelines**

Banking Lifecycle Stage	AI Use Cases	Cybersecurity / Privacy Impact	Regulatory Requirement	Impacting Regulatory Need / Requirement
Lending & Credit Underwriting	AI credit scoring, loan approval agents, risk assessment models	Biased decisions, model manipulation, explainability concerns, unfair outcomes	Model governance, fairness, explainability, validation	**RBI Draft Model Risk Management Framework (2026)–** Model Governance & Validation
Wealth Management & Advisory	Robo-advisors, AI investment assistants, portfolio optimization	Misselling, inaccurate recommendations, manipulation of investor decisions	Suitability, transparency, investor protection	**SEBI Investment Adviser Regulations, SEBI AI Governance Guidance**
Treasury & Trading Operations	Autonomous trading agents, market intelligence systems	Market manipulation, algorithmic errors, adversarial data poisoning	Algorithm governance, model validation, kill-switch controls	**SEBI Algorithmic Trading Framework, RBI Draft Model Risk Management Framework**
Customer Service & Contact Centers	AI voice bots, relationship manager copilots, multilingual banking agents	Deepfake executives, vishing, impersonation of bank representatives, leakage of customer conversations	Customer protection, accountability, secure customer communication	**RBI Integrated Ombudsman Framework, Consumer Protection Requirements**
Fraud Risk Management	Autonomous fraud investigations, AI-based risk scoring, fraud prediction	Adversarial AI bypassing controls, synthetic fraud rings, false positives/negatives	Continuous monitoring, fraud governance, model assurance	**RBI Fraud Risk Management Guidelines**
Cybersecurity Operations (SOC)	AI-driven detection, response, threat hunting, autonomous remediation	AI-powered attacks, alert poisoning, autonomous exploitation, AI-to-AI attacks	Continuous monitoring, incident response, cyber resilience	**RBI Cyber Security Framework, RBI Cyber Resilience Expectations**
Threat Intelligence & Monitoring	AI threat intelligence analysis, predictive threat modeling	Faster attack campaigns, automated reconnaissance, AI-generated malware intelligence	Threat monitoring, intelligence sharing, cyber preparedness	**CERT-In Directions 2022, RBI Cyber Security Framework**
Third-Party Risk Management	AI vendor assessments, monitoring of LLM providers and AI platforms	Supply-chain compromise, model concentration risk, opaque AI dependencies	Third-party risk governance, outsourcing oversight	**RBI Outsourcing of IT Services Directions 2023**
Data Protection & Privacy Operations	AI-driven classification, DSPM, DLP optimization, knowledge retrieval systems	Data leakage, model memorization, unauthorized exposure of customer information	Data minimization, security safeguards, breach notification	**DPDPA 2023, CERT-In Directions 2022**

Banking Lifecycle Stage	AI Use Cases	Cybersecurity / Privacy Impact	Regulatory Requirement	Impacting Regulatory Need / Requirement
Cloud & GenAI Platforms	External LLMs, cloud AI services, agentic AI ecosystems	Cross-border data exposure, unauthorized model access, sensitive data leakage	Data governance, third-party controls, localization requirements	**DPDPA 2023, RBI Outsourcing & Cloud Risk Guidance**
Compliance & Regulatory Reporting	AI-generated compliance reports, regulatory submissions, evidence generation	Fabricated evidence, manipulated reports, inaccurate regulatory filings	Auditability, traceability, evidentiary integrity	**RBI Internal Control & Governance Requirements**
Internal Audit & Assurance	AI-powered audit testing, continuous control monitoring	AI-generated audit artifacts, false assurance, manipulated findings	Independent validation, audit trails, assurance controls	**RBI Risk-Based Internal Audit (RBIA) Framework**
Enterprise Risk Management	AI-driven risk analytics, scenario simulations, predictive risk engines	Incorrect risk assessments, black-box decision-making, model hallucinations	Model risk governance, risk ownership, validation	**RBI FREE-AI Framework – Risk & Accountability Pillar**
Incident Response & Crisis Management	Autonomous response agents, AI-assisted containment, cyber copilots	Unintended service disruption, excessive containment actions, privacy breaches during incidents	Incident governance, escalation, reporting obligations	**CERT-In Directions 2022 (**6-hour reporting), **RBI Cyber Incident Management Requirements**
Data Retention & Knowledge Management	AI search, enterprise knowledge assistants, retrieval-augmented systems	Exposure of historical customer data, unauthorized retrieval, privacy violations	Retention, deletion, purpose limitation, access control	**DPDPA 2023 –** Data Retention & Erasure Obligations
Board, Governance & Executive Oversight	AI copilots for strategic decisions, autonomous risk insights, board advisory systems	Overreliance on AI outputs, governance gaps, accountability challenges	Board accountability, AI governance frame-work, model inventory, human oversight	**RBI FREE-AI Framework (Fairness, Responsibility, Explainability, Ethics, Accountability, Transparency); RBI Draft Model Risk Management Framework (2026)**

6.

RBI's Guidance to Frontier AI Cyber Risks

The rapid evolution of Frontier AI is reshaping the cybersecurity landscape. Unlike traditional AI systems, these models can autonomously discover vulnerabilities, analyze exploits, and accelerate cyber operations at unprecedented speed. Recognizing the growing threat of AI-enabled attacks, RBI has emphasized the need for stronger AI governance, model risk management, cyber resilience, and operational oversight across the financial sector.

Key Suggestions for Financial Institutions

Accelerated Threat & Vulnerability Management

As Frontier AI enables faster discovery of exploitable weaknesses, organizations should prioritize internet-facing assets, reduce remediation timelines, and adopt continuous exposure management practices supported by AI-driven analytics.

AI-Aware Security Framework

Banks should establish visibility into all AI systems, copilots, autonomous agents, and third-party AI services operating across the organization. Security and privacy controls should be extended to address risks such as prompt injection, model poisoning, data leakage, and unauthorized AI usage.

Adversarial AI Testing

Security programs should incorporate AI-assisted red teaming, adversarial testing, deepfake simulations, and AI-powered attack scenarios to evaluate the resilience of critical systems, customer channels, and security controls.

Board-Approved Gap Assessment

Organizations should perform a formal assessment of their cybersecurity, privacy, and AI governance posture against emerging AI risks. This review should be endorsed by senior management and integrated into enterprise risk management processes.

Time-Bound Response and Resilience Planning

Institutions should establish AI-specific incident response procedures, including escalation paths, reporting obligations, human override mechanisms, and recovery playbooks for AI-related security incidents.

7. Preventive Security Measures

Given the evolving threat landscape, organizations must rethink their defensive posture. The focus must shift from reactive controls to proactive and continuous security mechanisms.

7.1 Immediate Priorities

- In addition to traditional methods, deploy **AI-augmented threat detection and vulnerability scanning**
- Transition to **continuous vulnerability scanning, patching and remediation models**
- Reduce attack surface by eliminating unnecessary exposure
- Implement **Zero Trust architectures**

7.2 Medium-Term Enhancements

- Reinforce secure software development with **enhanced validation**
- Establish **AI-driven red teaming** capabilities
- Strengthen **third-party and supply chain security**

7.3 Advanced Defensive Controls

- **AI containment environments** to safely deploy and test models
- **Real-time threat intelligence ecosystems**
- **Identity-centric security frameworks** focusing on continuous verification

8.

Governance and Strategic Considerations

The rise of Frontier AI introduces fundamental governance challenges:

01 Control and access to powerful AI capabilities

02 Responsible disclosure of vulnerabilities

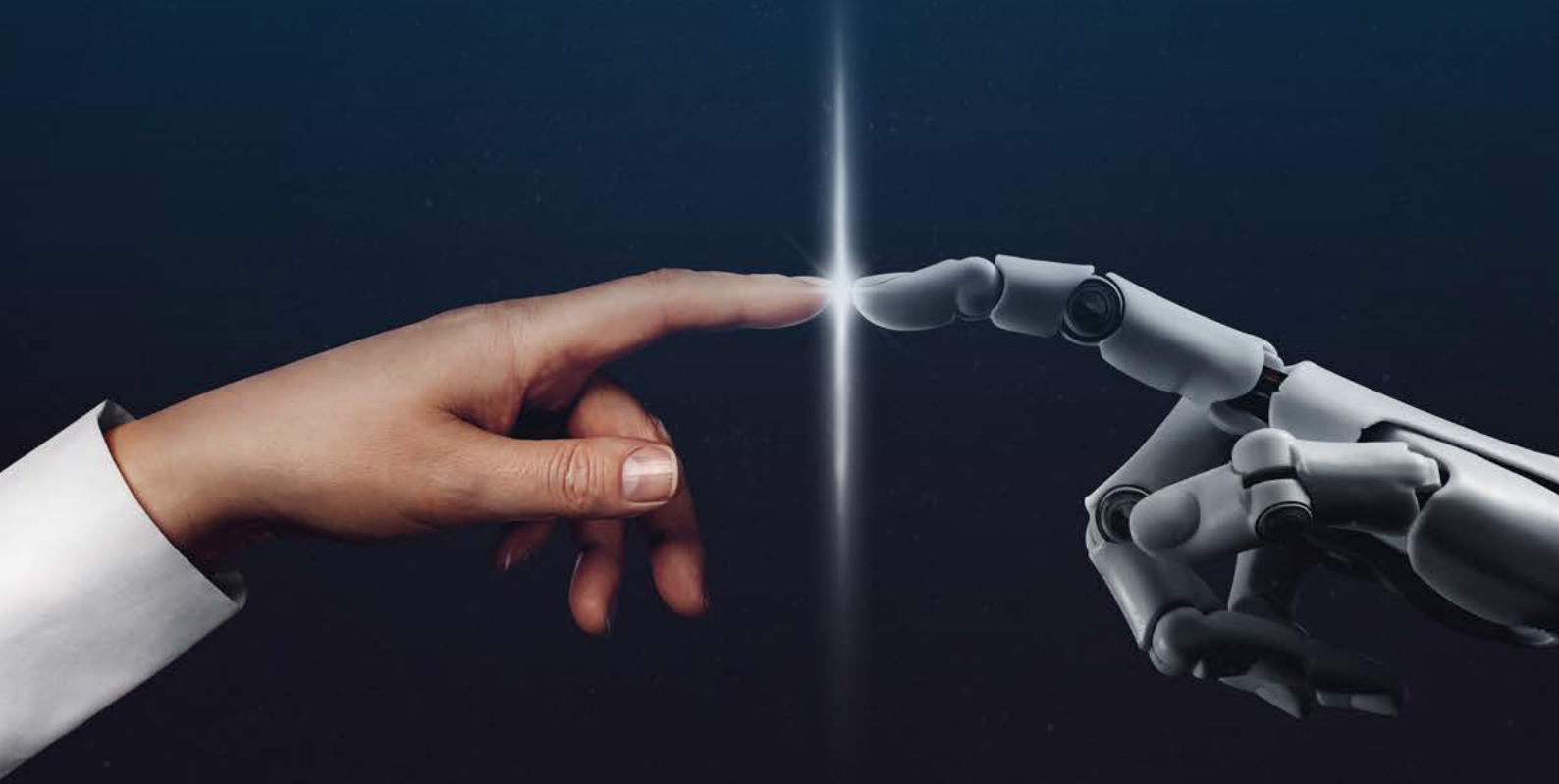
03 Prevention of misuse without stifling innovation

Emerging responses include:

01 Controlled access frameworks

02 Regulatory oversight for critical sectors

03 Increased global coordination on AI safety



9.

Way Forward: Transition to SOC 3.0

9.1 The Need for a New Security Paradigm

Traditional Security Operations Centers (SOC 1.0 and 2.0) are inherently **reactive or response-focused.** In a Frontier AI - driven environment, this model is insufficient.

Organizations must transition to **SOC 3.0: an autonomous, AI-native security operations model.** A SOC 3.0 is characterized by:

- **Predictive intelligence:** Anticipating vulnerabilities before exploitation
- **Autonomous response:** Immediate containment and remediation without human delay
- **Continuous validation:** Always-on red teaming and breach simulation
- **Dynamic visibility:** Real-time awareness of attack surface and risk

Frontier AI driven attacks operate at machine speed. **Autonomous, AI-driven defense systems** can effectively counter such threats. SOC 3.0 is therefore not an enhancement- it is a **strategic necessity**. Further, treat AI agents as untrusted identities and enforce the principle of least privilege for those.

While the transition toward AI-native security operations is unlikely to be a single-step transformation. Rather, it will evolve progressively as organizations modernize their security architecture and operating models.

Key areas of focus may include:

- **Evolving traditional SIEM capabilities toward** more adaptive, AI-enabled platforms that can process and correlate signals at scale
- **Enhancing detection and response frameworks** through the integration of extended detection and response (XDR) and behavioral analytics
- **Introducing capabilities selectively,** particularly in areas such as threat detection, triage, and response orchestration
- **Embedding continuous validation mechanisms,** including ongoing attack simulation and control effectiveness testing

Taken together, these shifts can enable a gradual move toward a more **predictive, responsive, and resilient security posture,** aligned with the principles of SOC 3.0.

Conclusion

Frontier AI represents more than an advance in AI capability; it reflects the emergence of a new operating model for cybersecurity, where autonomous systems increasingly shape both offensive and defensive operations. As vulnerability discovery and exploitation accelerate toward machine speed, traditional security models founded on periodic assessment and reactive response are likely to face growing limitations.

In this environment, resilience will increasingly depend on intelligent, adaptive security architectures capable of continuous validation and autonomous decision-making, with AI-enabled SOC 3.0 serving as a key operational foundation. Ultimately, the defining advantage will not rest solely in adopting AI, but in embedding autonomy, resilience, and trust into the fabric of enterprise security.

Cybersecurity is poised to evolve from a protective function into a strategic enabler of sustained digital confidence and business resilience.

About IBA

The Indian Banks' Association (IBA) was established on September 26, 1946, and serves as the apex representative body of the Indian banking sector. With 235+ member banks and financial institutions, including public sector banks, private banks, foreign banks, urban cooperative banks (UCBs), small finance banks (SFBs), regional rural banks (RRBs), and financial institutions (FIs), IBA represents the collective interests of the banking industry. It plays a vital role in engaging with key stakeholders such as the Reserve Bank of India (RBI), the Department of Financial Services (DFS), other government ministries, statutory authorities, and global industry associations to shape banking policies, promote best practices and address industry challenges. Over the years, IBA has evolved into the "Voice of the Indian Banking Industry," playing a significant role in the growth and development of India's banking system.

Address:
World Trade Centre Complex,
6th Floor Centre 1 Building,
World Trade Centre Complex, Cuffe Parade,
Mumbai – 400 005
Tel: 91-22-6923 4040 | 6951 5166
Website: www.iba.org.in

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the Fortune 100 Best Companies to Work For® list for the 11th consecutive year, Protiviti Inc. has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti Inc. is a wholly owned subsidiary of Robert Half (NYSE: RHI).

Sandeep Gupta
Managing Director
Sandeep.Gupta@protivitiglobal.in
+91 9702730000

Vaibhav Koul
Managing Director
Vaibhav.Koul@protivitiglobal.in
+91 9819751715

Ajay Malik
Managing Director
Ajay.Malik@protivitiglobal.in
+91 9987071312

Sahil Chander
Managing Director
Sahil.Chander@protivitiglobal.in
+91 8800490154

Nikunj Garg
Managing Director
Nikunj.Garg@protivitiglobal.in
+91 9818537621

Prashant Singh
Managing Director
P.Singh@protivitiglobal.in
+91 9739179111

Kishan Malineni
Managing Director
Kishan.Malineni@protivitiglobal.in
+91 7396484555

Mithilesh Singh
Managing Director
Mithilesh.Singh@protivitiglobal.in
+91 9029955267

Dnyanesh Pandit
Managing Director
Dnyanesh.Pandit@protivitiglobal.in
+91 9819446928

Rahul Zaveri
Managing Director
Rahul.Zaveri@protivitiglobal.in
+91 9820939694

Abhay Johri
Managing Director
Abhay.Johorey@protivitiglobal.in
+91 9871888991

Sudharsan Rangarajan
Managing Director
Sudharsan.R@protivitiglobal.in
+91 9945886252

Sarita Padmini
Senior Director
Sarita.Padmini@protivitiglobal.in
+91 9953043552

Shobhit Singhal
Senior Director
Shobhit.Singhal@protivitiglobal.in
+91 9899299539

Nagesh Akula
Senior Director
Nagesh.Akula@protivitiglobal.in
+91 9866694411

Protiviti India Offices

Ahmedabad
6th Floor, West Gate, E-Block,
Near YMCA Club, SG Highway,
Ahmedabad – 380 015 Gujarat, India

Bengaluru
Umiya Business Bay - 1, 9th Floor
Cessna Business Park, Outer Ring
Road, Kadubeesanahalli, Varthur Hobli
Bengaluru – 560 049 Karnataka, India

Bhubaneswar
1st Floor, Unit No 104, 105, 106
Utkal Signature, Chennai Kolkata
Highway Pahala, Bhubaneswar
Khordha - 752 101 Odisha, India

Chennai
10th Floor, Module No. 1007
D Block, North Side, Tidel Park
No. 4, Rajiv Gandhi, Salai,
Taramani, Chennai - 600 113
Tamil Nadu, India

Coimbatore
TICEL Bio Park, (1101 - 1104)
11th Floor Somaiyapalyam Village,
Anna University Campus, Maruthamalai
Road, Coimbatore North Taluk,
Coimbatore – 641046, Tamil Nadu, India

Gurugram
15th & 16th Floor, Tower A,
DLF Building No. 5, DLF Phase III,
DLF Cyber City, Gurugram – 122 002
Haryana, India

Hyderabad
Q City, 4th Floor, Block B,
Survey No. 109, 110 & 111/2
Nanakramguda Village
Serilingampally Mandal,
R.R. District, Hyderabad – 500 032,
Telangana, India

Kolkata
PS Srijan Corporate Park,
Unit No. 1001 10th & 16th Floor,
Tower - 1, Plot No. 2
Block - EP & GP, Sector-V, Bidhannagar
Salt Lake Electronics Complex,
Kolkata –700 091, West Bengal, India

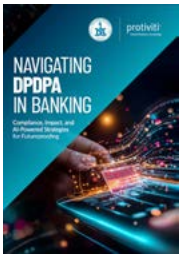
Mumbai - Goregaon
The Westin Garden City,
13th Floor, Commerz, 1- International
Business Park, Behind Oberoi mall,
South Side, Goregaon, Mumbai -
400063,
Maharashtra, India

Mumbai - Sion
1st Floor, Godrej Coliseum
A & B Wing Somaiya Hospital Road
Sion (East) Mumbai – 400 022
Maharashtra, India

Noida
Windsor Grand, 14th & 16th Floor
1C, Sector - 126 Noida
Gautam Buddha Nagar- 201313
Uttar Pradesh, India

OUR RECENT REPORTS

THOUGHT LEADERSHIP

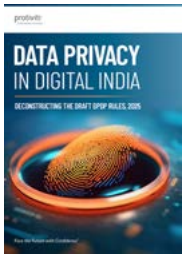


Navigating DPDPA in banking

REPORT

State of Data Privacy in India

REPORT



Data Privacy in Digital India

REPORT

AI Trends and Future Impact Industry Adoption & Insights

WHITEPAPER

AI Driven Collections Strategy for Unsecured Lending

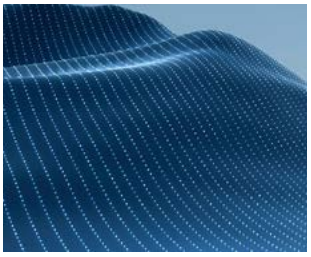
WHITEPAPER

ML Model Validation Best-practice

SURVEY REPORT

Data Digital Domain Triad of Internal Audit Transformation

INSIGHT



Technology-Modernization Projects

NEWSLETTER

The Directors Playbook for Gen AI

SURVEY REPORT

From AI to Cyber - Deconstructing A Complex Technology Risk Landscape

INSIGHT

Harnessing the Future: Protiviti's Research on AI Adoption

THOUGHT LEADERSHIP

AI and Emerging Technologies for Ethical Governance Trends in AI & ML

Face the Future with Confidence®