TURIZAM
Volume 29, Issue 4
230-238 (2025)
ORIGINAL
SCIENTIFIC PAPER

Bridging the Gap Between Digital Security and Tourist Experience in Smart Destinations

Apostolos Tsiakalos[A*], **Anastasios Tsiakalos**[B]

Received: July 2025 | Accepted: December 2025
DOI: 10.5937/turizam29-60329

Abstract

This paper introduces and tests the Security-Experience Alignment Model (SEAM), a framework that explores how real cybersecurity conditions influence the link between digital trust and tourist satisfaction in smart destinations. A sequential mixed-method design was applied. Quantitative survey data were collected from 210 thematic travelers to measure satisfaction, trust, and cybersecurity awareness. In parallel, a technical audit of smart tourism infrastructures—public Wi-Fi networks and mobile applications—was performed using standard penetration-testing tools. Data were analyzed through Partial Least Squares Structural Equation Modeling (PLS-SEM) to examine direct and mediating effects.

The analysis shows a clear gap between perceived digital trust and the actual security level of tourism infrastructures. While personalization and smart services improve satisfaction, hidden vulnerabilities weaken digital trust and may affect long-term loyalty. The SEAM model identifies cybersecurity resilience as an underlying factor that connects secure infrastructure with sustainable tourist experiences. The study extends smart-tourism research by integrating cybersecurity resilience into satisfaction and trust models. It offers both theoretical and managerial insights, emphasizing that secure digital environments are essential for reliable and satisfying experiences in smart destinations.

Keywords: *smart tourism, cybersecurity resilience, digital trust, tourist satisfaction, smart destinations*

Introduction

Smart tourism ecosystems increasingly rely on data-driven personalization, ubiquitous connectivity, and mobile applications to enhance visitor experiences. In such environments, tourist satisfaction is largely determined by the quality of digital interactions, service reliability, and perceived personalization benefits (Gretzel et al., 2015; Li et al., 2017). At the same time, the deep integration of connected technologies creates new layers of vulnerability. Public Wi-Fi networks, mobile applications, and cloud-based tourism platforms often expose sensitive user data and operational systems to cyber threats (Radoglou-Grammatikis et al., 2020).

[A] School of Informatics, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece, coresponding author: atsiakalos@csd.auth.gr

[B] Department of Electrical and Computer Engineering, University of Western Macedonia, 50100, Kozani, Greece aff00144@uowm.gr

Recent research in smart infrastructure management shows that security and trust are critical components of user experience. Studies on smart grids and Internet of Things (IoT) environments have introduced trust-evaluation and anomaly-detection mechanisms to enhance system resilience and reliability (Pliatsios et al., 2020; Pliatsios et al., 2021). These findings suggest that digital trust depends not only on perceived service quality but also on the robustness of underlying infrastructures. In tourism contexts, however, this connection remains underexplored. While the literature has examined satisfaction, personalization, and perceived value in depth, cybersecurity resilience has rarely been included as a determinant of tourist trust and loyalty (Buhalis, Leung, 2022; Zhang, Law, Zhao, 2023; Florido-Ben´ıtez, 2024).

Therefore, a significant research gap exists in understanding how objective cybersecurity conditions interact with psychological constructs such as trust and satisfaction in smart destinations. Addressing this gap, the present study proposes the *Security-Experience Alignment Model (SEAM)*, which integrates cybersecurity resilience into the established satisfaction–trust framework. Through a mixed-method approach that combines behavioral survey data with technical cybersecurity assessments, this research provides an integrated analysis of how infrastructural security affects perceived trust and overall satisfaction.

The study contributes theoretically by extending satisfaction models with a security dimension that links infrastructural integrity to experiential outcomes, and practically by offering insights for the design of secure-by-default tourism infrastructures that foster both trust and sustainable loyalty.

Theoretical Framework and Hypothesis Development

Tourist Satisfaction in Smart Destinations

Tourist satisfaction has traditionally been modeled through frameworks such as SERVQUAL and Expectation–Confirmation Theory (ECT), where service quality, personalization, and perceived value shape behavioral intentions and destination loyalty (Parasuraman et al., 1988; Oliver, 1980). In smart tourism contexts, real-time information delivery, personalized recommendations, and digital service reliability are regarded as key enablers of positive tourist experiences (Li et al., 2017).

Recent research, however, highlights that satisfaction extends beyond utilitarian performance and includes psychological dimensions such as perceived trust, safety, and data security (Zare et al., 2022; Florido-Ben´ıtez, 2024). While smart services enhance convenience and enjoyment, tourists increasingly expect transparency and protection of personal data in their interactions with digital platforms. Despite these developments, cybersecurity—an essential element of infrastructural safety—remains largely excluded from established satisfaction models, leaving a theoretical gap in understanding how technical security influences perceived trust and overall experience.

Cybersecurity Resilience as a Latent Construct

Cybersecurity resilience refers to the capacity of digital infrastructures to anticipate, resist, and recover from cyber incidents while maintaining reliable service quality (Radoglou-Grammatikis et al., 2020). Studies in smart grids and industrial Internet of Things environments demonstrate that dynamic trust evaluation and anomaly-detection mechanisms can significantly strengthen resilience and sustain user confidence under uncertainty (Pliatsios et al., 2020; Pliatsios et al., 2021). Advanced defensive architectures such as federated honeypots and covert detection systems further illustrate how proactive learning and distributed intelligence enhance network reliability and trustworthiness (Siniosoglou et al., 2021).

Drawing on these insights, this study conceptualizes cybersecurity resilience as a *latent construct* composed of both objective infrastructure indicators (e.g., encryption standards, vulnerability exposure) and subjective user perceptions of digital safety. Within tourism systems, this construct is proposed to mediate or moderate the relationship between service personalization and long-term loyalty intentions, functioning as an underlying determinant of perceived trust.

The Security-Experience Alignment Model (SEAM)

Building upon the above, the *Security-Experience Alignment Model (SEAM)* integrates cybersecurity resilience into a traditional satisfaction–trust–loyalty framework. The model assumes that secure infrastructures not only support reliable service delivery but also shape the psychological foundations of trust that sustain satisfaction over time. Accordingly, the following hypotheses are proposed:

- **H1**: Personalization services positively influence tourist satisfaction.
- **H2**: Cybersecurity resilience positively influences perceived digital trust.
- **H3**: Perceived digital trust positively influences overall satisfaction.
- **H4**: Cybersecurity resilience indirectly affects satisfaction through the mediation of digital trust.
- **H5**: Higher cybersecurity resilience positively correlates with long-term loyalty intentions.

This integrative framework extends existing satisfaction theories by recognizing cybersecurity resilience as a core experiential dimension that links technical infrastructure with psychological responses in smart tourism environments.

Methods and Data

Research Design

This study applies a sequential mixed-methods design that combines quantitative behavioral data with a technical cybersecurity assessment. The mixed approach enables the triangulation of subjective perceptions of satisfaction and trust with objective indicators of infrastructural cybersecurity conditions in smart tourism environments. This design was selected because it allows validation of the proposed SEAM model from both human-centric and system-centric perspectives.

Behavioral Data Collection

A structured online questionnaire was developed to measure the main constructs of the SEAM framework. The instrument was pre-tested with ten participants to ensure clarity and reliability before full deployment. The survey consisted of four parts:

1. **Demographics:** Age, gender, education, and previous experience with smart tourism services.
2. **Tourism Preferences:** Primary travel motivations (e.g., cultural, ecological, adventure, educational).
3. **Satisfaction and Trust Indicators:** Likert-scale items (1 = strongly disagree to 5 = strongly agree) assessing satisfaction with personalization, perceived digital trust, and destination experience.
4. **Cybersecurity Awareness:** Self-reported familiarity with digital security practices (e.g., use of secure Wi-Fi, app permissions, data-sharing concerns).

Data were collected between March 2023 and June 2023 through social-media travel communities and university mailing lists. After removing incomplete or inconsistent responses, **N = 210** valid questionnaires remained. All respondents were adults (aged > 18) who had visited at least one smart tourism destination within the previous 12 months.

Participation was voluntary and anonymous, with informed consent obtained prior to completion of the questionnaire.

Cybersecurity Infrastructure Assessment

In parallel, a technical cybersecurity audit was performed on representative digital infrastructures used in smart destinations. The assessment focused on three common touchpoints:

- **Public Wi-Fi hotspots:** Simulated Evil-Twin and Man-in-the-Middle attacks were executed to test encryption and session handling.
- **Mobile tourism applications:** Static and dynamic analyses were performed to detect plaintext data leakage, insecure storage, and API vulnerabilities.
- **Online booking portals:** Transport-layer encryption and session management were evaluated for compliance with contemporary TLS protocols.

All penetration tests were carried out under ethical, non-intrusive conditions using open-source tools such as Metasploit, Wireshark, and SSLStrip. The results were anonymized and aggregated to protect the integrity of tested systems.

Data Analysis

Quantitative survey data were analyzed using **Partial Least Squares Structural Equation Modeling (PLS-SEM)** with SmartPLS 4. This method was selected because it is suitable for theory development and exploratory models with latent constructs and moderate sample sizes. Model reliability and validity were confirmed through composite reliability, average variance extracted (AVE), and discriminant validity using the Fornell–Larcker criterion. Mediation and indirect effects were evaluated through bootstrapping with 5,000 resamples.

Cybersecurity testing results were synthesized into a composite **Cybersecurity Resilience Index (CRI)** that reflected three key dimensions: encryption strength, vulnerability exposure, and data-leakage incidents. The CRI was standardized on a 0–1 scale, where higher scores indicated more resilient infrastructures. This objective index was then incorporated into the SEM model as an infrastructural variable to test its mediating and direct effects on digital trust and satisfaction.

Results

Descriptive Statistics

The final sample included 210 respondents, representing a balanced gender distribution (55.7% female and 44.3% male). Most participants (62.4%) were between 25 and 44 years old, and a large proportion (71.8%) held at least a bachelor's degree. Regarding tourism preferences, cultural (33.8%) and eco-tourism (29.5%) categories were most common, suggesting a sample of digitally active and environmentally aware travelers.

Overall, respondents reported high satisfaction with smart services (mean = 4.32, SD = 0.47) and personalization features (mean = 4.28, SD = 0.52). These values indicate that digital convenience and tailored content strongly contribute to positive experiences in smart destinations. However, cybersecurity awareness was considerably lower: only 18.5% of participants expressed confidence in identifying secure digital services during travel. This discrepancy points to an emerging *perception gap* between enjoyment of digital convenience and understanding of security risks. It highlights the importance of cybersecurity education as part of the smart tourism experience.

Preliminary correlation analysis also revealed a moderate positive association between cybersecurity awareness and perceived digital trust (r = 0.42, p ¡ 0.01), suggesting that tourists who understand digital risks are more likely to trust destinations with visible security measures. These findings provide a foundation for the structural modeling presented in the next section.

Cybersecurity Infrastructure Vulnerability Assessment

The technical cybersecurity audit revealed substantial weaknesses across the analyzed smart tourism infrastructures. These findings confirm that, while digital services are widely adopted, many systems still rely on outdated or insufficient security configurations.

- **Wi-Fi Testing:** In 78% of the examined public networks, simulated Evil Twin attacks successfully captured unencrypted session cookies within ten minutes of deployment. This indicates that most tourist Wi-Fi services remain vulnerable to basic interception threats and lack modern encryption standards such as WPA3.
- **Mobile Application Testing:** Static and dynamic analyses revealed insecure local data storage and unencrypted API communication in three out of five commonly used tourism applications. Such practices expose users to potential identity theft and data leakage when interacting with destination-related apps.
- **Booking Portals:** SSL/TLS misconfiguration was detected in 40% of tested websites, with legacy protocols (TLS 1.0/1.1) still active. These vulnerabilities compromise the confidentiality of payment and personal information, diminishing user trust in online booking systems.

The resulting **Cybersecurity Resilience Index (CRI)** showed low-to-moderate performance across the evaluated infrastructures (mean = 0.43 on a normalized 0–1 scale). This suggests that many smart destinations remain in an early stage of cybersecurity maturity. When compared with tourists' high satisfaction and trust perceptions, these objective weaknesses reveal a notable *security–perception misalignment* that could threaten long-term destination reputation if left unaddressed. The CRI results therefore support the assumption that infrastructural integrity plays a hidden yet influential role in shaping the digital experience.

Structural Equation Modeling (SEM) Results

The PLS–SEM analysis produced satisfactory measurement and structural model statistics:

- Composite Reliability (CR) values exceeded 0.80 for all constructs.
- Average Variance Extracted (AVE) values were above the 0.50 threshold.
- Discriminant validity was confirmed using the Fornell–Larcker criterion.
- The hypothesized relationships within the SEAM model were strongly supported:
- **H1:** Personalization positively influences tourist satisfaction ($\beta = 0.54$, $p < 0.001$).
- **H2:** Cybersecurity resilience positively influences perceived digital trust ($\beta = 0.37$, $p = 0.002$).
- **H3:** Perceived digital trust positively influences overall satisfaction ($\beta = 0.46$, $p < 0.001$).
- **H4:** Cybersecurity resilience indirectly affects satisfaction through digital trust ($\beta_{\text{indirect}} = 0.17$, $p = 0.006$).
- **H5:** Cybersecurity resilience directly influences loyalty intentions ($\beta = 0.29$, $p = 0.008$).

Collectively, these results validate the structural assumptions of the SEAM framework. They demonstrate that although personalization remains the strongest driver of satisfaction, the security dimension significantly shapes digital trust and indirectly affects tourists' loyalty. The mediating role of trust underscores that a secure technological environment is not merely a technical requirement but a key experiential determinant that sustains positive perceptions over time.

Summary of Key Findings

Overall, the empirical evidence supports the conceptual assumptions of the *Security–Experience Alignment Model (SEAM)*. Despite consistently high levels of reported satisfaction, significant cybersecurity weaknesses persist across smart tourism infrastructures. The results confirm that objective security conditions exert an indirect but meaningful influence on satisfaction and loyalty through the mediating role of digital trust. This highlights a persistent misalignment between the perceived and actual security performance of smart destinations.

Discussion

The findings of this research offer multidimensional insights into how technological integrity interacts with human experience in smart tourism ecosystems. In line with earlier studies, personalization remains a dominant predictor of satisfaction (Gretzel et al., 2015; Li et al, 2017). Yet the present analysis extends theoretical understanding by introducing cybersecurity resilience as an additional experiential dimension that bridges technical and psychological domains.

A key contribution lies in confirming the existence of a **security–experience gap**—a paradox where high user satisfaction coexists with weak cybersecurity practices. This result aligns with broader digital-trust literature showing that users often equate convenience with safety (Florido-Benıtez, 2024; Zhang et al, 2023). By empirically validating this gap, the SEAM framework demonstrates that trust does not merely emerge from user perception but is conditioned by the robustness of the underlying digital infrastructure.

From a theoretical standpoint, the SEAM model integrates two previously disconnected streams of research: service-experience theory and cybersecurity resilience. It repositions security from a purely technical concern to a latent experiential factor that co-determines satisfaction and loyalty. This integration enriches established models such as SERVQUAL and Expectation–Confirmation Theory by embedding infrastructural trustworthiness as a precondition for sustained satisfaction in digital environments.

From a managerial perspective, the results underline that cybersecurity must be treated as a visible and measurable component of the tourist experience. Destination managers and service providers should:

- Implement transparent data-protection practices and communicate them clearly to visitors.
- Incorporate security-performance indicators (e.g., encryption compliance, data-breach response time) into quality-assurance systems.
- Provide traveler education on safe digital behaviors through in-destination apps and signage.

Such initiatives can transform security from a hidden technical layer into a source of competitive differentiation and trust-based branding for smart destinations.

Looking forward, the *security–experience alignment* perspective suggests that future tourism strategies should balance innovation with protection. Continuous monitoring, adoption of privacy-by-design architectures, and cross-sector collaboration between ICT experts and tourism planners will be essential. By embedding resilience into experience design, destinations can sustain both technological advancement and long-term visitor confidence.

Conclusion

This study advances the understanding of how cybersecurity conditions shape tourist experiences in smart destinations. By combining behavioral analysis with technical infrastructure assessment, it provides empirical support for the *Security–Experience Alignment Model (SEAM)* and confirms that digital trust functions as the psychological bridge between secure infrastructures and visitor satisfaction.

The results reveal that high satisfaction levels may coexist with weak security configurations, exposing a latent vulnerability in the long-term sustainability of digital tourism ecosystems. The SEAM framework thus reframes cybersecurity resilience as an integral dimension of experience design rather than a peripheral technical concern.

From a theoretical standpoint, this research contributes to smart-tourism literature by integrating infrastructural trustworthiness into satisfaction and loyalty models. It expands traditional service-quality theories such as SERVQUAL and Expectation–Confirmation Theory through the inclusion of security-related constructs, offering a more comprehensive explanation of digital trust formation.

From a managerial perspective, the findings emphasize that trust-building in smart destinations requires both human-centered and technology-centered interventions. Investment in secure digital infrastructure, visible communication of data-protection measures, and continuous cybersecurity education for both tourists and staff can transform security into a competitive advantage and a driver of loyalty.

Future studies should examine cross-cultural differences in security perception, longitudinal effects of cybersecurity incidents on destination image, and the integration of real-time threat analytics into experience management systems. Embedding cybersecurity resilience into every stage of smart destination planning will ensure that technological innovation translates into genuinely safe, trustworthy, and satisfying visitor experiences.

Limitations and Future Research

Several limitations of the present study should be acknowledged. First, the cross-sectional research design constrains the ability to capture longitudinal variations in tourists' trust or satisfaction following cybersecurity incidents. Future studies could employ panel or experimental designs to monitor how perceptions evolve over time in response to repeated exposure to secure or insecure digital environments.

Second, the sample focused on thematic tourists within a single national context, which may limit generalizability to broader or cross-cultural visitor groups. Comparative studies across different smart destinations and cultural backgrounds would enhance the external validity of the *SEAM* framework and reveal how cultural attitudes toward risk and privacy influence digital trust formation.

Third, the cybersecurity assessment was restricted to publicly accessible components—such as Wi-Fi networks, tourism applications, and booking portals—and did not include backend systems, data management platforms, or third-party service integrations. Future work could integrate technical forensics and real-time intrusion detection data to provide a more complete picture of infrastructural resilience.

In methodological terms, future research could also combine the SEAM model with advanced analytics, such as machine learning–based anomaly detection or dynamic structural modeling, to explore causal pathways between cybersecurity events and behavioral responses. Incorporating emerging paradigms such as *zero-trust architectures*, *privacy-by-design* frameworks, and real-time threat monitoring will not only refine the model's robustness but also align it with the evolving landscape of smart tourism governance.

Ultimately, expanding and validating SEAM across diverse destinations and technological contexts will enable a deeper understanding of how security and experience converge to shape sustainable digital trust ecosystems in global tourism.

References

Buhalis, D., & Leung, R. (2022). Smart tourism and digital trust: Managing data-driven experiences. *Tourism Management*, 92, 104579.

Florido-Ben´ıtez, L. (2024). The cybersecurity applied by online travel agencies and hotels to protect users' private data in smart cities. *Smart Cities*, 7(1), 475–495.

Gretzel, U., Sigala, M., Xiang, Z., & Koo, C. (2015). Smart tourism: Foundations and developments. *Electronic Markets*, 25(3), 179–188.

Li, Y., Hu, C., Huang, C., & Duan, L. (2017). The concept of smart tourism in the context of tourism information services. *Tourism Management*, 58, 293–300.

Oliver, R. L. (1980). A cognitive model of the antecedents and consequences of satisfaction decisions. *Journal of Marketing Research*, 17(4), 460–469.

Parasuraman, A., Zeithaml, V. A., & Berry, L. L. (1988). SERVQUAL: A multiple-item scale for measuring consumer perceptions of service quality. *Journal of Retailing*, 64(1), 12–40.

Pliatsios, D., Sarigiannidis, P. G., Efstathopoulos, G., Sarigiannidis, A., & Tsiakalos, A. (2020). Trust management in smart grid: A Markov trust model. *International Conference on Modern Circuits and Systems Technologies (MOCAST)*, IEEE, 1–5.

Pliatsios, D., Sarigiannidis, P. G., Fragulis, G., Tsiakalos, A., & Margounakis, D. G. (2021). A dynamic recommendation-based trust scheme for the smart grid. *IEEE Conference on Network Softwarization (NetSoft)*, 1–8.

Radoglou-Grammatikis, P., Sarigiannidis, P., Efstathopoulos, G., Kllapi, H., & Tsiakalos, A. (2020). An anomaly detection mechanism for the IEC 60870–5–104 protocol. *IEEE Access*, 8, 116256–116272.

Radoglou-Grammatikis, P., Sarigiannidis, P., Efstathopoulos, G., Kllapi, H., & Tsiakalos,

Siniosoglou, I., Argyriou, V., Lagkas, T. D., Tsiakalos, A., Sarigiannidis, A., & Sarigiannidis, P. G. (2021). Covert distributed training of deep federated industrial honeypots. *IEEE Globecom Workshops*, 1–6.

Zare, S., Khosravi, M., & Ghasemi, R. (2022). Tourists' trust and post-COVID travel intentions: The mediating role of hygiene perception. *Journal of Destination Marketing & Management*, 23, 100684.

Zhang, H., Law, R., & Zhao, X. (2023). Privacy and data protection in smart tourism destinations: Tourists' perceptions and behavioral outcomes. *Information Technology & Tourism*, 25(1), 75–93