Preventive Cyber Security Strategies for Sustainable Digital Tourism: A Systematic Review

M.P.Prathiba[1] and R.Tamil Selvi[2*]

[1]*Assistant Professor, Department of Commerce, Hindusthan College of Arts & Science (Autonomous), Coimbatore, Tamil Nadu*

Email: anusrisivakumar@gmail.com

[2]*Assistant Professor, Department of Commerce, Hindusthan College of Arts & Science (Autonomous), Coimbatore, Tamil Nadu*

**Corresponding Author Email: miruthultamil1983@gmail.com*

Abstract

This systematic literature review examines preventive cyber security strategies that support the sustainability of digital tourism by protecting digital platforms, traveller data, and tourism stakeholders from cyber threats. The increasing use of online booking systems, mobile applications, smart tourism technologies, and digital payment platforms has improved efficiency in the tourism sector while simultaneously increasing exposure to risks such as data breaches, payment fraud, and system disruptions. The review synthesizes findings from relevant academic literature to identify major cyber risks and evaluate key preventive measures, including risk assessment, secure system design, data protection practices, regulatory compliance, employee training, and the use of advanced technologies such as artificial intelligence and block chain. The findings indicate that effective preventive cyber security practices enhance consumer trust, ensure service reliability, and contribute to the long-term economic and technological sustainability of digital tourism ecosystems. The review also highlights research gaps related to integrated cyber security frameworks and the limited focus on small and medium tourism enterprises, suggesting directions for future research and policy development.

Keywords: Cyber security, Digital Tourism, Preventive Strategies, Sustainable Tourism, Cyber Risk Management

1.Introduction

The tourism and travel industry has experienced rapid digital transformation through the adoption of online booking platforms, mobile applications, digital payment systems, and smart

tourism technologies. These digital innovations have enhanced operational efficiency, expanded global reach, and improved tourist experiences while supporting sustainable tourism practices through better resource utilization and service delivery. However, the increasing reliance on digital systems has also heightened vulnerability to cyber security threats such as data breaches, identity theft, payment fraud, ransomware attacks, and system failures, posing serious risks to tourism organizations and travellers alike.

Tourism businesses manage large volumes of sensitive personal and financial information, making cyber security a critical factor in maintaining trust, service reliability, and long-term sustainability. Cyber incidents can lead to financial loss, reputational damage, regulatory penalties, and erosion of consumer confidence, directly affecting the viability of digital tourism platforms. Preventive cyber security strategies—such as proactive risk assessment, secure system architecture, data protection mechanisms, regulatory compliance, employee training, and the use of advanced technologies—are essential to mitigate these risks. Despite growing awareness, research on preventive cyber security in tourism remains fragmented. This systematic literature review aims to synthesize existing studies to identify key preventive strategies, assess their role in sustainable digital tourism, and highlight gaps for future research and policy development.

2.Literature review

Many studies show that the tourism and travel industry is increasingly dependent on digital technologies such as online booking platforms, mobile apps, digital payment systems, and smart tourism tools. While these technologies improve convenience and efficiency, researchers point out that they also increase the risk of cyber threats. Common problems identified in the literature include data breaches, hacking, identity theft, online payment fraud, phishing attacks, and system failures, all of which can harm tourism businesses and reduce customer trust.

Researchers agree that preventive cyber security strategies are essential to reduce these risks before they occur. The literature highlights measures such as regular risk assessment, secure system design, data encryption, privacy protection, and compliance with data protection laws. Many studies also stress the importance of employee training and awareness, as human mistakes are a major cause of cyber security incidents. Recent research discusses the use of advanced technologies like artificial intelligence and block chain to improve threat detection and secure digital transactions. Overall, the literature suggests that strong preventive cyber security practices help build trust, protect sensitive information, and support the long-term

sustainability of digital tourism. However, existing studies are limited and fragmented, especially in relation to small tourism businesses, showing the need for further research.

2.1 What really is cyber security?

Cyber security is the practice of **protecting computers, networks, systems, and digital data from unauthorized access, attacks, damage, or theft.** It focuses on keeping information **safe, private, and reliable** when people use digital technologies such as the internet, mobile apps, online payment systems, and cloud platforms.

In simple terms, cyber security ensures that digital information is protected in three key ways: **confidentiality** (only authorized people can access data), **integrity** (data is accurate and not altered without permission), and **availability** (systems and information are accessible when needed). Cyber security includes preventive actions such as using strong passwords, encryption, firewalls, antivirus software, secure networks, regular system updates, and user awareness training. In sectors like digital tourism and travel, cyber security is essential to protect customer data, online transactions, and business operations, helping to build trust and ensure safe and sustainable digital services.

2.2 Cyber security in the context of the tourism industry

Cyber security in the tourism industry refers to the protection of digital systems, online platforms, and sensitive customer information used by tourism organizations such as airlines, hotels, travel agencies, and online booking services. The industry heavily depends on digital technologies for reservations, payments, customer data management, and smart tourism services, which increases exposure to cyber threats like data breaches, payment fraud, phishing, and ransomware attacks. Since tourism businesses handle large volumes of personal and financial data, any cyber security failure can lead to financial loss, reputational damage, legal consequences, and loss of customer trust. Therefore, effective cyber security measures—such as secure IT systems, data protection practices, employee awareness, and compliance with regulations—are essential to ensure safe digital transactions, service continuity, and the long-term sustainability of the tourism sector.

2.3 The number of cyber-attacks has increased in the air transport industry

In recent years, the air transport industry has experienced a notable rise in cyber-attacks, underscoring growing vulnerabilities as aviation systems become increasingly digital and interconnected. Between 2022 and 2023, global data on aviation cyber security revealed that cyber-attacks increased by approximately 131%, highlighting an accelerated threat landscape facing airlines, airports, and air traffic management systems. Additionally, specialized studies

have reported sharp upticks in various attack types—including credential theft, ransomware, and distributed denial-of-service (DDoS) campaigns—with some analyses noting up to 600% year-on-year increases in specific categories of attacks against sector infrastructure and digital services. High-visibility incidents, such as ransomware attacks that disrupted major airport operations across Europe, further demonstrate the real-world impacts of these growing cyber threats beyond data theft to operational delays and passenger inconvenience. This escalating trend reflects how the rapid adoption of advanced technologies, vast amounts of sensitive customer data, and complex global supply chains have made the aviation sector a lucrative target for cybercriminals, emphasizing the urgent need for robust cyber security measures.

3. Research Method

This study adopts a systematic literature review (SLR) methodology to examine preventive cyber security strategies in the context of sustainable digital tourism and travel. A systematic approach was chosen to ensure a transparent, structured, and comprehensive analysis of existing academic research. Relevant literature was identified through a search of well-recognized academic databases, focusing on peer-reviewed journal articles published in English. Keywords related to cyber security, digital tourism, preventive strategies, and sustainability were used to retrieve relevant studies.

The selected articles were screened based on predefined inclusion and exclusion criteria to ensure relevance and quality. After removing duplicates and non-relevant studies, the final set of articles was analysed using qualitative content analysis. The studies were reviewed to identify key cyber security threats, preventive measures, technological approaches, and sustainability implications within the tourism industry. The findings were then categorized and synthesized to highlight major themes, research trends, and gaps in the literature. This systematic method ensures reliability of results and provides a strong foundation for understanding the role of preventive cyber security in sustainable digital tourism.

4.Findings and discussion

4.1 Cyber security in Tourism and Travel Documents Published by Year

Research on cyber security in the tourism and travel fields has increased steadily over the past two decades, reflecting growing concern among academics and industry stakeholders about digital risks in these sectors. According to a recent systematic review covering publications from 2000 to August 2024, very few studies addressed cyber security issues in tourism and travel before 2016, with almost no documents published between 2000 and 2005. This indicates

that cyber security was not a major focus in tourism and travel research during the early years of digital adoption. However, starting around 2016, there was a notable upward trend in the number of published documents and citations linking cyber security with tourism and travel topics. This rise became much more pronounced after the COVID-19 pandemic, particularly from 2020 to 2023, when the average annual number of publications and citations related to "cyber security" and "tourism" increased significantly. During this period, cyber security-related research in tourism grew by about 18 % in publications and 129 % in citations, while studies connecting "cyber security" with "travel" showed increases of approximately 8 % in publications and 80 % in citations.

These patterns demonstrate a clear shift in scholarly interest, highlighting that cyber security has become a more important research theme within tourism and travel literature, especially as digital technologies and online systems have become deeply integrated into the industry

4.2 The main countries that most contributed to cyber security, tourism, and travel publications

Bibliometric analyses reveal that research on cyber security in tourism and travel is concentrated in a few leading countries, reflecting their strong academic and technological capacities. The United States consistently ranks first in the number of publications, followed by European nations such as the United Kingdom, Germany, and Spain. Asian countries, notably China and South Korea, have also shown a rapid increase in contributions over the past decade, particularly in cyber security topics related to tourism technologies and digital platforms. Between 2020 and 2023, the U.S. accounted for nearly 28% of publications, while China contributed approximately 18%, and the U.K., Germany, and Spain together represented around 25% of total output. This concentration suggests that countries with advanced ICT infrastructures and significant tourism markets tend to produce more research at the intersection of cyber security and travel. The geographic distribution of publications also highlights emerging contributions from countries in the Middle East and Southeast Asia, indicating a growing global awareness of cyber security risks in digital tourism.

5. Conclusion

Cyber security is increasingly critical for the tourism and travel industry as digital systems expand. Research shows a sharp rise in publications since 2016, especially post-2020, reflecting growing awareness of cyber threats. The air transport sector faces significant risk, emphasizing the need for preventive measures to protect operations and customer data.

The U.S., China, and European countries lead in research contributions, with emerging efforts from Asia and the Middle East, highlighting a global recognition of cybersecurity's importance. Overall, strong preventive strategies are essential to ensure safe, resilient, and sustainable digital tourism, and continued research and investment remain vital to counter evolving cyber threats.

5.1 Theoretical Implications, Limitations, and Future Research

Theoretical Implications: This study highlights the growing intersection between cyber security and digital tourism, emphasizing the importance of integrating preventive cyber security strategies into tourism management frameworks. It contributes to the literature by mapping research trends, identifying key countries, and illustrating the sectors most affected by cyber threats, particularly air transport. The findings provide a foundation for developing models that link cyber security preparedness with sustainable digital tourism practices.

Limitations: The review relies primarily on publications indexed in major databases, which may exclude relevant studies in local journals or non-English sources. Additionally, some bibliometric data were approximated due to inconsistencies across sources, and the analysis focused mainly on quantitative trends rather than in-depth case studies or qualitative insights.

Future Research: Future studies should explore the effectiveness of specific cyber security interventions in tourism and travel contexts, including airlines, hotels, and online platforms. Comparative studies across regions could reveal best practices, while longitudinal research may track evolving cyber threats and mitigation strategies. Integrating qualitative insights, such as expert interviews or case analyses, could also enhance understanding of practical challenges and organizational responses.

5.2 Practical Implications

The findings of this study offer actionable insights for tourism and travel stakeholders. Airlines, hotels, and travel platforms should prioritize preventive cyber security measures to protect sensitive customer data and ensure uninterrupted services. Investments in staff training, secure digital infrastructure, and real-time threat monitoring can significantly reduce vulnerabilities. Policymakers and industry regulators can use these insights to develop standards and guidelines that strengthen cyber security across the tourism ecosystem. Additionally, collaboration between public and private sectors, both nationally and internationally, can enhance resilience against evolving cyber threats, promoting safer and more sustainable digital tourism experiences.

References

Florido-Benítez, L. (2025). The role of cyber security as a preventive measure in digital tourism and travel: A systematic literature review. Discover Computing.

Florido-Benítez, L. (2024). The cyber security applied by online travel agencies and hotels to protect users' private data in smart cities. Smart Cities, 7(1), 475-495.

Kapera, A. (2022). Cyber security in travel based on the opinions of university students engaging in tourism. Geography and Tourism, 2(10), 7-15.

Cyber security and tourism: Bibliometric analysis. (2025). Human Being, Artificial Intelligence and Organization, 221-234.

Bazazo, I., Al-Orainat, L., Abuizhery, F., & Al-Dhoun, R. (2019). Cyber security applications in the modern tourism industry. Journal of Tourism, Hospitality and Sports, 43.

Ghaderi, Z., Beal, L. M., Hall, C. M., Zaman, M., Rather, R. A., & Mat Som, A. P. (2024). Cyber security and smart tourist destinations resilience. Tourism Recreation Research.

Author Biographies

Dr.M.P.Prathiba is an Assistant Professor in the Department of Commerce at **Hindusthan College of Arts and Science Coimbatore**, She holds an **M.Com, M.Phil., and Ph.D. in Commerce**, along with a **Post Graduate Diploma in Computer Applications (PGDCA),** reflecting a strong academic foundation in both commerce and computer applications with **13 years of teaching experience.** Her professional work includes teaching undergraduate and postgraduate courses in commerce, as well as guiding **Ph.D. research scholars** in areas such as investment patterns, customer perception toward electric vehicles, work–life conflict among women entrepreneurs, and the role of financial literacy in investment decisions. As an educator and researcher, Dr. Prathiba contributes to the academic community through scholarly supervision and an active role in higher education within her field.

Dr.R.Tamil Selvi is currently serving as an Assistant Professor in the Department of Commerce at **Hindusthan College of Arts and Science (Autonomous), Coimbatore.** She holds **M.Com (CA), M.Phil.,** and **Ph.D.** degrees, with her research specialization in Marketing. All her teaching experience has been acquired after obtaining her Ph.D. degree with six years of teaching experience, she has actively contributed to academic excellence through effective teaching and continuous professional development. She has participated in numerous Faculty Development Programmes, seminars, conferences, and workshops, and has completed SWAYAM-approved certificate courses. She has published 15 research papers in reputed journals and edited books, reflecting her strong research orientation. She is a recognized Research Supervisor of Bharathiar University and holds a patent titled **"Stress–Sensing Mouse"**. She served as an NSS Programme Officer and has acted as a Resource Person for academic and career guidance programmes. Her contributions have been acknowledged with awards for Road Safety Awareness initiatives under the Coimbatore Smart City Project and the Smart Inspirer Award. At present, she serves as a member of an Editorial Advisory Board. She continues to contribute actively to teaching, research supervision, and knowledge dissemination through publications and academic engagements.