European Economic Letters
ISSN 2323-5233
Vol 15, Issue 4 (2025)
http://eelet.org.uk

From Chanakya's Arthashastra to Industry 5.0: A Neo-Vedic Framework for E-Banking Cybersecurity in the Indian Legal System

Prof JP Yadav

Director, School of Legal studies, CGC University Mohali,

Corresponding Author: Dr Gagandeep Kaur,

Senior Associate Professor in Law, School of Law, UPES

Dr Gurdeep Kaur,

HoD, School of legal studies, CGC University Mohali

Mr Amit Singh,

Assistant Professor, School of legal studies, CGC University, Mohali

Abstract

Cybersecurity in e-banking has become a critical concern in India's financial sector, demanding robust legal and strategic frameworks. This paper explores a *neo-Vedic* approach to cybersecurity by drawing parallels between ancient principles from Chanakya's *Arthashastra* and the demands of modern Industry 5.0 technologies. Through doctrinal legal analysis and comparative framework evaluation, authors examined how age-old wisdom on governance, espionage, and statecraft can inform contemporary cyber defense strategies. Authors analyzed current Indian cybersecurity statutes – including the Information Technology Act of 2000 (and its amendments), Reserve Bank of India (RBI) guidelines, and emerging data protection laws – in the context of e-banking. Balancing historical-philosophical foundations with modern technological elements (such as Artificial Intelligence (AI) and the Internet of Things (IoT) under Industry 5.0), authors proposed a *Neo-Vedic* cybersecurity framework. This framework emphasizes ethical duty (*dharma*), strategic intelligence (*chanakya-neeti*), and collaborative defense, aligning ancient principles with cutting-edge practices. The analysis highlights gaps in the current legal regime and offers recommendations to strengthen India's cyber law architecture for banking. The study concludes that integrating timeless strategic wisdom with modern technological safeguards can enhance cyber resilience in e-banking, fostering a secure digital banking environment consistent with Indian cultural values and international best practices.

Keywords: Arthashastra; Cybersecurity; E-Banking; Industry 5.0; Indian Cyber Law; Chanakya; AI; IoT; Data Protection; Neo-Vedic Framework.

Introduction

Modern electronic banking (e-banking) systems operate in an environment of unprecedented technological complexity and risk. The rise of Industry 5.0 that is characterized by human-centric integration of advanced technologies like AI, IoT, robotics, and big data – has transformed banking services, but also expanded the cyber threat surface (Breque *et al*., 2021). Indian banks increasingly use AI-driven chatbots, biometric authentication, and IoT-connected devices, offering efficiency and personalization. However, these advancements come with *evolving cybersecurity challenges*, including sophisticated malware, phishing attacks, data breaches, and AI-driven fraud. In 2022–2023 alone, India's Computer Emergency Response Team (CERT-In) recorded over 1.3–1.5 million cybersecurity incidents, many targeting the financial sector (Bharadwaj, 2025). The financial loss from data breaches in India's banking industry reached an average of $2.18 million in 2023, a sharp rise over recent years (Reserve Bank of India [RBI], 2023). Such statistics underscore the urgency for resilient cybersecurity frameworks tailored to the banking context.

Amid these modern threats, there is value in looking to *ancient wisdom* for foundational principles of security and governance. Over two millennia ago, Chanakya (also known as Kautilya), the chief advisor to Emperor Chandragupta Maurya, authored the *Arthashastra* – a treatise on statecraft, economics, military strategy, and law. The *Arthashastra* offers detailed prescriptions on securing a kingdom's assets, intelligence gathering, fortification of defenses, and administering

justice. It notably emphasizes that a ruler's foremost duty (*rajadharma*) is to protect the state and its people through any means necessary, including espionage, strict law enforcement, and ethical governance (Gautam, 2021). Chanakya's insights into crime and punishment exhibit a remarkably pragmatic understanding: he documented numerous offenses and suggested that as society evolves, new forms of crime emerge, requiring adaptive responses (Jeph & Vijaywargia, 2023). For example, Chanakya anticipated that technological or societal changes would create novel criminal opportunities, a prescient observation echoed today as the digital revolution spawns cybercrime (Jeph & Vijaywargia, 2023). The enduring relevance of the *Arthashastra* in strategic thinking has been acknowledged in modern Indian defense and governance discourse (Gautam, 2018; Kanwal, 2016). This suggests that *historical-philosophical foundations* could inform contemporary cybersecurity strategies, especially in a culturally rich context like India's.

This paper thus bridges ancient and modern paradigms by proposing a Neo-Vedic framework for e-banking cybersecurity. By "Neo-Vedic," authors imply a modern reinterpretation of Vedic and classical Indian principles (as encapsulated by Chanakya's *Arthashastra* and related texts) to address the challenges of the Industry 5.0 era. This paper perform a doctrinal analysis of current Indian cyber laws and regulations governing banking, and compare them with strategic tenets from the *Arthashastra*. The objectives of this study are threefold: (1) to elucidate the parallels between Chanakya's strategic wisdom and modern cybersecurity best practices; (2) to critically analyze the existing Indian legal framework for e-banking security (statutes, regulations, and guidelines) in light of these principles and international norms; and (3) to formulate recommendations for strengthening cybersecurity governance in India's banking sector by integrating ancient insights with modern technology governance.

The remainder of this paper is organized as follows. The Methodology section outlines the research approach, which is rooted in doctrinal (legal textual) analysis and comparative historical analysis. Authors then delve into the **Historical-Philosophical Foundations** derived from the *Arthashastra*, distilling key principles relevant to security and governance. Next, it eamined the Industry 5.0 Technological Landscape in Banking, describing how AI, IoT, and other innovations shape cybersecurity risks. The Indian Cybersecurity Legal Framework section discusses current laws (such as the Information Technology Act, RBI guidelines, and data protection regulations) and their efficacy in addressing e-banking cyber risks. A Comparative Analysis section then juxtaposes the Arthashastra's approach to security with modern legal and technical frameworks, highlighting synergies and gaps. Authors propose the Neo-Vedic Cybersecurity Framework for E-Banking, articulating how ancient principles can be operationalized alongside contemporary measures. Finally, paper provide Conclusions and Recommendations, suggesting policy and legal reforms for a more secure e-banking ecosystem in India, guided by both past wisdom and future needs.

Methodology

This research adopts a doctrinal and comparative methodology. A doctrinal approach is used to analyze legal texts, including statutes, regulatory guidelines, and case law relevant to cybersecurity in India's banking sector. Key legislative instruments (e.g., Information Technology Act 2000/2008, RBI circulars, and the Digital Personal Data Protection Act 2023) are examined to discern their provisions, scope, and limitations regarding e-banking security. Authors also review secondary sources such as academic journals (IEEE, ScienceDirect, law reviews) and authoritative reports to contextualize how these laws function in practice.

Comparatively, the study employs a historical-comparative framework: it compares principles from the *Arthashastra* (and broadly, ancient Vedic norms of governance) with contemporary cybersecurity frameworks. Textual analysis of the *Arthashastra* (English translations and scholarly interpretations) is performed to extract themes pertinent to information security, espionage, risk management, and legal control of wrongdoing. These themes are then mapped to modern cybersecurity concepts. For instance, Chanakya's emphasis on espionage and counterintelligence is compared with today's cyber threat intelligence and intrusion detection mechanisms. Table 1 (in the subsequent section) provides a structured comparison of such analogues. The comparative analysis is also extended geographically – albeit briefly – by referencing international standards (like ISO 27001, NIST framework, GDPR, etc.) to gauge how India's cybersecurity legal posture aligns with global best practices and where improvements are needed.

No human subjects or empirical fieldwork were involved; the research is purely analytical, drawing from literature and law. This *interdisciplinary approach* (merging law, history, and technology) allows for a rich exploration of how enduring

strategic insights can complement legal norms. The methodology is inherently qualitative, focusing on interpretation of texts and synthesis of ideas across time periods. By combining doctrinal legal research with a comparative historical lens, the paper crafts a novel perspective – a Neo-Vedic framework – that is both rooted in Indian philosophical heritage and attuned to the realities of cutting-edge cyber technology. Ensuring rigor, all claims are supported with citations from credible sources (academic publications, official reports, or primary legal documents). The APA in-text citation style is used for scholarly consistency. Ultimately, this methodology aims to yield a holistic understanding of e-banking cybersecurity that transcends a purely technical or legal view, incorporating ethical and strategic dimensions from one of India's oldest knowledge traditions.

Historical-Philosophical Foundations: Insights from *Arthashastra*

Chanakya's *Arthashastra* (4th century BCE) is one of the world's earliest comprehensive treatises on governance and law. Though written for an ancient empire, it contains remarkably systematic thinking about security, economics, espionage, and jurisprudence that can inspire modern policy. In the context of safeguarding the state (or by analogy, a financial system), several key *Arthashastra* concepts stand out:

- **Dandaniti (Rule of Law and Punishment):** Chanakya advocated *dandaniti* – the science of punishment – as essential to governance. The *Arthashastra* enumerates crimes ranging from theft and fraud to treason, and prescribes calibrated punishments to deter wrongdoing (Gautam, 2021). Crucially, it supports differential sanctions: the punishment should fit the crime's severity and the offender's context, to maintain order and justice (Jeph & Vijaywargia, 2023). Chanakya also emphasized compensating victims for their losses, showing a victim-centric approach (Jeph & Vijaywargia, 2023). In modern cyber law, we see echoes of *dandaniti* in provisions that penalize hacking, data theft, and online fraud with fines and imprisonment, as well as mechanisms (like damages under IT Act Section 43A) to compensate data breach victims. The ancient principle reinforces the idea that a well-defined legal deterrent and enforcement of consequences are foundational to security be it a kingdom's or a bank's information systems.

- **Matsya Nyaya (Protection of the Weak):** *Arthashastra* warns against *matsya nyaya*, the "law of the fishes," meaning in an anarchic situation the big fish devour the small (Rangarajan, 1987, commentary). Chanakya insisted that a strong sovereign (or governing framework) must prevent this by protecting the vulnerable. Transposed to cybersecurity, this implies that the state and institutions have a *dharma* (duty) to protect citizens and customers (the "small fish") from powerful threat actors (cybercriminals, hackers – the "big fish"). This principle resonates with modern expectations that banks must safeguard consumers from fraud and that governments must crack down on cybercrime networks. It underpins the concept of cyber justice: ensuring the digital realm is not a lawless jungle but a governed space where even the weakest users' rights are protected.

- **Intelligence and Espionage (Surveillance and Threat Intelligence):** Chanakya famously built an elaborate **spy network** for the Mauryan Empire, using agents to gather intelligence on threats, be it enemy plots or internal conspiracies. He distinguished between *sabotage, espionage,* and *counterintelligence*, valuing information as a weapon of war (Gautam, 2021). In the Arthashastra, covert measures and surveillance were legitimized to preempt threats and maintain state security. The modern analog in cybersecurity is threat intelligence and monitoring. Just as Chanakya's spies would infiltrate and report on enemy plans, today's banks deploy Security Operations Centers (SOC) with real-time monitoring, intrusion detection systems, and cyber threat intel feeds to detect and foil attacks in their early stages. Honeypots and deception technologies used to lure and identify attackers mirror the *counterespionage* tactics advocated by Chanakya (Kulkarni, 2024). Moreover, the Arthashastra's counsel to test loyalty of officials and guard against insider betrayal translates to modern insider threat programs and zero-trust architectures that "trust no one" by default in a network (Kulkarni, 2024). The enduring lesson is the proactive gathering of information and readiness to act on it, which is central to both ancient statecraft and contemporary cybersecurity best practices.

- **Fortification and Defense in Depth:** In ancient times, fortifying one's city or citadel – through walls, moats, and guards – was paramount. Chanakya detailed how forts should be constructed and defended at multiple layers (Rangarajan, 1987). This concept of *layered defense* has direct relevance to protecting digital assets. Modern

cybersecurity espouses a Defense-in-Depth strategy, wherein multiple layers of security controls (firewalls, encryption, multi-factor authentication, network segmentation, etc.) protect systems such that if one layer is breached, others still stand (Kulkarni, 2024). It is observed that *Arthashastra's* influence in the idea that relying on a single line of defense is folly; resilience comes from depth and redundancy. For instance, an e-banking platform today might have perimeter firewalls (outer wall), intrusion detection systems (patrolling sentries), internal network segmentation (inner gates), and rigorous access controls (guarded entry points), much like a well-fortified ancient city. Table 1 below illustrates this and other parallels.

- **Alliances and Collaboration:** Chanakya's foreign policy was summarized by the saying "My enemy's enemy is my friend." He encouraged forging alliances with friendly kingdoms or internal stakeholders – as a force multiplier for security (Bhat & Shukla, 2024). In cybersecurity, this is analogous to collaboration and information sharing. No bank or institution can single-handedly fend off all cyber threats; partnerships are vital. Banks today collaborate through industry groups and share threat intelligence (for example, through the Indian Bank's Centre for Analysis of Risks and Threats, or the Cyber Threat Intelligence units under CERT-In). The RBI and Indian Banks Association also encourage collective drills and information exchange on frauds. The *Arthashastra's* emphasis on diplomacy and alliance-building supports the modern push for public-private partnerships in cybersecurity, where government agencies (like CERT-In, or the National Cyber Crime Coordination Centre) and financial institutions work together to mitigate threats (Bharadwaj, 2025). This reflects an understanding that security is a shared responsibility – a notion present both in ancient treatises and current cyber policy ethos.

- **Ethical Governance and Training:** Despite advocating realpolitik, Chanakya also stressed ethical governance and the education of leaders. He believed knowledge (*vidya*) and righteousness were key to sustaining power. This extends to ensuring officials are well-trained and corruption is minimized. In the digital age, this translates to cybersecurity education and ethics. Ensuring that employees at banks are trained in cyber hygiene and that there is a culture of integrity (for instance, not abusing privileged access, promptly reporting incidents) is crucial. Chanakya's belief that "an informant who is learned, intelligent and clever achieves success in his missions" highlights the value of investing in skilled personnel (Menon, 2023). Modern banks similarly must invest in skilled cybersecurity professionals (like Chief Information Security Officers and security analysts) and continuous training to adapt to evolving threats. The ancient focus on *dharma* (duty/ethics) can inform today's **cyber ethics**, stressing that those who handle sensitive data or manage security systems have a duty to act responsibly and in the public's interest.

Table 1. Parallels between Chanakya's Arthashastra Principles and Modern Cybersecurity Practices

Arthashastra Principle	Description (Ancient Context)	Modern Cybersecurity Parallel (E-Banking)
Espionage & Counterintelligence	Use of spies and informants to gather intel and foil plots.	Threat intelligence, network monitoring, honeypots for intruder detection (Kulkarni, 2024).
Fortification & Layered Defense	Multi-layered forts, defenses at gates, walls, moats to protect the city/treasury.	Defense-in-depth: firewalls, multi-factor authentication, encryption, network segmentation to protect bank systems.
Dandaniti (Deterrence by Punishment)	Strict penalties for crimes; enforcement of law to deter misconduct.	Cyber law enforcement: legal penalties for hacking, fraud under IT Act; regulatory fines (e.g., RBI imposing fines for data breaches).
Alliances & Diplomacy	Forming alliances with other states for mutual security.	Collaboration: Banks sharing threat intelligence; public-private partnerships (CERT-In, fintech, law enforcement cooperation).

Arthashastra Principle	Description (Ancient Context)	Modern Cybersecurity Parallel (E-Banking)
Insider Vigilance (Integrity of officials)	Mechanisms to test and ensure loyalty of ministers; prevent insider betrayal.	Zero Trust security model ("verify every user"), insider threat programs, background checks and monitoring of staff with privileged access.
Crisis Management & Preemption	Preparedness for disasters (natural or man-made); pre-emptive strikes on threats.	Incident response planning, cybersecurity drills, proactive threat hunting, zero-day vulnerability patching in anticipation of attacks.
Ethical Governance & Education	Emphasis on ruler's duty (dharma) to protect subjects justly; training in statecraft.	Organizational cyber ethics and compliance culture; cybersecurity awareness training for staff and customers; duty of care to protect user data.

Sources: Adapted from Arthashastra (Rangarajan, 1987) and modern cybersecurity frameworks (Kulkarni, 2024; Jeph & Vijaywargia, 2023).

As Table 1 suggests, the strategic paradigms from the Arthashastra can be mapped onto contemporary cybersecurity measures. This historical-philosophical foundation establishes a lens through which we can evaluate current legal and technological frameworks: Are we, in today's Indian banking cybersecurity regime, living up to the spirit of Chanakya's counsel on proactivity, layered defense, intelligence use, and strict but just governance? In the following sections, we keep this question in mind as we shift to the modern landscape of Industry 5.0 and the legal instruments in play.

The Industry 5.0 Landscape in E-Banking

Industry 4.0 vs. Industry 5.0: To appreciate the current landscape, it is vital to distinguish Industry 5.0 from its predecessor. Industry 4.0, over the past decade, digitized banking through automation, cloud computing, mobile platforms, and data analytics. It brought innovations like online banking portals, mobile payment apps, and algorithmic fraud detection – all of which improved convenience but also created new cyber risks (Narsimha *et al*., 2022). Industry 5.0 builds upon those digital foundations but reintroduces the human element in collaboration with automation. In an Industry 5.0 paradigm, technologies such as Artificial Intelligence (AI) and Machine Learning (ML), Internet of Things (IoT) devices, robotic process automation, and even augmented reality interfaces are integrated in banking operations in a *human-centric* way (Breque *et al*., 2021). This means AI and robots are not just automating tasks, but working alongside human experts to deliver personalized services and innovative products. For example, a bank might use AI to analyze customer data and suggest customized financial products, while a human relationship manager makes the final judgment – combining machine efficiency with human empathy.

Technological Elements and Cyber Risks: Industry 5.0 in banking entails several cutting-edge components, each bringing cybersecurity implications:

- **Artificial Intelligence & ML:** Banks employ AI for fraud detection, credit scoring, chatbot customer service, and even investment advisory (FinTech applications). While AI enhances efficiency, it also presents novel vulnerabilities – e.g., adversaries might try to trick ML models (through adversarial inputs) or steal sensitive training data. There are concerns about algorithmic decisions: if an AI incorrectly flags or approves a transaction due to a flaw (or due to being manipulated by a hacker), who is accountable? Moreover, attackers are leveraging AI themselves, using AI to generate convincing phishing emails or automate attacks. The Indian legal system is only beginning to grapple with AI's implications; questions of liability and standards for AI in critical sectors (like banking) are under discussion (Kaur, 2025).

- **Internet of Things:** IoT in banking includes smart ATMs, security cameras and sensors in branches, wearable payment devices, and even smart appliances integrated with payment capabilities (like a smart fridge that can order groceries). Each IoT device is effectively a computer that could be compromised. IoT devices often have vulnerabilities due to weaker hardware or default credentials, making them entry points for hackers. A notorious example globally was the use of security cameras or HVAC systems as entry vectors in breaches. In India, the

proliferation of digital payment kiosks and POS machines means more endpoints to secure. Industry 5.0 envisions seamless connectivity – but that means a breach in one IoT component could pivot into the bank's core network if not properly isolated. Legal guidelines specifically for IoT security in banking are not yet explicit, but general IT security rules apply. The need for **standards** (secure coding, regular patching) in IoT is acknowledged in principle by international frameworks (ISO/IEC 27001:2022 covers IoT device management), yet Indian regulation here remains an evolving patchwork.

- **Big Data and Cloud Computing:** Modern banks rely on massive data analytics to glean insights from customer transactions and behavior. These datasets often reside in cloud environments or large data centers, including third-party cloud providers. While cloud infrastructure offers scalability, it introduces reliance on external parties and potential jurisdictional issues (data stored outside India, raising compliance issues with data sovereignty laws). A breach of a cloud database or a misconfigured cloud storage (a sadly common occurrence worldwide) can expose millions of customer records. The RBI has issued guidelines on outsourcing and cloud risk management, but enforcement is challenging. Big data algorithms also raise privacy concerns – extensive profiling might conflict with privacy laws if done without consent or proper safeguards, an area the new data protection law will address (Digital Personal Data Protection Act, 2023).

- **Robotics and Automation:** Some banks are experimenting with robotic process automation for back-office tasks (like loan processing) and even humanoid robots in branches for customer service. These robots run on software that could be hacked to cause disruption or to siphon information. Industrial robots in other sectors have been hacked before; in banking the risk is more on data integrity and continuity of operations if automation fails or is manipulated. Industry 5.0's emphasis on co-working with robots means cybersecurity must cover not just traditional IT but operational technology (OT) as well – a blurred line when robots handle data.

- **Mass Personalization and Open Banking:** Industry 5.0 aims for personalized services. In banking, this is facilitated by Open Banking APIs, where banks share certain data with third-party fintech apps (with customer consent) to provide innovative services. India's Unified Payments Interface (UPI) is a prime example of open API integration at scale. While hugely successful for financial inclusion and convenience, open APIs expand the threat surface. If a third-party app or API endpoint is insecure, attackers could abuse it to access bank systems or customer data. Recognizing this, the RBI and National Payments Corporation of India (NPCI) have set security standards for payment interfaces and require strong customer authentication (e.g., two-factor authentication is mandatory for electronic payments in India) (RBI, 2016). Nevertheless, the *interconnectedness* that Industry 5.0 promotes means a weak link in the ecosystem (whether a small fintech partner or a supply chain vendor) can lead to breaches – as seen in some recent supply-chain cyber attacks globally.

In summary, Industry 5.0 in banking amplifies the principle of connectivity and intelligent automation, but this also amplifies cybersecurity risks. The interconnected nature yields increased attack vectors: more devices, more software, more external partners (Frontiers, 2024). Data security concerns become paramount as vast sensitive data is generated and transferred in real time (Frontiers, 2024). Additionally, the integration of humans and machines raises unique security considerations: secure authentication is needed not only between people and systems but also machine-to-machine, and even verifying that an AI's output hasn't been tampered with becomes a concern (Breque *et al*., 2021).

From a philosophical angle, Industry 5.0's human-centric approach dovetails with the *Arthashastra's* focus on wise human oversight. The advanced tech should be seen as tools to be guided by human ethics and strategy, rather than supplant human judgment entirely. This perspective is crucial for legal systems: laws must ensure that accountability and human responsibility are maintained even as AI and automation increase.

Indian Cybersecurity Legal Framework for E-Banking

India's cybersecurity legal framework is a mosaic of general cyber laws, sector-specific regulations, and policy guidelines. For the banking and financial sector (often termed BFSI – Banking, Financial Services, and Insurance), there are multiple layers of applicable rules. Here paper outlines the *current statutes and regulations* most relevant to e-banking cybersecurity, and evaluate their efficacy:

European Economic Letters
ISSN 2323-5233
Vol 15, Issue 4 (2025)
http://eelet.org.uk

Information Technology Act, 2000 (IT Act) and Amendments

The **Information Technology Act, 2000** is India's foundational cyber law. Enacted at the dawn of the internet era in India, it provides legal recognition to electronic transactions, digital signatures, and penalties for cybercrime. The IT Act 2000 (as substantially amended in 2008) contains several sections that address offenses pertinent to e-banking security (CIS-India, 2021). Notable provisions include:

- **Section 43 & 43A:** impose civil liability for damage to computer systems and failure to protect personal data. Section 43A (added in 2008) is critical – it mandates that businesses (including banks) handling sensitive personal data implement "reasonable security practices and procedures," and if they are negligent in doing so and cause wrongful loss to any person, they are liable to pay damages (Information Technology Act, 2000, Sec.43A). This effectively introduced an obligation for data security compliance in the corporate sector, arguably a precursor to personal data protection law. Banks, dealing with financial personal data, clearly fall under this and have to follow prescribed security standards (the government tied these standards to the IS/ISO 27001 in the SPDI Rules 2011, discussed below). Section 43A provides a legal lever for customers to seek compensation if a bank's poor cybersecurity leads to theft of their data or funds.

- **Sections 65-66:** define and criminalize certain activities like tampering with computer source code (65), hacking and dishonestly damaging computer systems (66), receiving stolen computer resources or communication devices (66B), identity theft (66C), and cheating by personation (phishing) via computer (66D). These are prosecutable offenses with imprisonment and fines. For instance, a hacker who breaches a bank's server can be booked under Section 66 (computer related offenses, which covers unauthorized access or damage to computer systems) and potentially Section 66F if it endangers national security (cyber terrorism). While these sections provide a basis to punish cybercriminals, their enforcement requires effective investigation and digital forensics – a challenge for law enforcement. As of 2025, many cases of banking fraud (like phishing scams) are registered under these sections, though conviction rates remain relatively low due to jurisdictional issues and technical evidence hurdles. Nonetheless, the IT Act's criminal provisions signal that India considers cybercrimes as serious as analogous offline crimes (even if procedural law and capacity need strengthening).

- **Section 67 & 67B:** though primarily about obscenity and child pornography online, these sections underscore the Act's broad coverage of misuse of electronic media. They are less directly relevant to e-banking, except that they remind banks of their responsibility as intermediaries to not allow their platforms to be misused for any illegal content or activity.

- **Sections 70 and 70A:** Section 70 allows the government to declare any computer resource as a "Protected System" if its incapacitation would harm national security or economy. Many critical systems in banking (like core banking servers of major banks or NPCI's payment switches) could be notified under this, making unauthorized access to them a serious offense. Section 70A (added in 2008) led to the establishment of the National Critical Information Infrastructure Protection Centre (NCIIPC), designating sectors like banking and finance as critical information infrastructure (Bharadwaj, 2025). The NCIIPC works with major financial institutions to audit and enhance the security of critical banking networks. While not directly imposing obligations on banks, this highlights that banking infrastructure is considered part of India's critical infrastructure, warranting heightened security and oversight.

- **Section 72A:** penalizes disclosure of personal information in breach of lawful contract – applicable if, say, a bank employee or any service provider mishandles or leaks customer data intentionally. This complements general data protection by criminalizing certain privacy violations.

The IT Act was path-breaking in 2000 and the 2008 amendments updated it after the explosion of Web 2.0. However, critics note that it is still a general law, not specifically tailored to sectoral needs like banking. Also, cybercrime definitions need constant updating; for example, the Act doesn't explicitly mention ransomware, denial-of-service attacks, or new forms of digital fraud (though they can be prosecuted under broad terms). The government and judiciary have clarified over time that offenses like cyber fraud are indeed covered (The Supreme Court in a 2021 petition affirmed cyber-attacks and data

theft fall under the IT Act and relevant IPC sections) (UpGuard, 2025). A new "Digital India Act" is reportedly in drafting stages to replace the IT Act with a more modern law, but until then, the IT Act remains the default legal backbone for all things cyber in India, including e-banking.

Sectoral Regulations: RBI Cybersecurity Framework and Guidelines

Given the criticality of banking, the Reserve Bank of India (RBI) – India's central bank and banking regulator – has been proactive in issuing cybersecurity guidelines specific to banks and NBFCs. While these are not "laws" passed by Parliament, they are regulatory mandates that banks must comply with, and thus have quasi-legal force (non-compliance can invite penalties and even license cancellation in extreme cases under the Banking Regulation Act). Key RBI instruments include:

- **RBI's Cyber Security Framework (2016):** In June 2016, RBI issued a landmark circular titled *Cyber Security Framework in Banks* (RBI, 2016). This came on the heels of increasing cyber incidents in the financial sector globally. The framework required banks to:
    - Formulate a robust cyber security policy, distinct from broader IT policy, approved by the Board, to cover strategies for combating cyber threats (RBI, 2016). Banks had to classify their inherent risks (low, moderate, high, very high) based on their technologies, products, and threat landscape, and accordingly adopt an appropriate level of security measures.
    - Establish a Security Operations Center (SOC) for continuous surveillance (RBI, 2016). The circular explicitly mandates real-time monitoring capabilities, recognizing that attacks can occur anytime and often stealthily.
    - Conduct regular vulnerability assessments and penetration tests. Continuous surveillance and prompt cyber incident response were emphasized. Banks were instructed to report unusual incidents to RBI immediately.
    - Implement baseline security controls as listed in an annex (covering access controls, network security, secure configuration, anti-malware, employee training, etc.). This was effectively a minimum standard for all banks.
    - Develop an adaptive Incident Response and Recovery plan for cyber incidents, including crisis management and communication strategies. Banks also had to participate in sectoral drills.

This framework was a comprehensive attempt to uplift the cyber resilience of Indian banks. It aligns with global standards like the U.S. FFIEC guidelines and ISO 27001. Implementation, however, has been varied – large banks have set up full-fledged SOCs and follow advanced practices, whereas smaller banks (and cooperative banks) have faced challenges due to limited expertise and resources. RBI conducts periodic cyber audits and has criticized some banks for laxity, indicating the need for continuous improvement.

- **RBI Guidelines on Electronic Banking & IT (Gopalakrishna Committee):** Even before 2016, RBI had released guidelines on electronic banking security and IT governance in 2011 (based on recommendations of the G. Gopalakrishna Committee). These touched on securing internet banking, two-factor authentication for online transactions, better user awareness, and fraud risk management. For example, RBI mandated two-factor authentication for card-not-present transactions way back in 2009, which has been credited with reducing fraud in online card usage in India as compared to regions that only later adopted it (RBI, 2011). The Indian approach of requiring OTPs (One Time Passwords) for payments is now considered a global best practice in user authentication. The IT governance guidelines also required banks to have IT Committees at the Board level and policies for data security. These have laid the foundation which the 2016 framework strengthened.
- **Payment Systems Security:** As digital payments grew, RBI issued specific advisories. In 2019, RBI directed banks to secure their SWIFT messaging infrastructure after some banks suffered SWIFT-related hacks (similar to the Bangladesh Bank heist modus operandi). In 2021, RBI issued a Master Direction on Digital Payment Security

Controls, applicable to payment system operators and banks, covering requirements for robust customer authentication, transaction monitoring, encryption of payment data, etc. Furthermore, NPCI (under RBI's aegis) issues procedural guidelines for UPI and card networks to ensure security (e.g., mandatory tokenization for card data storage by 2022). These sector-specific guidelines supplement the general framework, addressing unique risk areas like inter-bank fund transfers, ATM networks, and mobile wallets.

- **Other Financial Regulators:** It's worth noting that alongside RBI, entities like SEBI (Securities and Exchange Board of India) and IRDAI (Insurance Regulatory and Development Authority of India) have released cybersecurity guidelines for their respective sectors. SEBI in 2015 and 2018 issued cyber security and cyber resilience framework guidelines for stock exchanges, depositories, and other market intermediaries, requiring similar measures (SEBI mandates exchanges to have 24x7 SOC, periodic audits, etc.). IRDAI in 2017 introduced guidelines for insurers to have a dedicated CISO and cyber crisis management plans (UpGuard, 2025). While these are beyond banking, they ensure the entire financial industry moves towards a higher security baseline. There is cross-sector coordination too: for example, the Financial Sector Development Council (FSDC) in India has a Cyber Security subgroup to harmonize efforts between RBI, SEBI, IRDAI, etc. For an e-banking user, this matrix of regulations means that whether they are using a bank, a digital wallet, or a trading app, the institutions behind them are bound by some cybersecurity oversight.

Personal Data Protection and Privacy Laws

Cybersecurity often overlaps with data protection – securing systems is also about protecting personal data from unauthorized access or breach. Until recently, India lacked a dedicated data protection statute, relying on Section 43A of the IT Act and the SPDI (Sensitive Personal Data) Rules, 2011. However, the landscape changed with the passage of the Digital Personal Data Protection Act, 2023 (DPDP Act). Key aspects of the DPDP Act relevant to banking cybersecurity:

- It requires entities (data fiduciaries) to implement reasonable security safeguards to prevent personal data breaches. This essentially codifies the obligation that was earlier in IT Act 43A, but with stronger enforcement – the Data Protection Board can levy hefty penalties for data breaches. For instance, failing to protect personal data leading to a breach can invite fines up to ₹250 crore (approximately USD 30 million) under the new Act. Banks, which process vast amounts of personal and financial data, are definitely significant data fiduciaries under this law. Thus, a cybersecurity lapse leading to leakage of customer data (say account details, KYC info) could now not only cause reputational and civil liability but also regulatory fines under DPDP Act.

- The DPDP Act promotes data minimization and purpose limitation – which indirectly helps cybersecurity by reducing unnecessary data retention. For example, if banks adhere to collecting only what is needed and not storing data beyond its purpose, the impact of breaches can be minimized. It also requires notification to authorities in case of significant data breaches, pushing for transparency.

- While primarily a privacy law, DPDP Act's recognition of concepts like data protection impact assessments and the need for organizational security measures means banking institutions will have to bolster their info-security governance. Many banks have already been aligning with global standards due to serving international customers (e.g., complying with GDPR for EU clients), but a native law brings focus internally.

Besides the DPDP Act, the Indian Penal Code (IPC) is also sometimes invoked for cyber incidents (e.g., IPC Section 420 for cheating in online banking fraud cases, since cyber fraud is essentially a form of cheating). Law enforcement agencies often register both IPC and IT Act sections together for cybercrime FIRs to cover all bases. However, the IPC being a 19th-century law has obvious limitations in addressing digital nuances – a fact that highlights why IT Act and sectoral regulations are indispensable.

National Cybersecurity Policies and Reporting Requirements

On the policy front, India had a National Cyber Security Policy, 2013, which was more of an aspirational document. A new National Cyber Security Strategy has been drafted (as of 2024) but not officially released (Bharadwaj, 2025). Nonetheless, certain administrative orders shape the cybersecurity regime:

- **CERT-In Directions (2022):** In April 2022, CERT-In, empowered under Section 70B of IT Act, issued directions that made it *mandatory* for all organizations (government or private) to report cyber incidents within 6 hours of detection (CERT-In, 2022). This includes banks and financial intermediaries. They also mandated logs to be maintained in India and prescribed time synchronization and other best practices. This was a significant step to improve incident reporting, which was historically under-reported. Banks now have to promptly notify CERT-In of incidents like network breaches, downtime due to cyber-attacks, or massive phishing campaigns affecting customers. This regulatory push aligns with global trends (for instance, the EU's NIS Directive mandates breach reporting in critical sectors). The challenge lies in compliance and handling the volume of incidents – but it undeniably increases situational awareness at a national level and fosters an ecosystem where banks cannot quietly bury incidents without consequence.
- **Cyber Crisis Management Plans:** RBI and CERT-In have urged financial institutions to maintain Cyber Crisis Management Plans (CCMPs). Many banks have their CCMP which is basically a playbook of how to respond to major cyber incidents (isolating affected systems, informing regulators, customer communication, etc.). The RBI often audits banks on their incident response readiness. The existence of a CCMP became vital after incidents like the 2018 Cosmos Bank cyber heist (in which hackers siphoned around ₹94 crore via malware and ATM withdrawals internationally). Lessons from such incidents have been absorbed into guidelines – e.g., RBI promptly required all banks to join centralized payment monitoring systems after that, and to strengthen firewall rules.
- **Critical Infrastructure Protection:** As mentioned, banking being categorized under critical information infrastructure means top banks and financial utilities work with NCIIPC for extra safeguards. While details of NCIIPC audits are confidential, it's known that they stress on network segmentation, whitelisting of traffic, continuity plans, etc., and share threat intel on advanced persistent threats (APT groups) that might target financial systems. This synergy between civil cyber agencies and banking IT departments exemplifies a Chanakyan alliance in practice, though there is scope for more systematic collaboration.

Table 2. Key Indian Legal and Regulatory Instruments for E-Banking Cybersecurity

Law/Guideline	Year	Scope & Relevance to E-Banking Security
Information Technology Act, 2000 (amended 2008)	2000/2008	Primary cyber law: defines cyber crimes (hacking, fraud, identity theft), legal recognition of e-transactions, mandates reasonable security practices (Sec.43A) and penalizes data breaches and cyber offenses. Forms the base legal recourse for cybercrimes impacting banks and customers.
IT (Reasonable Security Practices and Procedures and Sensitive Personal Data) Rules	2011	Rules under IT Act Sec.43A: Define "sensitive personal data" (includes financial info) and prescribe ISO 27001 or equivalent security practices. Banks as "body corporate" must follow these for handling customer data, including having a privacy policy and grievance officer.
Reserve Bank of India Cyber Security Framework for Banks	2016	Regulatory mandate for all banks: requires board-approved cyber policy, baseline security controls, continuous monitoring (SOC), incident reporting to RBI, and regular security assessments. Elevates cybersecurity to a governance level issue in banks.
RBI Master Directions on Digital Payment Security Controls	2021	Detailed requirements for regulated entities (banks, payment operators) on securing internet banking, mobile banking, card payments, UPI, etc. Covers authentication standards (e.g., compulsory 2FA), transaction limits, fraud monitoring, and customer awareness initiatives to reduce payment fraud.
Digital Personal Data Protection Act, 2023	2023	Comprehensive data protection law: imposes duties on banks to protect personal data of customers, report significant data breaches, and uphold privacy principles. Non-compliance (like failing to prevent a breach by not having

Law/Guideline	Year	Scope & Relevance to E-Banking Security
		adequate cybersecurity) can result in large fines, adding regulatory pressure to maintain strong security postures.
CERT-In Directives (Cyber Incident Reporting)	2022	Notified under IT Act: makes it mandatory for banks (and others) to report cyber incidents within 6 hours, to maintain server logs in India, to synchronize system clocks, etc. Increases accountability and timely involvement of national cyber emergency teams for any major incident in banks.
National Critical Information Infrastructure Protection Centre (NCIIPC) Guidelines	2013 onward	Sector-specific advisories for banking as CII: recommends advanced security measures (network isolation, supply-chain security, regular audits) for critical banking systems. Not public, but ensures critical banking infrastructure operators adhere to higher standards and coordinate with national security apparatus.
SEBI/IRDAI Cybersecurity Guidelines (for financial market & insurance)	2015–2017	Parallel regulations ensuring stock brokers, exchanges, and insurance companies (often allied with banks in conglomerates) also enforce cybersecurity. E.g., banks with demat services must also follow SEBI cyber rules. This holistic approach prevents regulatory arbitrage and secures the broader financial ecosystem.

Sources: Compiled from Government of India and RBI releases (RBI, 2016; IT Act, 2000; MeitY, 2011; DPDP Act, 2023; CERT-In, 2022; SEBI, 2015).

Table 2 encapsulates the multi-layered legal instruments governing e-banking security in India. The framework is robust on paper, but there are acknowledged *challenges*: enforcement and awareness. Many bank officials and police investigators have had to be trained in cyber law nuances to effectively use these laws. The judiciary, too, is catching up – special cybercrime courts and training of judges is underway. Another challenge is the overlap of jurisdictions and regulators, which sometimes leads to confusion; for instance, if a fintech app is hacked affecting a bank's customers, both RBI and the Ministry of IT may have roles. The recent streamlining via the Allocation of Business Rules (assigning MeitY for cybersecurity, MHA for cybercrime) aims to clear coordination issues (Bharadwaj, 2025).

Having examined both the ancient *Arthashastra* principles and the modern legal edifice, we can now engage in a deeper comparative analysis. How do current frameworks measure up to the strategic ideals? Where are the gaps that Chanakya might have cautioned us about? The next section provides this analysis, paving the way for recommending a synthesized Neo-Vedic framework.

Comparative Analysis: Ancient Principles vs. Modern Frameworks

In this section, authors analyze how the essence of *Arthashastra's* security doctrine compares to the prevailing modern cybersecurity frameworks in Indian banking. This comparative lens will help identify areas of strength and weakness in the current approach, and guide the formulation of a Neo-Vedic framework.

Strategic Foresight and Proactivity

One of Chanakya's hallmarks was strategic foresight that is anticipating threats and neutralizing them before they materialize. The *Arthashastra* advocates extensive preparations, intelligence gathering, and even pre-emptive strikes when facing potential danger. When we look at modern cybersecurity, the rhetoric often emphasizes proactive defense (e.g., "hunt" teams that seek out threats within networks, patching vulnerabilities proactively, etc.), but in practice many organizations remain *reactive*. Indian banks, under RBI guidelines, have improved in this aspect by setting up SOCs and participating in cyber drills. Yet, incidents like the Cosmos Bank Hack (2018) where hackers compromised the switching system and made off with millions indicate lapses in anticipating attack vectors – that particular breach was facilitated by malware that went undetected until money was already stolen, suggesting a failure of proactive monitoring.

If we measure against Chanakya's yardstick, modern banks need to invest more in *threat intelligence* (akin to spies) and in red-teaming exercises (simulating attacks to find weaknesses). The government's insistence on continuous surveillance (CERT-In's 24x7 monitoring directive) aligns well with the Arthashastra's teaching that vigilance must be unceasing (*"the fort gates should never be left unguarded"*). However, an area where modern practice might fall short is *long-term strategic planning*. Chanakya's plans spanned years if not decades, while cybersecurity plans often look at immediate threats but not systemic risks over longer horizons (for example, how to handle quantum computing threats or AI-enabled attacks in the next 5-10 years). A Neo-Vedic view would implore institutions to adopt a longer strategic horizon, integrating scenario planning for cybersecurity as part of corporate strategy – much like state security strategy.

Comprehensiveness and Layered Defense

The *Saptanga* theory in Arthashastra describes seven pillars of the state (the king, ministers, territory, fort, treasury, army, allies). A bank's analogy might be governance, management, digital assets, network perimeter (fort), capital and data assets (treasury), security team (army), and partners/regulators (allies). Chanakya emphasized that weaknesses in any one pillar could doom the state. Modern cybersecurity frameworks like NIST CSF or ISO 27001 also advocate holistic coverage: identify, protect, detect, respond, recover – covering people, process, technology.

India's legal framework does attempt comprehensive coverage: technology controls via RBI guidelines, process via audits and incident response plans, people via training mandates. But are we balanced across all pillars? It appears people (capacity) remain a weak link – many bank breaches trace back to human error or insider actions (phishing a staffer, or a rogue employee). Chanakya would remind us that even with strong forts, a traitor inside can cause collapse. Current Indian frameworks address insiders tangentially (background checks, need-to-know access in RBI's baseline controls), yet there is no specific law on insider cyber threats. Strengthening this might include stricter penalties for employees involved in data theft (which could be via IT Act Sec.66B/72A, but perhaps better internal oversight and legal clarity is needed).

On layered defense, banks generally have adopted it – thanks in part to RBI's nudges. For instance, multi-factor authentication is an inner layer that has saved many customers from account takeover fraud (contrast with some countries that only recently mandated it). Network segmentation in banks has improved, limiting lateral movement of attackers. However, as per reports by the NCIIPC and others, smaller cooperative banks and some financial institutions are not uniformly fortified (UpGuard, 2025). A single weak link – akin to an undefended small fort city – can be exploited to impact others (especially as banks are interconnected for payments). Thus, one comparative insight is the need for *uniform minimum defenses across the sector*. Chanakya standardized military training and fort standards across the empire; similarly, regulators may need to enforce baseline security uniformly, perhaps by extending regulations to currently less regulated entities (e.g., cooperative banks, some non-bank payment providers).

Deterrence and Punishment of Offenders

Chanakya believed in swift and certain punishment to deter enemies and criminals, but also in appropriate punishment not to alienate subjects. In the cyber realm, deterrence is tricky as many attackers are anonymous, across borders, or state-sponsored. Indian law enforcement has had successes (arrests of some phishing ring members, etc.) but by and large, the attackers in major cases (like the Lazarus group suspected in Cosmos attack, or North Korean APT in ATM server heists) remain outside reach. Thus, the legal threat of punishment does not loom large for them. However, for *insiders and negligent entities*, Indian law has room to deter: e.g., if a bank fails to secure systems and loses money, RBI can penalize the bank (recently RBI has fined banks for failing to comply with KYC/Cybersecurity guidelines). Under the DPDP Act, hefty fines for data breach could act as economic deterrent for negligence. This is akin to Chanakya's principle of also holding officials accountable (he prescribed fines for guards or treasurers who failed in their duties allowing theft).

One area to compare is responsiveness of law – the Arthashastra was updated with evolving times (it's thought to be a compilation over years). Indian cyber law, notably the IT Act, has not been amended since 2008 in any major way, despite huge changes in technology since then. This lag means some offenses or modus operandi are not explicitly covered, potentially weakening deterrence (attackers exploit ambiguities). A Neo-Vedic approach would treat the law as a living document, updating it as strategically required to cover new threats – for example, explicitly criminalizing distributed denial of service (DDoS) attacks, or deepfake-based fraud, etc., which are currently prosecuted under generic provisions. Encouragingly, the upcoming Digital India Act is expected to modernize these aspects.

Another deterrence aspect is public attribution and shaming – historically, conquered or caught spies would be made an example of to dissuade others. In cyber context, public-private collaboration could include "name and shame" of threat actors or sanctions against state-sponsored attackers. India has started to call out cross-border cyber intrusions diplomatically. But domestically, perhaps publishing statistics of enforcement (conviction rates, etc.) might help show that cybercrime is taken seriously. Today, victims often feel justice is elusive (due to low conviction). So strengthening the investigative apparatus (specialized cyber police, forensic labs) is vital for deterrence, aligning with Chanakya's insistence on well-equipped *kantakasodhana* (investigation department in Mauryan administration).

Alliances and Collective Security

As observed, collaboration is key. How does modern practice fare? Within India, we see silos gradually breaking: the establishment of I4C (Indian Cyber Crime Coordination Centre) and sectoral CSIRTs (like a planned CSIRT-Finance) are positive steps (Bharadwaj, 2025). The financial sector has its Information Sharing and Analysis Center (ISAC) for sharing anonymized threat information. India also engages globally (e.g., Budapest Convention on Cybercrime – though not signed, India cooperates in INTERPOL operations, and CERT-In has MoUs with many country CERTs for info exchange). These efforts resonate with the Arthashastra's principle of forming alliances to face common enemies. A bank alone is like a small kingdom; banding with others yields strength in numbers against cyber cartels.

One comparative gap is perhaps in public awareness – the citizens (customers) are part of the alliance too. Chanakya educated his populace in responsibilities; similarly, digital literacy and customer awareness programs are needed to avoid social engineering attacks. RBI and banks do run campaigns ("Think Before You Click" etc.), but fraud losses due to basics (like sharing OTPs) remain high. A Neo-Vedic approach would treat customer awareness as part of the defense fabric – just as villagers might be the eyes and ears to report suspicious movements in ancient kingdoms, today customers should be empowered to spot and report fraud attempts. Law can support this by mandating certain disclosures and quick fraud reporting channels, which RBI has indeed done (like banks must provide 24x7 helplines and quick dispute resolution for digital fraud).

Ethical Dimension and Trust

Lastly, the comparative analysis must consider the *ethical-philosophical dimension*. Vedic tradition put emphasis on *dharma* (duty, righteousness). In governance, this meant the king must not only be strong but also just, to maintain legitimacy. In cyber law, authors find an analog in the need to respect privacy and rights even as we secure systems. Over-securing (mass surveillance or draconian measures) can erode public trust, just as an unjust king loses mandate. India's legal system is continually trying to balance security with individual rights – for example, the debate around strong encryption: law enforcement sought a way to break encryption for catching criminals, but that raised constitutional issues regarding privacy (post the *Puttaswamy* judgment affirming privacy as a fundamental right). A balanced approach (perhaps using advanced lawful access methods without general backdoors) is still being evolved. Chanakya too balanced surveillance with privacy of citizens to some extent; he advised kings to spy but also warned against unnecessarily prying into loyal citizens' lives.

Thus, a Neo-Vedic framework would encourage trust-building between users and institutions. From a comparative viewpoint, India's push for data protection and consent (via DPDP Act) is a step to ensure that even as banks secure and use data, they do so transparently and with respect for customer rights. Trust is also built by accountability – the RBI's policy that customer losses in certain digital fraud cases must be made whole by banks (if the customer reports quickly and wasn't negligent) is a very dharmic approach, putting the onus on the stronger party (banks) to protect or compensate the weaker (customer) in the event of wrongdoing. This resonates with Arthashastra's recommendation of compensating victims (Jeph & Vijaywargia, 2023).

In conclusion of this comparative section, the authors find a largely *complementary relationship* – ancient wisdom often reinforces what modern frameworks strive for: comprehensive defense, proactive measures, strong deterrence, alliances, and ethical governance. The divergences or gaps identified (like need for more frequent law updates, better insider threat focus, longer-term strategy, and enhanced capacity for enforcement) can be addressed by consciously incorporating those ancient insights that might have been underappreciated. This sets the stage for articulating a cohesive Neo-Vedic framework for e-banking cybersecurity, which we do next, synthesizing the lessons learned.

European Economic Letters
ISSN 2323-5233
Vol 15, Issue 4 (2025)
http://eelet.org.uk

A Neo-Vedic Framework for E-Banking Cybersecurity

Drawing together threads from the Arthashastra and modern cybersecurity paradigms, authors propose a *Neo-Vedic framework* tailored for the Indian e-banking sector. This framework is not a single model or software, but rather a set of guiding principles and strategic directives that can inform policy-makers, regulators, and banking institutions in strengthening cybersecurity. The term "Neo-Vedic" signifies a blend of age-old Indian wisdom with contemporary technology management – essentially, *old wine in a new bottle*, where the wine is the timeless strategy and the bottle is the modern cyber context.

The Neo-Vedic framework can be conceptualized as comprising five pillars, which echo certain Sanskrit terms for conceptual continuity:

1. **Dharma (Ethical Duty and Accountability):** *Dharma*, in this context, refers to the duty of financial institutions to uphold trust and protect stakeholders. Cybersecurity should be seen as a fiduciary duty of banks towards their customers – as important as safeguarding depositors' money is safeguarding their data and online transactions. This pillar would encourage embedding ethical considerations into cybersecurity programs. For example, banks should implement *privacy-by-design* in their systems (as mandated by data protection law) as a duty, not a mere compliance checkbox. They should be transparent with customers about incidents (no cover-ups). At a regulatory level, Dharma implies holding organizations accountable (through penalties or public censures) when they fail to meet their duty of protection. It also means encouraging a culture of cyber ethics among employees – treating customer data with sanctity, just as Chanakya insisted on integrity among treasury officials. The RBI and government could incorporate Dharma by issuing guiding principles that boards of banks must treat cybersecurity as part of their corporate social responsibility (CSR), ensuring that protecting consumers is at the core of their mission.

2. **Suraksha (Multi-Layered Protection):** *Suraksha* means protection. This pillar embodies the defense-in-depth principle rooted in Arthashastra's fortification concept. Under Suraksha, the framework would list concrete expectations for layered controls: e.g., every e-banking system should have perimeter defense (firewalls, DDoS protection), robust access controls (MFA, privileged access management), internal segmentation (so a breach of a minor system doesn't expose crown jewels), continuous monitoring (SOC with SIEM tools), and data protection measures (encryption in transit and at rest, regular backups tested for recovery). Essentially, this pillar translates the RBI's 2016 framework and global best practices into a living doctrine. A Neo-Vedic twist here is emphasis on *redundancy and resilience* – Chanakya advised having fallback arrangements for everything critical. Likewise, banks should maintain backup systems, redundant communication links, and incident response playbooks with alternative procedures if primary systems fail (for instance, if the core banking system is under attack, have a read-only backup to at least let customers view balances, etc.). The regulator might enforce Suraksha through regular audits and perhaps a cybersecurity rating mechanism for banks, fostering a healthy competition to achieve higher security maturity.

3. **Anvikshiki (Wisdom/Strategy – Intelligence & Foresight):** *Anvikshiki* in ancient Indian philosophy means the science of inquiry or strategic philosophy. Here it encapsulates threat intelligence, analytics, and foresight. This pillar would formalize how banks gather intel on emerging threats and how they strategize for future risks. Concretely, it suggests creating sector-wide threat intelligence exchanges (if not already robust, perhaps an RBI-led FIN-CERT for banks to pool information on threats in real time). It also supports scenario planning exercises at the industry level – for example, conducting an annual "cyber war game" among major banks and regulators to simulate an attack on critical payment systems and assess collective preparedness. Under Anvikshiki, banks would also be encouraged to leverage AI for predictive security – using machine learning to detect anomalies in network traffic that might indicate a breach (aligning with Industry 5.0's AI usage but turning it towards security). A key recommendation here is the establishment of a Banking Cybersecurity Advisory Board comprising tech experts, law enforcement, and maybe scholars of security (including those versed in Kautilya's strategies) to periodically review threat landscape and update guidance. This keeps the strategy dynamic and knowledge-driven, much as Chanakya's counsel was considered cutting-edge for his time.

4. **Samagra Suraksha (Holistic Collaboration):** *Samagra* means integrated or whole. This pillar stresses that cybersecurity is a shared endeavor – no entity stands alone (similar to the Arthashastra's emphasis on allies). Under this, the framework would promote deeper collaboration: between banks (through industry bodies), between banks and government agencies (e.g., streamlined info-sharing with CERT-In and I4C), and between nations (since cybercrime is transnational, Indian entities should cooperate with global initiatives). One practical step could be developing a *Cyber Incident Response Alliance* in the BFSI sector, where, say, if Bank A is hit with a novel malware, it immediately shares indicators of compromise with all other banks via a secure channel so they can fortify themselves – this already happens informally, but formalizing it reduces lag. Another aspect is including telecom and tech providers in the alliance – many banking frauds involve phone/SMS or hosting providers (for phishing sites). Partnerships with telecom companies to quickly block phishing SMS or with web hosting companies to take down phishing pages targeting banks would be part of Samagra Suraksha. Legally, this might be facilitated by MoUs and also by refining the "takedown" provisions in law to react faster to phishing/fraud infrastructure. The Neo-Vedic ideal of collective security underlines that an attack on one should be seen as an attack on all, galvanizing a unified defense.

5. **Shastra-Bala (Technological Strength and Innovation):** *Shastra* means weapon or technology, and *Bala* means strength. In Chanakya's time, this could refer to military might and innovative war machines. In cybersecurity, this pillar calls for harnessing technology itself as a means of security – essentially, investing in cutting-edge "cyber weapons" for defense (and possibly offense, in the context of law enforcement). For banks, this means adopting advanced security technologies like endpoint detection and response (EDR), deception grids, blockchain for data integrity, quantum-safe encryption (preparing for future threats), etc. It also encourages supporting indigenous cybersecurity innovation – much like a kingdom would want locally made weapons to reduce dependence, India's banks could benefit from local cybersecurity startups solutions tailored to Indian needs (for example, AI models trained on Indian banking fraud patterns). Regulators under this pillar might create sandboxes for banks to safely test new security tech or fund pilot projects (similar to RBI's fintech sandbox but for regtech/cybertech). On the law enforcement side, Shastra-Bala implies enhancing cyber forensics capabilities, using AI to triage incidents, and perhaps legalizing certain controlled offensive actions (like government hacking of criminal servers under court order) to dismantle botnets or cybercriminal infrastructure threatening the banking sector. This pillar recognizes that in Industry 5.0, one must *fight fire with fire*, using the best of tech to counter tech-driven threats, all while staying within ethical and legal bounds.

These five pillars interrelate and reinforce each other. The Neo-Vedic framework is not a static checklist but an *ongoing paradigm*. For adoption, a multi-stakeholder approach is needed: RBI and government agencies would integrate these principles into guidelines and national strategy; banks would incorporate them into their enterprise risk management and governance structures; and audit mechanisms (internal and external) would assess compliance and effectiveness.

One could envision, for instance, RBI issuing a guidance circular that explicitly references drawing lessons from *Arthashastra* for modern cybersecurity governance, to culturally contextualize the importance. Already, some Indian strategic thinkers have advocated embedding Indian philosophical concepts into our understanding of security (Menon, 2023). This framework does exactly that for the cyber domain.

Conclusion

From the ancient halls of Chanakya's Takshashila to the modern server rooms of India's banks, the quest for security remains a continuous war of wits. This paper has traversed a unique journey: starting with the wisdom of *Arthashastra* – which taught us that strong fortifications, intelligence networks, just laws, and alliances are the bedrock of a secure state – and arriving in the era of Industry 5.0, where banks merge human insight with artificial intelligence and face threats unimaginable in ancient times. Despite the gulf of centuries, we find that many fundamental principles of safeguarding assets and people are unchanged. The challenge is to adapt these principles to new battlegrounds: the cyberspace and digital ecosystems that form the nervous system of e-banking.

Our analysis of current Indian legal frameworks revealed that India has made commendable strides in establishing a cybersecurity regime for banking. The IT Act and its offspring regulations provide a base legal structure for penalizing

cybercrimes and mandating security practices. The RBI, with its sector-specific guidelines, has proactively pushed banks to harden their defenses and treat cybersecurity as a board-level priority. New developments like the DPDP Act further strengthen the hand of regulators and consumers in ensuring data security. These are significant achievements, reflecting an understanding at policy levels that cybersecurity is integral to financial stability. It is telling that banking is classified as critical infrastructure – cybersecurity in this sector is not just about individual banks, but about national economic security.

Yet, gaps and challenges persist. Cyber threats are fast-evolving; our laws and institutional capacities often lag behind. Indian banks continue to face frequent cyber incidents, from ATM network breaches to phishing scams that defraud customers. Every major incident tests the resilience of the legal and technical safeguards in place. Where responses have been ad-hoc or slow, it undermines public trust in digital banking. Moreover, as Industry 5.0 technologies like AI permeate banking, the legal ambiguities around them (liability for AI errors, regulation of algorithms, etc.) need resolution. Internationally, cyber attackers are collaborating in a professionalized underground economy – this calls for equally strong collaboration among defenders across organizations and borders, something that requires constant nurturing of alliances and possibly new international agreements.

In this context, Chanakya's counsel appears strikingly relevant. His treatise reminds us to anticipate adversaries' moves (*"to foresee the attack is to half defeat it"*), to secure every flank, to administer deterrence justly, and to leverage every resource (human or technological) shrewdly. By proposing a Neo-Vedic framework, this paper suggests that Indian policymakers and banks embrace a culturally resonant yet forward-looking approach. This framework is not a rejection of global best practices – rather, it enriches them. It places familiar concepts like defense-in-depth or threat intelligence into a broader civilizational narrative of duty, strategy, and collective good. This could improve buy-in at all levels: boardrooms might take security more seriously when framed as a *dharma* as much as a compliance requirement; employees might commit more to training when they see themselves as part of a proud tradition of guardians; and even customers might be more vigilant if cybersecurity is presented as a shared societal value.

Recommendations: Building on our study, the following recommendations are offered to strengthen e-banking cybersecurity in India:

1. **Update and Unify Cyber Laws:** Expedite the introduction of the proposed Digital India Act to update definitions of cyber offenses (covering new threat vectors like ransomware, IoT-based crimes, AI abuse) and to incorporate provisions specific to critical sectors like banking. Consider a unified cybersecurity statute or at least a coordinated legal framework that harmonizes the IT Act, DPDP Act, and sectoral regulations, so that there are no gaps or overlaps. Within this, explicitly recognize concepts like critical infrastructure offense to deter state-sponsored attacks (e.g., making it clear that attacks on banking systems will invite stringent penalties, even in absentia, and possible retaliation under law).

2. **Strengthen Enforcement and Capacity:** Laws mean little without enforcement. Invest in training specialized cybercrime units in every state's police force to handle banking cyber fraud cases swiftly. Enhance the capacity of forensic labs so that digital evidence from bank breaches can be analyzed in time to aid prosecutions. On the regulatory side, RBI should continue to conduct cyber drills and even consider *mystery penetration testing* – hiring ethical hackers to test banks' defenses periodically (with appropriate legal safe harbor). A results-based "cyber hygiene rating" for banks (perhaps published annually) could foster accountability and consumer awareness.

3. **Ancient Wisdom in Modern Training:** Include modules on Kautilya's principles in cybersecurity leadership training for bank CISOs and risk officers. This is not to mystify the field but to provide a strategic lens that resonates with Indian ethos. Analogies from Arthashastra could be used in employee awareness programs to make the idea of insider threats or need for intelligence more relatable (storytelling can be a powerful tool – e.g., recounting how a careless guard led to a fort's fall, akin to a weak password leading to a breach). The government could even commission a concise "Chanakya's Cybersecurity Niti" booklet for widespread distribution, bridging classical concepts with digital security advice.

4. **Enhance Collaborative Mechanisms:** Establish a formal Financial Sector Cybersecurity Coordination Forum under the aegis of the Ministry of Finance or National Security Council Secretariat, which meets quarterly with participation from RBI, CERT-In, I4C, NCIIPC, and representatives of major banks and payment operators. This

forum would review threat intelligence, share lessons from incidents, and issue updated joint advisories. Essentially, institutionalize the alliance. Internationally, India should actively participate in shaping norms for cyber defense (for instance, leading conversations in G20 on securing digital payments, given India's success with UPI, etc.) – taking an alliance mindset globally too.

5. **Promote Technology Innovation and Self-Reliance:** Encourage public-private R&D for cybersecurity solutions tailored to Indian banking. The government could offer incentives or grants for developing indigenous encryption algorithms, secure core banking software modules, AI-based fraud detection tuned to local patterns, etc. This not only reduces reliance on foreign tech (which can be a security risk if there are hidden backdoors) but also aligns with Chanakya's notion of using one's own resources optimally. Similarly, adopt an approach of continuous innovation – what worked yesterday might not work tomorrow; hence, banks should have innovation sandboxes for cybersecurity just as they have for fintech.

6. **User-Centric Safety Measures:** On the customer end, regulators should push further measures to protect consumers. For example, implement liability frameworks where by default the bank refunds unauthorized transaction losses (up to certain limits) unless proven customer negligence – RBI has already moved in this direction with zero-liability and limited-liability policies for digital transactions; strict implementation will incentivize banks to enhance security to avoid losses. Additionally, leverage India's digital public infrastructure: perhaps integrate banking fraud reporting into the national cybercrime portal more seamlessly, and ensure quick action through a tie-in with telecom to deactivate mule accounts or phone numbers involved in fraud (like I4C's cyber fraud tracking system – expand and publicize it so every victim knows where to report and sees quick action).

7. **Periodic Strategy Reviews (Learning from History):** Just as Arthashastra was updated with new learnings, India's cybersecurity strategy for banking should be revisited regularly. Constitute a panel every few years including historians, technologists, legal experts, and bankers to review if any emerging risk is not addressed or if any regulation has become obsolete. This keeps the framework agile. Perhaps draw parallels from historical events – e.g., analyze a major cyber incident by comparing it to an ancient battle's lessons (for scholarly as well as practical insights). Such cross-disciplinary reflection can yield creative solutions.

In essence, these recommendations aim to create a resilient, culturally grounded, and forward-looking cybersecurity environment for Indian e-banking. By anchoring modern initiatives in the rich bedrock of India's own strategic thought (rather than relying solely on imported frameworks), there is potential to craft solutions that are not only effective but also resonate with stakeholders at a deeper level.

The journey from Chanakya's teachings to cyber firewalls illustrates a continuity of purpose: securing the prosperity and stability of the realm – whether that realm is an ancient kingdom or a digital financial network. As India continues to champion digital finance (with world-leading innovations in payments and fintech), it must equally champion digital security. A fusion of *jurisprudence, technology, and philosophy* could be India's unique contribution to global cyber security practices. In conclusion, by learning from the past and adapting for the future, India's legal system and banking industry can jointly build an e-banking ecosystem that is secure by design, resilient in the face of Industry 5.0 challenges, and anchored in the timeless values of duty, knowledge, and collective well-being. This Neo-Vedic framework for cybersecurity can serve as a guiding light in a world of evolving threats – much like the eternal wisdom of the Arthashastra has guided governance for centuries.

References

1. Bharadwaj, T. (2025). *Mapping India's Cybersecurity Administration in 2025*. Carnegie Endowment for International Peace. (Discusses recent developments in India's cyber governance, CERT-In statistics, and allocation of roles among agencies).
2. Bhat, V. R., & Shukla, T. (2024). Kautilya's Arthashastra: Timeless Strategies for Modern Governance. *Akhil Bhartiya Shiksha Samagam Conference Proceedings*. (Analyzes Arthashastra's relevance to contemporary governance issues, providing context for its strategic principles).

3. Breque, M., De Nul, L., & Petridis, A. (2021). *Industry 5.0: Towards a sustainable, human-centric and resilient European industry*. European Commission. (Introduces the concept of Industry 5.0 emphasizing human-machine collaboration, relevant for defining Industry 5.0 in this paper).
4. Gautam, P. K. (2018). Kautilya's Arthashastra and its Relevance to Contemporary Strategic Studies. *Journal of Defence Studies, 12*(3), 23-45. (Explores how Arthashastra's principles can be applied to modern strategic and security thinking).
5. Gautam, P. K. (2021). Kautilya's Arthashastra and Chanakya Niti. *Journal of Defence Studies, 17*(1), 23-45. (Provides insight into Chanakya's teachings on statecraft, law, and security, used to support historical analysis in this paper).
6. Jeph, A. K., & Vijaywargia, R. (2023). Challenges and Solutions of Cyber Crime in Indian Jurisprudence. *Journal of Advances and Scholarly Researches in Allied Education, 20*(2), 431-434. (Highlights Arthashastra's mention of crime and punishment, and discusses evolution of crime with technology in the Indian context).
7. Kanwal, G. (2016). *The New Arthashastra: A Security Strategy for India*. Journal of Defence Studies, 11(3), 1-436. (A comprehensive work linking ancient strategic thought to India's modern security strategy, reinforcing the idea of learning from Arthashastra).
8. Kulkarni, K. A. (2024). Cybersecurity Through the Lens of Chanakya: Strategic Wisdom from the Arthashastra for Modern Digital Defense. *ShodhKosh: Journal of Visual and Performing Arts, 5*(6), 2864–2869. (Draws parallels between Chanakya's tactics and modern cybersecurity measures like defense-in-depth and threat intelligence).
9. Kaur, G. (Ed.). (2025). *The Techno-Legal Dynamics of Cybercrime and Security in Industry 5.0*. Scrivener – Wiley. (A collection highlighting legal challenges of advanced technologies like AI/IoT in Industry 5.0; provides context especially on techno-legal issues in e-banking and comparative international perspectives).
10. Menon, S. (2023). The Arthashastra of Chanakya and Its Implications for National Security. *University of Kerala Working Paper*. (Reflects on how ancient Indian strategic thought can inform current national security and cyber strategy).
11. Narsimha, V. et al. (2022). Emerging threats in digital payment and financial crime. *International Journal of Computer Applications, 175*(30), 1-5. (Identifies cybersecurity risks in e-banking technologies and emphasizes the need for robust security measures in digital payments).
12. Reserve Bank of India (RBI). (2016). *Cyber Security Framework in Banks* – Circular DBS.CO/CSITE/BC.11/33.01.001/2015-16, June 2, 2016. (Outlines RBI's mandatory cybersecurity guidelines for banks, cited regarding board-approved policies, SOC, etc.).
13. Reserve Bank of India (RBI). (2023). *Annual Report 2022-23*. RBI Publications. (Includes discussion on operational risks in banks, cost of data breaches statistic cited in introduction).
14. UpGuard. (2025). Top Cybersecurity Regulations in India [Updated 2025]. *UpGuard Cybersecurity Blog*. (Summarizes India's cybersecurity laws and regulations including IT Act, amendments, sectoral regulations, used to cross-verify legal details).