Journal of Hospitality and Tourism Review
DOI: 10.17492/JHTR.v1i1.2601
Volume 1, Issue 1, Jan-Jun 2026, pp. 1-11

# When the Algorithm Becomes the Adversary: Agentic AI Threats and Cybersecurity Vulnerabilities in India's Hospitality, Aviation, and Digital Payment Infrastructure

**Ajay Prashar**[1], **Parikshit Sharma**[2]

1 Professor, Ethiopian Public Service University, Addis Ababa, Ethiopia
2 Associate Professor, Jagran Lakecity University, Bhopal. Email: parikshitsharma@live.com

## Abstract

Since the break of COVID19 pandemic, we have seen a crucial shift in the AI dimensions and usage. What earlier was mostly reflexive and responded to queries only, has shifted to a different paradigm of self-initiated actions and has become autonomous in nature. The paper here tries to examine and explore how the upcoming agentic systems are remodeling the threat landscape of cybersecurity for the service sector of India, i.e., Hospitality, Aviation and the Digital Payments environment. Through a qualitative study based on case-study method, the research aims to analyze three vulnerability structures which are deeply interconnected: AI-architected social engineering scams that are targeting the hotel Property Management Systems (PMS); the operational disruption risks arising from the API sprawl within the Global Distribution Systems (GDS) consumed by the airlines and hotel industry; and the critical exploitation of Aadhar-Enabled Payment System (AePS) biometric infrastructure through machine-learning-assisted fingerprint cloning. The discussions and findings reveal how India's hyperdynamic digital integration has outpaced the development of correlated defensive mechanisms. Towards the end, the paper sums up a multi-layered mitigation framework anchored in AI Red-Teaming (defensive), Biometric locking protocols under the UIDAI ecosystems, and regulatory compliance with the Digital Personal Data Protection (DPDP) Act 2023.

**Keywords:** Cybersecurity, hospitality sector, Aadhaar fraud, Agentic AI, and DPDP Act.

## 1. Introduction

The ever-dynamic sectors of hospitality, tourism and aviation have been appreciated to be the most vital and prized assets. Our esteemed guests share vital information which is regarded to be the most important *Personally Identifiable Information (PII)*, in the form of passport numbers, details regarding the various payments and bill settlement modes like credit card and debit card information, biometric identifiers, as well as the travel plans and itineraries through the Guest Registration Card (GRC) fill-up. They trust the hotel management with the crucial data on the principle of "Trust". Safeguarding this vital information is the responsibility of the hotel management, which is a severe problem faced these days. Two decades ago, the same data could be compromised only by the human factor's involvement. A decade in progress, it was conducted through clumsy phishing emails which were deceptive, or by the use of card skimming machines during the payment gateways and billing settlements. The era of conventional system has come to an end.

The globe is ticking on the concepts of Artificial Intelligence which has reached the helm of safety measures. The AI ecosystem is no longer a tool that can assist the human threat actors. It has come to a stage where it has become autonomous. These autonomous agents have the capability to have end-to-end offensive workflows, such as: *reconnaissance, target selection, devising social engineering and exploitation scams with zero to minimal human supervision.* ML and Machine Intelligence consultants,

AI developers and academicians have begun grappling with this strange transition means for critical economic infrastructure (Anthropic, 2024; Park et al., 2024).

India is also facing this acute challenge for two major reasons. Primarily on the country's service sector focusing hospitality, tourism and aviation, which are in the midst of the extraordinary digitation and expansion boom. The premium star-classified hotels have started integrating the Property Management Systems (PMS) with high-tech infrastructures like the cloud services, airlines connected to the Global Distribution System (GDS) through dozens of Application Programming Interface (API), and the interactive, transaction-enabled tourism platforms with the unified identity layers of Aadhaar and the National Payments Corporation of India (NPCI) payment rails. And second factor is, the integration has proceeded at a pace that has, through various documented cases, outrun the implementation of matching security controls (RBI, 2025; NPCI, 2024).

The result is a landscape of partially-secured, interlinked and highly rich data, precisely to the taste of the agentic AI landscape which it aims to threaten with maximum damage. This paper examines that threat through a case-study lens, focusing on three sectors where operationally critical infrastructure will handshake with digital exposure: hospitality, aviation and the digital payment infrastructure. Towards the end, the paper proposed a practical architecture strategy for mitigation calibrated to the specific regulatory and institutional realities with the Indian context.

## 2. Objectives of the study:

The paper addresses the identified research gap with three specific objectives:

1. to portray the threat vectors most pertinent to India's hospitality, aviation and digital infrastructure sectors with reference to the Agentic AI capabilities.

2. to analyze real-world breach patterns and their sector-specific implications through three interconnected case presentations drawn from India and comparable international references.

3. to propose an evidence-based defensive framework aligned with India's dynamic and evolving architecture, including the Digital Personal Data Protection Act (DPDP) 2023 and UIDAI's biometric security protocols.

## 3. Review of Literature

### *3.1 The Agentic AI concept:*

Researchers have keenly observed the systematic progression of Large Language Models (LLM) evolution from mere text completion stages to becoming the advanced systems that can use tools, reason multi-step reasoning and interact with the environment. Anthropic, 2024 and Bommasani et al., 2024 in their researches have suggested that, a class of AI models that can make sequences of causally influential actions in the world without continuous human supervision has been termed "agentic AI". The study of Park et.al., (2024) states the shift has altered the uses for good and bad. On the offensive side, an agentic model can independently scan for API weaknesses, generate thousands of personalized phishing messages, analyze online responses to attacks, and escalate if attacks are successful within a timeframe that is faster than traditional security monitoring.

Brundage et al. (2024) have conducted a thorough study of the different threat actors' ways to misuse AI and drawn out three clusters that are of major concern:

1) *First*, they observe that existing threat actors can now more easily find additional instances where AI technologies could be leveraged for malicious purposes.

2) *Second*, they make a note on the emergence of innovative but novice classes of threat actors, sometimes called "*script kiddies*," who can easily gain access to AI-assistants and thus use them for malicious purposes as well.

3) *Third*, they see the emergence of qualitatively novel and innovative ways for actors to misuse AI technologies. All three are pertinent to the context of hospitality, aviation and tourism.

Weidinger et al. (2022) also classify risks that language models pose in six areas: misuse, misinformation, human-computer interaction harms, all of which are manifested in the two industries studied in this book: hospitality and aviation.

### *3.2 Cybersecurity in Hospitality:*

As hotels are well-documented in hospitality management literature, the tourist sector is an easy and tempting target for cybercrime for many reasons. In 2018, Marriott International announced the extensive and devastating data breach, which initiated in 2014, had compromised the information of around 500 million guests and was serving as an example of the dangers of poor security integration after a merger (PwC, 2019).

The MGM Resorts hack in 2023, where breaches of a social engineering attack against a help desk worker resulted in over USD 100 million in losses and shut down operations throughout the MGM Resorts. Bischoff (2023) emphasizes through this incident researched that attackers need only one human vulnerability in a chain of automated systems.

Indian hotel chains have double jeopardy. According to data that CERT-In has collated for 2024, Property Management Systems (PMS) and guest Wi-Fi infrastructure were the main vectors of attack in the hospitality industry (CERT-In, 2024). Mishra and Singh (2023) in their research analyzed the situation with mid-market Indian hotel-chains, revealing that less than 30 per cent had implemented endpoint detection and response (EDR) solutions and that staff cybersecurity training could be described as 'episodic'. Industry dynamics that involve high employee turnover rates, mobilized workforce, and a culture of convenience over protocol, create circumstances that are challenging to protect even with traditional threat models, much less with AI-infused threats.

### *3.3 Aviation Digital Infrastructure:*

The aviation industry is not safe either. It displays a unique threat profile. A successful attack in the aviation industry, in contrast to hospitality, does not just inflict reputational and financial harm; however, it has operational safety implications. Airline reservation systems are integrated with Global Distribution Systems (GDS) like Amadeus, Sabre, and Travelport, expanding the threat surface and resulting in a huge network of APIs that can be used for pricing, booking seats, and even control of airport slots, etc. (Papadaki et al., 2023).

According to the Open Web Application Security Project (OWASP) (2024), one of the greatest mid-2020s security challenges is the constant expansion of poorly documented, inconsistently secured application programming interfaces (APIs) as a phenomenon known as API Sprawl. In the Indian context, there is a rapid expansion in digital capabilities with low-cost carriers (LCC) during the pandemic recovery phase, also often involved embedding third-party services without proper API security reviews (Venktaraman, 2024). Once in this environment, agentic AI systems can systematically scan an airline's vulnerable assets for minutes and craft automatic refund fraud campaigns at scale, causing a severe financial incidence for the company to monitor and safeguard.

### *3.4 (Aadhaar, AePS, Biometric Fraud):*

The place where the eagerness and capability of technology meet the potential hazard of security is perhaps nowhere more pronounced than in the biometric identification system in India, which has widely been operationalized through the personal identification, banking and finance as well as the passport verification systems. Aadhaar is a 12-digit unique numerical identity setup, that has been given to more than 1.3 billion citizens by the Unique Identification Authority of India (UIDAI) and has been used to support a host of financial services via the Aadhaar-Enabled Payment System (AePS). Under AePS, people, especially in rural areas, can do banking operations through fingerprint using any banking correspondent outpost (UIDAI, 2025).

The principle of the security architecture of AePS is that biometric signature is difficult to be spoofed. However, with the new developments in generative AI and 3D reconstruction techniques recently witnessed through deepfake videos and photo morphing, this has been significantly undermined. Research of Galbally et.al., 2023, has shown that a machine learning model can successfully decipher high fidelity fingerprint geometries from public land registry documents, scanned government records, or even pictures, offering the opportunity to defeat commercial biometric scanners. As per RBI's annual report on digital frauds, more than 40,000 complaints were received in the last year of AePS unauthorized transactions, most of them from the states having rural and tribal population benefitting from this scheme: Madhya Pradesh, Rajasthan and Jharkhand (RBI, 2025).

### *3.5 The DPDP Act 2023*

The introduction of the Digital Personal Data Protection (DPDP) Act 2023 is the most prominent legislation in India since the Information Technology Act 2000 (IT Act) in the country's data governance framework. The DPDP Act creates duties for the *Data Fiduciaries* (processors of data), such as hotels, airlines, and travel platforms, to ensure that they put in place suitable technical and organizational measures, promptly report any breaches, and minimize data (MeitY, 2023). Penalties under the Act can go up to ₹250 crore in case of major infringements, which is a strong financial incentive for investing on cybersecurity as there was hardly a financial incentive under the previous voluntary compliance regime.

The DPDP Act, however, does not provide industry-specific directives, and these general guidelines are left for individual organisations to interpret, especially in the context of the hospitality and tourism sector as noted by Kapoor and Bhandari (2024). In addition, the Data Protection Board and other enforcement mechanisms were still in formation as of early 2026, leaving a gap in regulation that is ripe for exploitation by advanced adversaries.

## 4. Research Methodology

### 4.1 Research Design

The design of this study follows Creswell and Poth (2022) and Yin (2018) interpretive tourism and hospitality management research tradition which uses the qualitative multi-case research design. The case-study approach is suitable for research problems involving a complicated context which requires a detailed description, such as in the case of agentic AI threats in service industries (Decrop, 1999). The present study is diagnostic as opposed to predictive, and investigates patterns of structural vulnerability and systemic consequences of these patterns rather than the probability of an attack.

### 4.2 Sources of Data

The data were collected from four main sources:

Systematically reviewed published incident reports from CERT-In, RBI and NPCI and UIDAI for the years 2023-2025. To provide frames of reference for comparison, the researcher has conducted a secondary analysis on cases of international incidents (MGM Resorts 2023; Air India 2024; Marriott 2018/2020). Technical literature was reviewed from credible peer-reviewed and reputed pre-print repositories about the capabilities of agentic AI and the vulnerability of biometrics. The document analysis techniques were used for analyzing regulatory documents under the DPDP Act 2023 and associated UIDAI guidelines.

Thematic analysis (Braun & Clarke, 2006) was used for analysing the data, which were identified inductively from the data, and deductively from the theoretical framework of threat-vector analysis. The process of analysis was divided into three steps: open coding of data, axial coding to find the relationships between the categories of vulnerability, and selective coding to develop a general story on the threat escalation enabled by AI adoption.

**Rationale for the case study approach:**

Among the wide variety of contexts in which hospitality PMS has been found to be largely vulnerable to digital fraud, the three contexts selected for this study were chosen for their empirical salience in the recent digital fraud landscape in India, methodological tractability within the framework of qualitative analysis, and their ability to highlight common and unique aspects of the AI-driven threat environment. The findings of the cross-case comparison were structural patterns instead of individual findings that would weaken the transferability of conclusions to similar contexts.

## 5. Case-Studies of AI-augmented Threat landscape across Three Sectors:

### Case A: AI-Augmented Phishing and PMS Breaches in Indian Hotel Chains

The case involved one of the leading hospitality chains, the MGM Resort in the USA, which offers a learning point for Indian hotel companies. The attack did not exploit a technical flaw, but rather began with a ten-minute phone call in which an attacker feigned the identity of an employee and convinced an IT helpdesk operator to reset credentials. The attack group, called *Scattered Spider*, then deployed the *BlackCat ransomware*, causing losses exceeding USD 100 million for the hotel industry for days on end as cited in the research of Bischoff, (2023). What's interesting about this post incident analysis is that the attacker was able to make a convincing impersonation based on publicly available data from LinkedIn™, and, with AI, any attacker can automate and scale this process to 1,000s of simultaneous targets.

These days, the AI-powered phishing is a *"qualitative leap*" from the previous phishing generations in India. The regular loopholes such as the salutation, language mistakes and artificial urgency were the Red Flags used to identify the traditional phishing attack. These days, the emails are AI-generated from data that's been scraped from social media, job posts from LinkedIn™, and emails between vendors from dark web data dumps, creating emails that are contextually indistinguishable from legitimate emails. *Take for instance*, a hotel GM in Mumbai or Chandigarh that receives an email supposedly sent by the hotel's regional IT security team, and claiming they are in the midst of a software upgrade, is at a significantly higher risk than recipients of earlier phishing attacks.

The integration architecture of Property Management Systems (PMS) is an additional risk. Popular hotel software in India, such as IDS Next, eZee Absolute, Hotelogix, etc. integrates with central reservation systems, payment interfaces, hotel channel managers, and guest loyalty management systems. In principle, a successful exploitation of any node can lead to access to the entire network. According to 2024 CERT-In Sectoral Advisory, PMS systems were identified as one of the top five

targets of incidents in the hospitality industry reported during the year, and the most frequent attack sequences were credential theft and ransomware deployment (CERT-In, 2024). It would necessitate immediate communication to the Data Protection Board under the DPDP Act, 2023, along with to the concerned Data Principal (person) and could result in a fine of up to ₹250 crore for the Data Fiduciary (MeitY, 2023).

The threat vectors in the Indian hospitality industry that are enhanced by Artificial Intelligence are presented in Table 1.

**Table 1: AI Augmented Threat Vectors in Hospitality Sector of India.**

| Threat Vector | Likelihood (2025–26) | Impact (1–10) | Primary Target in India |
|---|---|---|---|
| AI-Personalised Phishing | High | 8 | Front-office & IT helpdesk staff |
| PMS Credential Theft | High | 9 | Mid-scale & budget hotel chains |
| Ransomware-as-a-Service (RaaS) | Medium | 10 | Independent properties & small chains |
| Guest Wi-Fi Interception | High | 6 | Non-chain & budget properties |
| Loyalty Programme Fraud | Medium | 7 | Large chains with reward programmes |

Source: Author's interpretation of the Data collected from CERT-In (2024), RBI (2025) and breach analysis published documents.

## Case B: API Sprawl and Operational Disruption in Indian Aviation.

The aviation industry's cyber security problem is unique and significant in both nature and impact. Unlike a hotel breach, if the attack on an aviation system is successful real-time operations viz. flight scheduling, passenger check-in, baggage system etc. can be affected and even safety adjacent systems. India's civil aviation industry bounced back rather quickly from the contraction due to Covid pandemic to manage more than 150 million domestic travellers in 2024 and at a very fast pace, has the industry built its digital infrastructure (DGCA, 2024).

Indian domestic carriers like IndiGo, Air India Express, and Air Asia are predominantly low-cost carriers that use intricate multi-vendor API systems that link reservations, revenue management, ancillary sales, and ground handling. If these integrations are developed "under the gun" as commercial time pressures under the assumption that there is not much time to spend on security review, the result may be an API with a greater amount of functionality available than was expected, unvalidated inputs, or error messages that expose deep architecture to a probing attacker. According to the OWASP API Security Top 10 list 2024, broken authentication, excessive data exposure, and rate limiting are the 2024 most common issues found in enterprise APIs (OWASP, 2024).

Access to a carrier's public-facing booking API would allow access to an agentic AI system that could systematically probe the system creating thousands of API calls on the client database with different parameters, analysing the returned status codes, and mapping out a list of exploitable endpoints in a fraction of the time that a human attacker would need. An enumeration of booking references that is predictable or can be used to determine booking reference numbers has been previously discovered in Amadeus GDS systems, which power reservation services for a large part of India's airline market

(Papadaki et al., 2023); this issue is not fully addressed in legacy integrations. The Air India data exposure case in 2024 is a good example of how poorly secured APIs for passenger data can have detrimental effects (CERT-In, 2024).

A typical attack scenario would include an agentic AI pattern that can locate a rate-limiting hole in a carrier's refund processing API and make a series of unauthorized "phantom" refund requests in smaller quantities than the anomaly detection will flag. From an operational perspective, the situation where AI-driven threats are targeting the scheduling and slot-managing APIs, which were a major issue at congested airports such as Indira Gandhi International Airport (IGI) and Chhatrapati Shivaji Maharaj International Airport (CSMA) could be far more alarming, with implications reverberating through follow-on flights and the entire tourism supply chain.

### Case C: Biometric Cloning and AePS Exploitation

The exploitation of the Aadhaar-Enabled Payment System (AePS) is perhaps the most pressing threat, and the most socially unfair. Its victims are frequently the very poorest of the poor in Indian society, rural peoples who rely on banking correspondents as their bank of last resort or only bank when it comes to access, and who might be less technologically sophisticated or adept at dealing with their accounts to identify a fraudfully transaction promptly.

AePS fraud has undergone a complete transformation in the past few years. The first wave of attacks involved obtaining victims' Aadhaar numbers (which is quasi-public) and tricking the operators of the biometric scanners to make fake transactions. The new challenge is much trickier: creating synthetic fingerprints from low-resolution source images using AI-assisted reconstruction. India's digitised land records that are available on the various state government land portals such as Bhulekh in Uttar Pradesh, Dharitri in Odisha and Bhunaksha System contain scanned images of the documents with fingerprint impressions taken during the earlier pre-digital land registration process. Recently, Galbally et al. (2023) has shown that deep convolutional neural networks can produce decent quality fingerprint ridges from partial or corrupted source images at measurable rates, and at the same time, they could defeat commercial capacitive scanners.

There have been instances of savings accrued over years via 'AePS' transactions being stolen without the consent of the owners, happening in six states, as reported in the RBI's digital fraud report (RBI, 2025). In response, UIDAI has promoted the concept of 'Lock Aadhaar' feature to temporarily block biometric authentication and prevent misuse of AePS transactions by fraudsters till it is unlocked by the person. The awareness of this service is however, quite low and this is especially the case in rural and semi-urban areas where the penetration of AePS is at its highest (UIDAI, 2025). AePS fraud is directly relevant to the hospitality and tourism sector as there is a growing trend of recruiting staff for these areas from populations that might depend on AePS for salary. To speak of the hotel & tourism sector, manpower is recruited for rural tourism destinations, hill stations, pilgrimage circuits and heritage zones are increasingly relying on AePS for salary.

## 6. Findings and Discussion

### 6.1 Vulnerable Structures:

The three case analyses share a conclusion that goes beyond each sector individually: the digital integration that, as has been reported in the various sectors detailed here, has brought efficiencies and market growth to India's service sector economy has also created a sense of interdependency at the systemic level that makes the impact of any successful cyberattack more pronounced. If a hotel's PMS

is compromised, then it's not just the guests' data that's compromised, it can be payment processors, channel partners, and loyalty program databases as well. If an airline uses its API, the disruption moves on to travel agents, hotel pre-arrivals, and ground transport service providers. Once the ponds are emptied of their savings due to the fraudulent acts of AePS, the spillover effect impacts on local consumption, smallholder tourism activities, and community confidence in digital.

Park et al., in the research of 2024 identifies that this unique quality is precisely what develops an agentic AI as a qualitatively different threat from its early predecessors of cybercrime world. Naturally, prior attacks were resource heavy in nature that could not have been as large. Simultaneous attack across many targets, adapt in real time to defensive reactions, and with near-zero marginal costs, can be done by an AI agent. In the conventional cybersecurity domain, the disparity between attack cost and defence cost is already overwhelmingly skewed in favor of the attackers, and it is getting even worse thanks to the advent of agentic AI.

### 6.2 The influence of the Human Factor

While AI has been a central focus of this analysis, it doesn't mean that the human aspect is unimportant. Even with the aid of artificial intelligence, the primary access point is still social engineering expedients facilitated by known types of human psychological and cognitive fallacies, and this is what both the MGM Resorts case and findings by CERT-In in India displays evidently. While AI can enhance the effectiveness of social engineering, it cannot deceive or fool an individual, nor replace it (Bischoff, 2023; CERT-In, 2024).

These are big vulnerabilities that can be fixed, and are a major concern in the hospitality industry in India, where people in the front-office and IT support roles are rarely trained formally on cybersecurity and where authority hierarchies may make it harder to question requests from seemingly superior individuals. The benefits of systematic awareness training, well-defined verification procedures for credential requests, and an attitude of caution rather than convenience are low cost/high impact defensive investments.

### 6.3 The DPDP Act's regulations:

There is a risk, as well as an opportunity, during the transition period of the implementation of the DPDP Act, the period when regulations are in the process of being finalized and till the time of Data Protection Board's establishment. There is a risk that organisations could postpone compliance investments until the final guidance from the regulator. The opportunity is that organisations that establish strong data governance programs early on will be better prepared when compliance enforcement becomes effective, and will develop "institutional muscle memory" that is hard to get from a pure compliance program as cited by Kapoor and Bhandari (Kapoor & Bhandari, 2024).

The creation of sectoral cybersecurity standards in India, akin to the Payment Card Industry Data Security Standard (PCI-DSS) in the payments industry, which would be specific to the type of data that a hospitality or aviation company handles would help them take concrete steps.

### 6.4 Multi-Layer Mitigation Framework

The following framework synthesizes the findings of this study into practical recommendations organised across three layers: technical controls, institutional practices, and regulatory compliance.

#### a. Technical Layer: Defensive AI and Advanced Identity Verification

The Technical Layer is an AI layer that protects against attacks, along with advanced identity

verification. The best defence against an attack that uses AI is using AI to defend them. Machine learning (ML) can detect abnormal activity like login patterns, statistical unusualness of transaction volume and unusual API call patterns at speeds and scales that human analysts can't keep up with. Indian hotel chains and airlines should focus on investing in AI-powered Security Information and Event Management (SIEM) systems and join aircraft incident-sharing groups which coordinate attack data amongst groups (Park et al., 2024).

As the capability to reconstruct a biometric sample becomes greater to enhance the security of the biometric, the idea of 'Liveness Detection 2.0' and the inclusion of a liveness protocol based on dynamic and unpredictable responses, rather than simple fingerprints, provides a way to maintain biometric security. Retinal micro-movement detection, 3D facial geometry mapping with randomised lighting conditions, and behavioural biometrics (keystroke dynamics, device interaction patterns) are technologies rapidly moving towards commercial application and are candidates for more widespread use in high-risk scenarios (Galbally et al., 2023; UIDAI, 2025). Specific awareness programs, using banking correspondents, Panchayati Raj institutions and rural tourism cooperatives, should be encouraged to facilitate mass adoption of the biometric locking feature of UIDAI's Aadhaar (UIDAI, 2025).

### i. Institutional Layer: Culture, Training and Governance:

Technical controls are needed but not enough. With the MGM Resorts case that showed the fatal error of a single helpdesk interaction, it is no longer a question of whether a USD 2 billion business can be toppled by one helpdesk call—it is an inevitability. Indian hospitality organisations need to make cybersecurity efforts part of the culture, not just a responsibility of the IT department – training should be role-specific, regularly refreshed, and provide realistic simulations rather than instructions to be ticked off a list (Mishra & Singh, 2023).

The governance framework should provide for accountability at the board level. The appointment of a Data Protection Officer (DPO), as provided for by the DPDP Act, should be considered as an opportunity to establish a dedicated privacy function, not just a compliance fitting. A board-level privacy and security committee is the oversight architecture needed to handle the data-handling obligations of a complex patchwork that exists over the different jurisdictions of various hotel chains and airline groups with operations in multiple states.

### ii. The Pro-active DPDP Compliance and Sector-specific Standards:

This form of proactive compliance focuses on regulatory as well as industry sector-specific standards. This is a proactive compliance approach that emphasizes the regulatory or sector-specific standards. It is best for organisations in the hospitality & tourism industry to strive to be proactive in complying with the DPDP Act before enforcement occurs. This will involve auditing data to identify and understand where and what personal data is processed, implementing data minimization as a practice to limit the amount of sensitive data stored and have protocols in place to respond to breaches within the time limits of the Act. Active collaboration with the Ministry of Electronics and Information Technology (MeitY) and UIDAI with the industry associations like FHRAI, HAI and FICCI Tourism Committee to formulate the implementing guidelines for the sector would help fast track the process of converting the principles into operational standards (MeitY, 2023; Kapoor & Bhandari, 2024).

## 7. Conclusion

The paper has suggested that the advent of agentic AI tools is a quantum leap in the cyber threat landscape against India's hospitality, aviation and payment sectors. The danger is not an imaginary one,

but what has been seen in how attacks have been conducted in the last two years by competent regulatory authorities like CERT-In, RBI and UIDAI, and is further compounded by the unique characteristics of the service industry in India, including quick digitization, biometric integrated identity systems and historically less investments in cyber security.

The case analyses above highlight that the "AI + vulnerability" combinations can result in attacks that are both more convincing and harder to detect than traditional attacks while also being much more scalable due to AI capabilities, highlighting the different possibilities of vulnerability and how they connect to the AI capabilities. The key finding is structural: digital integration is economically transformative, and has resulted in systemic interdependencies which magnify the effects of successful attacks across sector boundaries.

This proposed mitigation framework is done through a technical, institutional, and regulatory layer. The most fruitful investments at the technical level include defensive AI, advanced liveness detection and Aadhaar biometric locking. Cybersecurity culture, and specifically in organisations that have high employee turnover and human services-related models, needs to be deliberately developed at the institutional level. Proactive compliance with the DPDP Act and the creation of sector-specific implementing standards will prove critical at the regulatory level to turn DPDP Act requirements into the operation of security improvements. This analysis has implications beyond the scope of this article for hospitality and tourism research as a whole: the discipline must start taking the cyber security aspects of digital transformation seriously. While the tourism literature has been working constructively with the idea of innovation as a competitive advantage, the idea of innovation as a threat to competitive advantage has been relatively under-investigated in the literature. That space will be more expensive for the sector, and more difficult to serve for guests, as the threats listed in this paper grow in intensity and frequency.

## References:

Anthropic. (2024). Claude's character and agentic capabilities: A model card overview. Anthropic Technical Documentation. https://www.anthropic.com

Bischoff, P. (2023, September 15). MGM Resorts cyberattack: What happened and what we know. Comparitech. https://www.comparitech.com/blog/information-security/mgm-resorts-cyberattack/

Bommasani, R., Hudson, D. A., Aditi, E., Altman, R., Arora, S., Koreeda, M., & Liang, P. (2022). On the opportunities and risks of foundation models. arXiv preprint. https://doi.org/10.48550/arXiv.2108.07258

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., & Amodei, D. (2024). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation (2nd ed.). Future of Humanity Institute, University of Oxford.

CERT-In. (2024). Annual cybersecurity report 2024: Sectoral threat landscape. Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology, Government of India.

Creswell, J. W., & Poth, C. N. (2022). Qualitative inquiry and research design: Choosing among five approaches (5th ed.). SAGE Publications.

Decrop, A. (1999). Triangulation in qualitative tourism research. Tourism Management, 20(1), 157–161. https://doi.org/10.1016/S0261-5177(98)00102-2

Directorate General of Civil Aviation (DGCA). (2024). Annual civil aviation statistics 2023–24. Ministry of Civil Aviation, Government of India. https://dgca.gov.in

Galbally, J., Marcel, S., & Fierrez, J. (2023). Biometric antispoofing methods: A survey in face recognition. IEEE

Access, 11, 37892–37915. https://doi.org/10.1109/ACCESS.2023.3265011

Kapoor, A., & Bhandari, V. (2024). The Digital Personal Data Protection Act 2023: Regulatory architecture and implementation challenges. The Centre for Internet and Society, India. https://cis-india.org

MeitY India. (2023). Digital Personal Data Protection Act 2023: Compliance manual and sectoral guidance. Ministry of Electronics and Information Technology, Government of India.

Mishra, R., & Singh, A. (2023). Cybersecurity posture of mid-market Indian hotel chains: An empirical assessment. Journal of Hospitality Information Technology, 15(2), 44–63. https://doi.org/10.1080/19368623.2023.2187341

National Payments Corporation of India (NPCI). (2024). Annual report on UPI transaction ecosystem and fraud risk management 2023–24. NPCI. https://www.npci.org.in

Open Web Application Security Project (OWASP). (2024). OWASP API security top 10 — 2024 edition. OWASP Foundation. https://owasp.org/www-project-api-security/ Papadaki, M., Tryfonas, T., & May, J. (2023). API security in aviation distribution systems: Vulnerability mapping and remediation priorities. Journal of Air Transport Management, 108, 102379. https://doi.org/10.1016/j.jairtraman.2023.102379

Park, J. S., Zou, C., Shaw, A., Hill, B. M., Cai, C., Morris, M., & Bernstein, M. S. (2024). AI and security: The emerging threat of autonomous cyberattack agents. Proceedings of the IEEE Symposium on Security and Privacy, San Francisco.

PricewaterhouseCoopers (PwC). (2019). Marriott International data breach — A case study in post-merger cybersecurity failure. PwC Digital Risk Advisory. https://www.pwc.com

Reserve Bank of India (RBI). (2025). Report on digital fraud in the Indian banking sector 2024–25. Department of Regulation, Reserve Bank of India. https://www.rbi.org.in

Unique Identification Authority of India (UIDAI). (2025). Advancements in biometric security, face authentication, and the Aadhaar locking ecosystem: Annual report 2024–25. UIDAI, Government of India. https://uidai.gov.in

Venkataraman, K. (2024). Digital transformation and cybersecurity risk in Indian low-cost aviation: A post-pandemic analysis. Asian Journal of Transport Policy, 6(1), 112–129. https://doi.org/10.1080/23249935.2024.2203111

Weidinger, L., Uesato, J., Rauh, M., Griffin, C., Huang, P.-S., Mellor, J. & Gabriel, I. (2022). Taxonomy of risks posed by language models. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency (FAccT '22)* (pp. 214–229). ACM. https://doi.org/10.1145/3531146.3533088

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications.