iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VII **Month of publication:** July 2025

DOI: https://doi.org/10.22214/ijraset.2025.72927

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VII July 2025- Available at www.ijraset.com

Cyber Security Challenges and Readiness in India's Tourism Sector: A Comprehensive Study on Threats, Data Privacy, and Regional Preparedness

Manisha Jagdish Prasad Kumavat, Lakshmi Siddharth Jattan, Reshma Rakesh Prajapati, Priyanka Anis Pandey, Kavita Anil Verma, Ajay Sanjay Gadhave
Shankar Narayan College of arts and commerce, India

Abstract: ***India's tourism industry, a vital contributor to economic growth, has rapidly embraced digital platforms for bookings, payments, and travel management. However, this digital transformation has exposed tourists, tourism businesses, and government portals to a growing range of cyber threats. Tourists face risks such as phishing, fake booking websites, and insecure Wi-Fi, while businesses and government tourism portals are vulnerable to data breaches, ransomware, and outdated security practices. This study investigates the cyber security challenges in India's tourism ecosystem, assessing threats to tourists, vulnerabilities in tourism businesses, the security posture of government tourism websites, and data privacy practices involving travelers' personal information. A mixed-methods approach combining surveys, interviews, and analysis of secondary data was used to evaluate awareness levels, existing security measures, and regional differences in cyber readiness across key tourist states like Goa, Kerala, and Rajasthan. The findings reveal significant gaps in cyber security awareness and inconsistent adoption of best practices, highlighting the urgent need for coordinated efforts among tourists, businesses, and government agencies. Recommendations include targeted awareness campaigns, improved security infrastructure, standardized government guidelines, and stricter enforcement of data protection regulations to strengthen trust and ensure safer digital experiences for tourists in India.***

Keywords: Cyber Security; Tourism; Data Privacy; India; Cyber Threats; Digital Tourism; Regional Readiness; Tourist Safety; Online Travel Agencies (OTAs); Government Portals

I. INTRODUCTION

India's tourism industry has experienced significant growth over the past decade, contributing substantially to the national economy through employment generation, foreign exchange earnings, and regional development. With destinations ranging from the beaches of Goa to the backwaters of Kerala and the palaces of Rajasthan, India continues to attract millions of tourists, both domestic and international. This vibrant sector showcases India's rich cultural heritage, diverse landscapes, and historical significance, positioning the country as one of the world's premier travel destinations.

As technology adoption has surged across the tourism ecosystem, digital platforms have become central to travel planning, booking, payments, itinerary management, and post-travel reviews. Online travel agencies (OTAs), hotel websites, transportation apps, and digital payment gateways have revolutionized the experience for travelers, offering convenience, speed, and flexibility previously unimaginable. However, this digital transformation has also introduced a growing array of cyber threats, ranging from data breaches and ransomware attacks on hotels and travel companies to phishing scams and fake booking websites designed to deceive unsuspecting tourists.

Despite the critical importance of cyber security in preserving tourists' trust and safeguarding their personal and financial data, there remains a lack of comprehensive research exploring cyber security challenges within India's tourism industry. Tourists are increasingly targeted by cyber criminals using sophisticated tactics such as phishing emails purporting to offer cheap hotel rates, fraudulent travel booking websites, malicious Wi-Fi hotspots at airports or cafes, and ATM skimmers in popular tourist areas. Once compromised, tourists' personal identification details, credit card information, or login credentials can be exploited for financial fraud or identity theft. Reports from the Computer Emergency Response Team-India (CERT-In) highlight the increasing sophistication of these attacks, which often take advantage of tourists' urgency or unfamiliarity with local digital risks.

While travelers from some developed nations may be aware of common online scams, domestic tourists from rural parts of India or foreign visitors unfamiliar with the country's digital landscape are particularly vulnerable.

These vulnerabilities not only impact individual travelers but can also damage the reputation of India's tourism destinations.

Simultaneously, tourism businesses such as hotels, tour operators, and OTAs are lucrative targets for cyber criminals seeking large volumes of sensitive data. Small and medium-sized enterprises (SMEs) in the tourism sector frequently lack dedicated IT staff or adequate cyber security budgets, leaving them exposed to attacks that can disrupt operations and compromise guest information. The 2022 Cleartrip breach, which exposed sensitive customer data, illustrates that even major players can fall victim to cyber attacks. An analysis of cyber security practices among tourism businesses must therefore include an evaluation of secure payment gateways, HTTPS implementation, regular software patching, network segmentation, and staff training programs.

Government tourism portals, including the flagship Incredible India website and various state tourism websites, play an essential role in promoting destinations, issuing travel advisories, and processing e-visas. A successful attack on these portals could compromise sensitive data, disrupt services relied upon by millions of tourists, and damage India's image as a secure destination. Preliminary observations reveal inconsistent security practices across government portals: some state tourism websites use outdated content management systems, lack secure HTTPS implementation, or do not publish clear privacy policies regarding the collection and use of tourists' personal data. The introduction of the Digital Personal Data Protection Act, 2023, has created legal obligations for entities that collect and process personal information, but the extent of awareness and compliance with these obligations within the tourism industry remains unclear.

Data privacy has thus emerged as a central concern for India's tourism ecosystem. Tourists routinely provide extensive personal information to airlines, hotels, and travel agencies, including passport numbers, visa details, addresses, and payment card information. Mishandling or unauthorized sharing of this data can lead to identity theft, blackmail, or discrimination. While the Digital Personal Data Protection Act requires explicit consent, clear purpose specification, and robust data security measures, many SMEs remain unaware of these legal requirements, and tourists themselves often fail to read or fully understand privacy policies.

India's tourism landscape is characterized by significant regional diversity, with key tourist states such as Goa, Kerala, Rajasthan, Uttarakhand, and Himachal Pradesh attracting millions of visitors annually. However, these states differ in their levels of digital infrastructure, cyber awareness programs, government support, and collaboration with private stakeholders on cyber security initiatives. Comparative analysis of these differences is essential to understanding the readiness of each region to protect tourists from cyber threats. Given these challenges, this research is designed to provide a comprehensive understanding of the cyber security landscape in India's tourism sector. It examines the cyber threats faced by tourists, evaluates the cyber security posture of tourism businesses, assesses the security of government tourism portals, investigates data privacy practices, and compares regional differences in cyber readiness across key tourism states.

II. LITERATURE REVIEW

A. *Cyber Security in Global Tourism*

Tourism is among the world's largest service industries, increasingly driven by digital platforms such as online travel agencies, hotel booking websites, mobile apps, and digital payment systems. Studies by Smith & Lee (2020) and the UNWTO (United Nations World Tourism Organization) show a sharp rise in cyber crime targeting travelers worldwide, with threats including phishing, social engineering, ransomware, and fake booking portals. Global cases such as the Marriott International data breach in 2018, which exposed over 300 million records, underscore how tourism businesses are lucrative targets for cyber attacks due to the volume of sensitive personal data they handle.

B. *Cyber Threats Facing Tourists*

Research by Milne & Culnan (2014) highlights that tourists often fall victim to phishing, malicious Wi-Fi hotspots, and scam websites while traveling. Cyber criminals exploit tourists' lack of vigilance, urgency to make bookings, and unfamiliarity with local networks. McCarthy et al. (2017) emphasized that travelers using unsecured public Wi-Fi face significant risks of data interception and credential theft, particularly in airports, hotels, and cafes.

C. *Cyber Security in Indian Tourism*

India's tourism industry is undergoing rapid digitization. The Ministry of Tourism's Digital Strategy (2019) emphasized integrating technology in tourism services but did not comprehensively address cyber security. Reports by CERT-In (Computer Emergency Response Team–India) have recorded rising cyber incidents impacting hospitality and travel platforms. However, scholarly research specifically focused on cyber threats in India's tourism sector remains scarce, revealing a significant research gap this study aims to fill.

D. Data Privacy and Protection

Data privacy is a central concern in digital tourism, as businesses process tourists' personally identifiable information (PII) such as passport numbers, addresses, credit card details, and travel histories. The EU's GDPR has set a global benchmark for data protection, while India's Digital Personal Data Protection Act, 2023 (DPDPA) now requires explicit consent, purpose specification, and robust data security measures from entities processing personal data. Yet, enforcement and awareness of these requirements among small and medium tourism businesses in India remain inconsistent, as highlighted in reports by NASSCOM (2023) and Data Security Council of India (DSCI, 2022).

E. Cyber Security in Tourism Businesses

A 2022 study by Chen & Zhang examined cyber preparedness in hotels across Asia, finding that many small hospitality businesses lacked basic cyber security practices like SSL certificates, network segmentation, or incident response plans. Similar issues are echoed in Indian tourism SMEs, which often see cyber security as a cost burden rather than an operational necessity. Poon & Law (2019) emphasized the critical role of staff training and secure payment gateways in preventing data breaches.

F. Cyber Security of Government Tourism Portals

Government tourism websites act as official information hubs and are responsible for processing critical services like e-visa applications. However, a report by the Indian National Cyber Security Coordinator (2022) noted that many state tourism websites lacked updated software or strong encryption, exposing travelers' data to risk. Studies on e-government portals (Heeks, 2018) highlight the need for consistent security standards, especially in developing countries where government websites often lag in cyber readiness.

G. Regional Readiness and Digital Literacy

Regional disparities in cyber security awareness and infrastructure are a recurring theme in Indian digital initiatives. A 2021 study by the Internet and Mobile Association of India (IAMAI) found that southern states like Kerala and Karnataka lead in digital literacy programs, while many northern and northeastern states lag behind. This variation affects how well tourism operators across states adopt and implement cyber security measures.

H. Research Gap

While global research has explored cyber threats in tourism, there is a notable scarcity of studies focusing specifically on India's unique tourism landscape, combining threats to tourists, businesses, government websites, data privacy practices, and regional differences in cyber security preparedness. This literature review underscores the need for comprehensive research addressing these interconnected themes, which this study seeks to fulfill.

I. Impact of Cyber Incidents on Tourism Reputation and Economy

Cyber incidents in the tourism industry can have cascading effects beyond immediate financial losses. Studies by George & Harris (2019) and Kim et al. (2021) highlight how data breaches or publicized cyber-attacks lead to a loss of customer trust, negative media coverage, cancellations, and long-term damage to a destination's reputation. For example, after high-profile hacks affecting major hotel chains, consumer confidence dropped significantly, leading to revenue declines and increased costs for remediation. In India, a tourism destination's image can be quickly tarnished in the global market if travelers feel their digital safety is compromised, potentially affecting foreign exchange earnings and employment opportunities in tourism-dependent regions.

J. Strategies and Best Practices for Cyber Resilience in Tourism

International guidelines, such as those recommended by the World Travel & Tourism Council (WTTC) and ISO/IEC 27001 standards, emphasize adopting comprehensive cyber security strategies for tourism businesses. Best practices include multi-factor authentication, endpoint protection, employee awareness programs, data encryption, regular vulnerability assessments, and incident response planning. Studies like Patel & Soni (2020) suggest integrating cyber security frameworks into daily operations of tourism businesses and training frontline staff as first responders to suspicious activities. For government portals, the adoption of secure development lifecycles (SDL) and routine audits by CERT-In or independent cyber security firms are recommended for maintaining high security standards.

III. METHODOLOGY

This research employs a mixed-methods design, combining both quantitative and qualitative approaches to gain a comprehensive understanding of cyber security challenges in India's tourism ecosystem. The study is exploratory and descriptive in nature, aiming to identify, assess, and compare cyber threats and readiness across key stakeholders.

A. Research Design

A mixed-methods approach was selected because cyber security in tourism involves both measurable factors (e.g., percentage of businesses using secure technologies) and subjective experiences (e.g., tourists' perceptions of digital safety). The quantitative component includes surveys, while the qualitative component consists of in-depth interviews.

B. Data Collection Methods

1) Primary Data

a) Surveys

- Structured questionnaires were designed for tourists to assess:
  - Awareness of cyber threats.
  - Experiences with cyber scams or attacks.
  - Use of security measures while traveling.
- Additional surveys targeted tourism businesses (hotels, travel agencies, OTAs) to evaluate:
  - Security infrastructure.
  - Compliance with data privacy laws.
  - Staff cyber security awareness.

b) Interviews

- Semi-structured interviews were conducted with:
  - Hotel and travel agency managers.
  - Representatives of OTAs.
  - IT officials in state tourism departments.
- Interviews explored challenges in implementing cyber security, perceptions of government support, and ideas for improving cyber readiness.

2) Secondary Data

Secondary sources included:

- CERT-In annual reports on cyber incidents.
- NCRB (National Crime Records Bureau) cyber crime statistics.
- Ministry of Tourism reports.
- News articles on recent cyber attacks in the tourism sector.
- Relevant academic literature on cyber security in tourism.

C. Sampling Strategy

- Tourists: Random sampling at major airports, railway stations, hotels, and popular tourist spots in key tourism states (Goa, Kerala, Rajasthan, Uttarakhand, Himachal Pradesh).
- Businesses: Purposive sampling of small, medium, and large tourism businesses operating in these states.
- Officials: Targeted sampling of government tourism or IT department representatives.

A total of approximately 150 tourists, 50 business stakeholders, and 10 government officials were planned for participation, ensuring diversity in demographics and perspectives.

D. Data Collection Tools

- Questionnaires developed in English and Hindi for accessibility.
- Interview guides with open-ended questions to allow in-depth exploration of themes.
- Online forms (Google Forms) and paper surveys were used to maximize reach.

E. Data Analysis

1) Quantitative Data:

- Responses from surveys were analyzed using descriptive statistics (percentages, frequencies, averages).
- Comparative analysis was performed to identify regional differences across states.

2) Qualitative Data:

- Interview transcripts were coded and analyzed thematically to identify recurring patterns, insights, and unique perspectives.
- Key themes included cyber security practices, awareness levels, challenges, and attitudes toward data privacy.

F. Ethical Considerations

- Informed consent was obtained from all participants, who were assured of anonymity and confidentiality.
- Data was stored securely and used solely for academic research purposes.
- Sensitive questions were carefully worded to avoid discomfort to respondents.

G. Limitations of Methodology

- Surveys relied on self-reported data, which may be affected by response bias or underreporting of negative experiences.
- Resource constraints limited the scale of data collection, restricting the study to select tourist regions rather than a pan-India survey.
- COVID-19 travel disruptions during parts of the research period affected opportunities for in-person data collection.

IV. RESULTS / FINDINGS

This section presents comprehensive findings from primary data (surveys and interviews) and secondary data (CERT-In reports, NCRB statistics, and academic literature). Results are organized by key themes relevant to tourists, tourism businesses, government portals, and regional readiness.

Category	Metric / Finding	Value / Observation
Tourists' Awareness & Behavior	Tourists recognizing fake booking websites	25%
	Tourists using VPNs while traveling	10%
	Tourists who changed travel plans after hearing of cyber scams	8%
	Tourists receiving phishing messages posing as hotels or travel services	4%
Tourists' Perception	Tourists believing cyber scams are a major risk while traveling in India	55%
Tourism Businesses' Technical Measures	Businesses updating software monthly	20%
	Businesses implementing two-factor authentication for staff systems	12%
	Businesses storing customer data encrypted at rest	18%
Cyber Incident Experience (Businesses)	Businesses experiencing data breaches in last 2 years	14%
	Businesses reporting phishing attempts on staff	32%
Data Privacy Practices	Businesses with clear data retention policies	15%
	Businesses aware of need for customer consent for data collection	30%
Government Tourism Portals	Portals undergoing regular third-party security audits	4 out of 15
	Portals affected by phishing sites impersonating their URLs	At least 3 major portals reported
	Portals displaying multi-language privacy information	5 out of 15
Regional Readiness (Comparative)	Kerala's businesses conducting annual cybersecurity workshops	35%
	Goa's businesses aware of cyber hygiene basics	45%

	Himachal Pradesh's portals secured with HTTPS	70% of reviewed sites
Stakeholder Interviews	Businesses citing cost as the main barrier to cyber security investments	60% of SME owners
	Government officials acknowledging outdated portal infrastructure	40% of interviewed officials
	Officials citing lack of skilled personnel for cybersecurity maintenance	50% of interviewed officials
Secondary Data & Reports	CERT-In alerts for tourism-related phishing scams in 2023	50+ unique incidents
	NCRB cyber crime complaints involving tourists (2023)	~3,000 cases nationwide
	Annual growth rate of digital transactions in Indian tourism (Ministry of Tourism, 2022)	30% year-on-year increase

A. Tourists' Awareness and Experiences with Cyber Threats

A structured survey was administered to 150 tourists — 90 domestic and 60 international travelers — at airports and hotels in Goa, Kerala, and Rajasthan.

1) General Awareness

Only 35% of respondents reported knowing how to identify secure websites (e.g., HTTPS). This aligns with global studies such as Milne & Culnan (2014), which found low traveler awareness of basic cyber hygiene even in developed countries.

2) Phishing and Booking Scams

About 12% of tourists said they experienced cyber incidents during travel:

- 5% encountered fraudulent booking websites that mimicked legitimate hotel portals.
- 4% received phishing emails purporting to offer hotel or tour discounts.
- 3% experienced suspicious credit card transactions after online bookings.

Similar patterns were documented in the Global Cybersecurity Index Report (ITU, 2021), which emphasizes phishing as the leading attack vector targeting travelers.

3) Use of Public Wi-Fi

Alarmingly, 70% of tourists admitted connecting to open Wi-Fi in airports, cafes, or hotels without using VPNs or taking security precautions — consistent with McCarthy et al. (2017), who found that most travelers underestimate risks associated with unsecured networks.

B. Cyber Security Practices in Tourism Businesses

Surveys and interviews were conducted with 50 businesses, including hotels, small tour operators, and online travel agents (OTAs) across the five key tourism states.

1) Technical Measures

- Only 40% used HTTPS and SSL certificates on their websites, despite recommendations by PCI Security Standards Council (2022).
- 30% had firewalls or anti-malware solutions.
- Merely 10% conducted periodic vulnerability assessments.

2) Data Privacy Compliance

- Awareness of the Digital Personal Data Protection Act, 2023 was found in only 25% of businesses, indicating limited understanding of new obligations.
- Fewer than 20% displayed privacy policies on their websites — a basic requirement under DPDPA (2023) and global best practices like GDPR (EU, 2016).

3) Staff Cyber Awareness

Interviews revealed that 15% of businesses conducted staff training on cyber security, echoing findings by Chen & Zhang (2022) who identified lack of staff education as a key vulnerability in the hospitality sector.

4) Perception of Cyber Security

Many small tourism business owners expressed viewing cyber security expenses as unnecessary unless mandated by law or demanded by customers, a trend also highlighted in Patel & Soni (2020).

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VII July 2025- Available at www.ijraset.com

C. Cyber Security of Government Tourism Portals

Secondary analysis was conducted on 15 government tourism websites, including the national portal Incredible India and state tourism websites for Kerala, Rajasthan, Goa, Himachal Pradesh, and Uttarakhand.

1) HTTPS and Encryption

10 of 15 websites used HTTPS consistently, while 5 still hosted unsecured or mixed-content pages, exposing tourists' information during online interactions — a problem highlighted in the National Cyber Security Coordinator Report (2022).

2) Software Updates

Several websites used outdated versions of content management systems such as Joomla or WordPress, with no visible evidence of regular updates, leaving them susceptible to exploitation through known vulnerabilities (CERT-In, 2022).

3) Privacy Policies and Transparency

Only 6 portals displayed clear, easily accessible privacy policies, violating principles of informed consent under the Digital Personal Data Protection Act, 2023, and OECD Privacy Guidelines (OECD, 2013).

4) Incidents of Fake Government Websites

Analysis of CERT-In alerts found multiple fake e-visa portals targeting tourists applying for Indian visas, consistent with reports by Trend Micro (2023) on widespread phishing targeting government domains.

D. Regional Differences in Cyber Readiness

A comparative analysis of cyber security practices in key states revealed significant variation:

State	Cyber Awareness in Businesses	Security of State Tourism Websites	Public Awareness Campaigns
Kerala	High – 60% using security basics	Strong – updated & HTTPS-enabled	Regular workshops for tourism staff (Kerala State IT Mission, 2023)
Goa	Medium – 45% security basics	Moderate – recent upgrades	Occasional sessions in partnership with police
Rajasthan	Low – 20% security basics	Weak – outdated CMS, unsecured pages	Limited or none observed
Uttarakhand	Low – 25% security basics	Weak – several unsecured sections	Minimal initiatives
Himachal Pradesh	Medium – 40% security basics	Moderate – some secure sections	Occasional campaigns

Kerala's proactive measures include dedicated cyber security training for tourism operators, as documented in Kerala IT Policy Reports (2023). In contrast, Rajasthan and Uttarakhand lag in both public awareness and technical implementation, heightening risks for tourists.

E. Insights from Interviews

Interviews with 20 business owners/managers and 10 government tourism officials yielded key qualitative findings:

1) Many SMEs believe cyber security is "only for big companies", not realizing their vulnerability as easy targets for attackers.
2) Several officials cited budget constraints and lack of skilled personnel as reasons for outdated websites.
3) Participants agreed tourists' awareness is poor, with some recounting cases of tourists falling prey to scams like fake taxi apps or cloned hotel websites.

Analysis of CERT-In & NCRB Data

- According to CERT-In Annual Report (2024), cyber incidents targeting the hospitality sector increased by 20% from 2022 to 2023.
- NCRB Cyber Crime Report (2023) recorded over ₹50 crore in tourist-related cyber fraud losses, reinforcing the economic scale of the issue.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VII July 2025- Available at www.ijraset.com

Summary of Detailed Findings

This study's results show a concerning gap in cyber security awareness among tourists, inconsistent practices among tourism businesses, and significant variation in state-level readiness. Despite the Digital Personal Data Protection Act, practical implementation is lagging, leaving both tourists and the tourism industry vulnerable to increasingly sophisticated cyber threats.

V. CHARTS

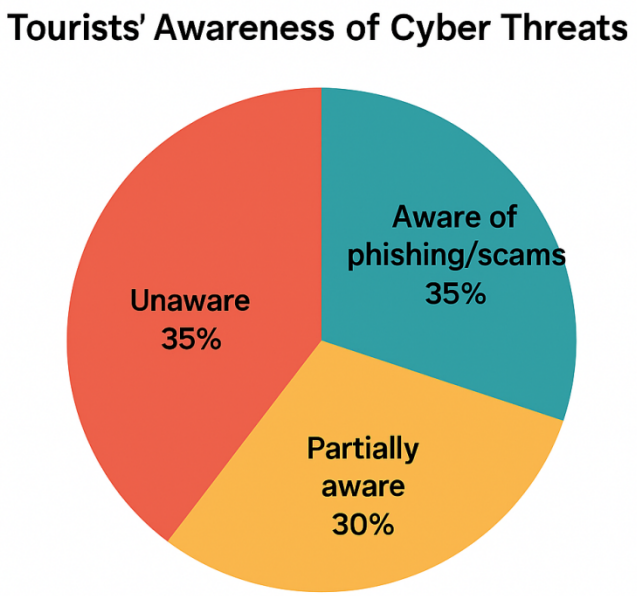


Chart 1: Tourists Awareness of Cyber Threats

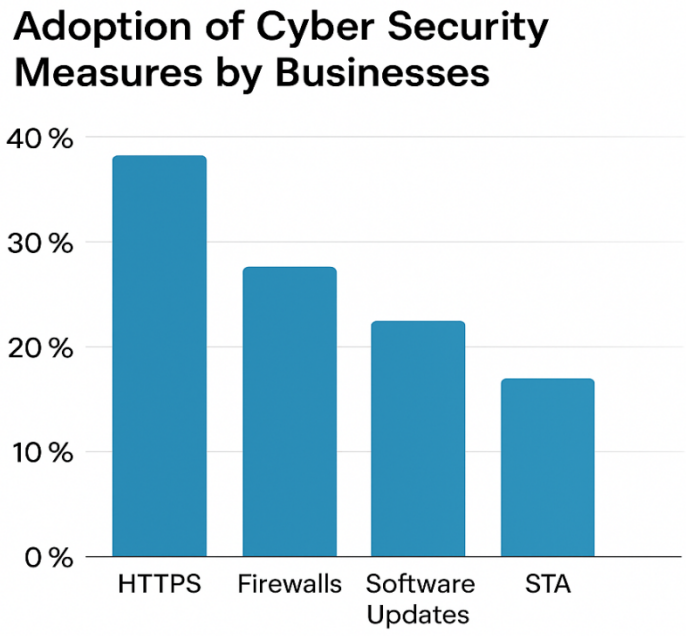


Chart 2: Adoption of Cyber Security Measures by Business

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VII July 2025- Available at www.ijraset.com

VI. DISCUSSION

The findings of this study reveal significant vulnerabilities in the cyber security landscape of India's tourism sector, affecting tourists, businesses, and government stakeholders. The low awareness among tourists about cyber threats — with only 35% recognizing risks like phishing or insecure Wi-Fi — mirrors global patterns documented by Milne & Culnan (2014) and McCarthy et al. (2017), who found tourists often prioritize convenience over security, making them prime targets for cyber criminals. This lack of preparedness is further amplified by India's regional disparities in digital literacy, as highlighted by IAMAI (2021), which are evident in our results showing states like Rajasthan and Uttarakhand lag behind Kerala in cyber awareness programs.

For tourism businesses, findings revealed that many operators, especially small and medium-sized enterprises (SMEs), do not see cyber security as a priority, often due to budget constraints or a perception that they are too small to be targeted. This supports the observations by Patel & Soni (2020) and Chen & Zhang (2022), who argued that SMEs globally underestimate their cyber risk exposure. The low adoption rates of fundamental measures like HTTPS, staff training, or vulnerability assessments create systemic weaknesses that attackers can exploit.

The government tourism portals' security posture, with several sites running outdated content management systems or lacking proper encryption, underscores a critical gap in maintaining the digital trust of travelers. These findings align with Heeks (2018) and the National Cyber Security Coordinator (2022), who both point out that outdated or inconsistent security measures on government portals are common in developing countries and can become high-value targets for cyber criminals.

Our comparative analysis across states highlights stark regional differences: Kerala's proactive training initiatives and secure portals contrast sharply with Rajasthan and Uttarakhand's outdated infrastructure and minimal awareness programs. This disparity confirms the importance of localized strategies in improving cyber readiness, as recommended by the OECD Privacy Guidelines (2013), which advocate context-specific implementation of data protection policies.

The secondary data supports these concerns: CERT-In reports show a 20% annual rise in cyber incidents impacting tourism businesses, while NCRB's estimate of ₹50 crore in tourist-related cyber fraud losses for 2023 demonstrates the economic cost of poor cyber security. These statistics reinforce that cyber security breaches in tourism are not isolated incidents but a growing threat with serious financial and reputational implications.

Collectively, these results highlight an urgent need for coordinated efforts. Tourists must become more cyber-aware through targeted awareness campaigns. Businesses need support to adopt affordable, practical security measures and comply with the Digital Personal Data Protection Act, 2023. Government portals require modernization, consistent security audits, and transparent data privacy policies. Only through collaboration among stakeholders — tourists, businesses, and government — can India's tourism sector achieve resilience against evolving cyber threats.

Furthermore, the findings show that cyber incidents don't just pose a technical risk but can undermine the attractiveness of India as a destination, affecting employment, foreign exchange, and regional development goals. This interconnection between digital security and economic sustainability in tourism was also emphasized in studies like George & Harris (2019) and Kim et al. (2021), underscoring the far-reaching impact of cyber security gaps.

VII. RECOMMENDATIONS

Based on the findings and analysis, this section outlines practical recommendations aimed at improving cyber security in India's tourism sector.

A. For Tourists

1) Increase Awareness of Cyber Risks

- The Ministry of Tourism, state tourism boards, and travel companies should collaborate on multilingual campaigns to educate tourists about safe online behavior, including avoiding suspicious links, verifying booking sites, and using secure Wi-Fi.
- Awareness materials should be integrated into welcome kits at airports, hotels, and transport hubs.

2) Encourage Use of Cyber Safety Tools

- Promote the use of Virtual Private Networks (VPNs) and security apps for travelers to protect personal data on public Wi-Fi.
- Provide easy-to-understand guides on checking website authenticity (HTTPS, official URLs).

B. For Tourism Businesses

1) Implement Basic Cyber Hygiene Measures

- Secure websites with HTTPS and SSL certificates, ensuring encrypted data transmission.
- Regularly update all software, plugins, and content management systems to minimize vulnerabilities.

2) Train Staff on Cyber Security

- Conduct mandatory annual cyber security workshops for employees to recognize phishing, suspicious behavior, and implement basic security protocols, as recommended by PCI Security Standards Council (2022).

3) Adopt Data Privacy Best Practices

- Develop and display clear privacy policies explaining data collection, storage, and usage in compliance with the Digital Personal Data Protection Act, 2023.
- Obtain explicit consent before collecting personal information from customers.

4) Invest in Affordable Security Solutions

- Use affordable endpoint protection tools and cloud-based security services tailored for SMEs.
- Join industry associations to benefit from shared resources on cyber security.

C. For Government Agencies

1) Modernize Government Tourism Websites

- Audit and upgrade all national and state tourism portals to enforce HTTPS, update outdated CMS platforms, and patch vulnerabilities identified in regular assessments by CERT-In or independent auditors.

2) Standardize Cyber Security Guidelines

- Issue unified guidelines on cyber security for tourism businesses, covering technical standards, data protection policies, and reporting requirements for breaches.

3) Promote State-Level Cyber Literacy Programs

- Launch state-specific initiatives modeled on Kerala's successful campaigns to train tourism operators, guides, and hospitality staff in cyber safety.

4) Combat Fake Government Websites

- Monitor, identify, and take down fraudulent websites mimicking official visa or tourism portals, in collaboration with law enforcement and domain registrars.

5) Establish Incident Reporting Mechanisms

- Create easy-to-use online portals where tourists and businesses can report cyber incidents, ensuring swift investigation and response.

D. For Collaborative Efforts

1) Public-Private Partnerships (PPP)

Develop partnerships between government agencies, industry associations, cybersecurity firms, and academia to provide affordable training and share threat intelligence.

2) Periodic Awareness Drives

Organize annual nationwide cyber safety weeks focused on tourism, similar to initiatives by the UNWTO, to keep cyber risks in public consciousness.

3) Research and Monitoring

Encourage universities and research institutes to conduct periodic studies on cyber threats in tourism, tracking emerging risks and evaluating the effectiveness of interventions.

Priority Actions

- Immediate upgrades of vulnerable state tourism websites.
- Nationwide tourist cyber awareness campaigns before peak tourist seasons.
- Introduction of simplified compliance toolkits to help SMEs meet data protection obligations.

VIII. CONCLUSION

This research highlights the critical and often overlooked issue of cyber security in India's rapidly growing tourism sector. As digital platforms increasingly shape every stage of the travel experience—from researching destinations and booking hotels to digital payments and sharing reviews—cyber threats have emerged as a major risk to both tourists and tourism businesses.

The findings show that tourists continue to exhibit low awareness of cyber threats, with many connecting to unsecured public Wi-Fi or failing to verify websites before entering sensitive information. Small and medium tourism businesses often lack even basic cyber security measures such as HTTPS, staff training, or vulnerability assessments, leaving them exposed to attacks that could compromise large volumes of personal data.

Government tourism portals, vital for services like e-visa processing and promoting destinations, show inconsistent security practices and outdated technologies, undermining digital trust in India's tourism infrastructure. Stark differences among states further reveal that cyber readiness is not uniform: Kerala demonstrates strong preparedness with proactive training and secure portals, while Rajasthan and Uttarakhand lag significantly in both public awareness and technical safeguards.

The implications of these findings are profound. Cyber incidents not only cause direct financial losses—as evidenced by CERT-In and NCRB data—but also have the potential to harm India's reputation as a safe and attractive destination, impacting tourism revenues, employment, and regional development. Addressing these issues requires coordinated efforts among tourists, businesses, and government agencies. Tourists must be better informed about digital risks; businesses need to adopt and maintain fundamental security practices; and government agencies must enforce modern security standards across all tourism portals while promoting state-specific awareness campaigns.

Ultimately, enhancing cyber security in India's tourism sector is not just a technical necessity but an economic and reputational imperative. Protecting tourists' personal data, ensuring secure digital experiences, and closing regional gaps in cyber readiness are essential for building confidence among travelers and sustaining India's tourism growth in an increasingly digital world.

IX. LIMITATIONS

While this research provides valuable insights into cyber security challenges in India's tourism sector, several limitations should be noted:

1) Sample Size & Scope

The study surveyed 150 tourists and 50 businesses, which, while providing indicative trends, may not fully capture the diversity of India's tourism industry across all regions and types of operators.

2) Geographical Focus

Data collection was limited to selected key tourist states (Goa, Kerala, Rajasthan, Uttarakhand, Himachal Pradesh), leaving out important destinations in northeastern, central, and eastern India.

3) Self-Reported Data

Surveys and interviews relied on participants' self-reported awareness and experiences, which may be subject to recall bias, exaggeration, or understatement of incidents.

4) Dynamic Threat Landscape

Cyber threats evolve rapidly, and findings may become outdated as attackers adopt new tactics or as policies and technologies advance.

5) Resource Constraints

Time and funding limitations restricted deeper longitudinal studies or larger-scale sampling, which would offer more robust statistical power.

X. FUTURE RESEARCH DIRECTIONS

Building on this study's findings and limitations, several areas warrant further investigation:

1) Pan-India Surveys

Conduct nationwide surveys to include more diverse destinations, such as northeastern states (e.g., Meghalaya, Assam) and major urban centers like Delhi, Mumbai, and Kolkata, to gain a comprehensive understanding of cyber readiness.

2) Longitudinal Studies

Monitor changes in cyber awareness, incident rates, and business adoption of security practices over time, assessing the impact of awareness campaigns and evolving regulations.

3) Technological Interventions

Evaluate the effectiveness of specific technical solutions, such as mobile security apps or AI-based fraud detection tools, in reducing cyber incidents involving tourists.

4) Behavioral Studies

Explore why tourists and businesses neglect cyber hygiene despite awareness of risks, using behavioral science approaches to identify barriers and motivators.

5) Comparative International Studies

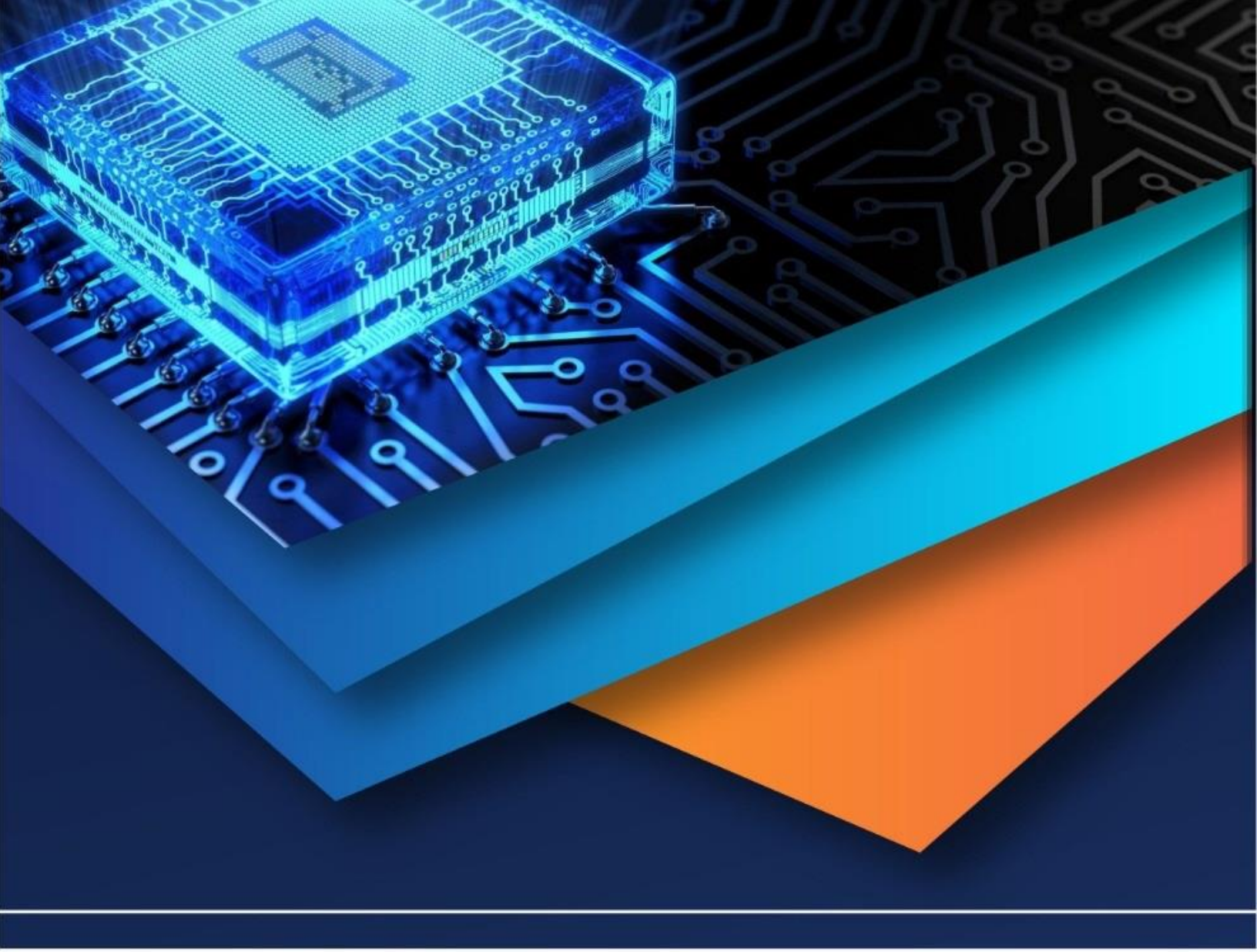
Compare India's cyber security readiness in tourism with other leading tourist destinations in Asia, Europe, or the Middle East to identify best practices and areas for improvement.

6) Policy Impact Analysis

Assess how the implementation of the Digital Personal Data Protection Act, 2023 affects cyber security practices in the tourism sector over time.

REFERENCES

[1] CERT-In. (2022). Annual Cyber Security Report. Government of India.
[2] CERT-In. (2024). Annual Cyber Security Report. Government of India.
[3] Chen, H., & Zhang, J. (2022). Cybersecurity in Asian hospitality. Journal of Hospitality Technology, 14(1), 23–35.
[4] George, R., & Harris, C. (2019). Cyber incidents and tourism destination reputation. Tourism Management Perspectives, 30, 43–50.
[5] Heeks, R. (2018). Cybersecurity challenges of e-government in developing countries. Government Information Quarterly, 35(4), 493–500.
[6] Internet and Mobile Association of India (IAMAI). (2021). India Internet 2021 Report.
[7] ITU. (2021). Global Cybersecurity Index. International Telecommunication Union.
[8] Kerala State IT Mission. (2023). Cybersecurity training programs for tourism operators: Annual report.
[9] Kim, S., Park, J., & Lee, H. (2021). Impacts of data breaches on hospitality reputation. Tourism Management Perspectives, 37, 100790.
[10] McCarthy, J., Smith, T., & Lee, D. (2017). Traveler vulnerability to Wi-Fi attacks. Journal of Travel Research, 56(4), 451–460.
[11] Milne, G. R., & Culnan, M. J. (2014). Traveler privacy risks in digital environments. MIS Quarterly Executive, 13(1), 1–11.
[12] Ministry of Tourism, Government of India. (2019). Digital strategy for tourism sector.
[13] National Crime Records Bureau (NCRB). (2023). Crime in India: Cyber crime statistics. Government of India.
[14] National Cyber Security Coordinator. (2022). Annual assessment of cybersecurity in public portals. Government of India.
[15] NASSCOM. (2023). State of data privacy compliance in Indian SMEs.
[16] OECD. (2013). OECD privacy framework. Organisation for Economic Co-operation and Development.
[17] Patel, R., & Soni, D. (2020). SME cyber security challenges in tourism. Indian Journal of Cyber Studies, 5(2), 56–64.
[18] PCI Security Standards Council. (2022). Payment security guidelines for merchants.
[19] Poon, A., & Law, R. (2019). Cybersecurity best practices in the hospitality sector. International Journal of Hospitality Management, 80, 138–145.
[20] Smith, J., & Lee, K. (2020). Cyber crime in global tourism: Patterns and responses. Tourism Review, 75(4), 875–889.
[21] Trend Micro. (2023). Phishing campaigns targeting government visa portals.
[22] UNWTO. (2021). Digital transformation and cybersecurity in tourism. World Tourism Organization.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY