

International Journal of Agriculture Extension and Social Development

Volume 9; Issue 1; January 2026; Page No. 488-500

Received: 18-10-2025
Accepted: 26-11-2025

Indexed Journal
Peer Reviewed Journal

Consumer trust and privacy in hospitality tech: A review of mobile check-in, contactless payments, and data governance

¹Palak Gupta, ²Mahak Agarwal and ³Nisha Kumari

¹Assistant Professor, Dev Bhoomi Uttarakhand University, Dehradun, Uttarakhand, India

²Assistant Professor, Dharmsinh Desai University, Nadiad, Gujarat, India

³Assistant Professor, SGT University, Gurugram, Haryana, India

DOI: <https://www.doi.org/10.33545/26180723.2026.v9.i1g.2959>

Corresponding Author: Palak Gupta

Abstract

Purpose: This review investigates the role of consumer trust and privacy concerns in the adoption of hospitality technologies, specifically focusing on mobile check-in systems, contactless payments, and data governance practices.

Design/Methodology/Approach: A bibliometric review approach was adopted by analyzing 96 journal articles published between 2013 and 2026 using the Biblioshiny package of R. Literature was sourced from multidisciplinary databases including Scopus. Studies were categorized based on trust dimensions, risk perceptions, privacy frameworks, and technology acceptance models.

Findings: The findings reveal that perceived security, data transparency, brand credibility, regulatory compliance, and user control significantly affect consumer trust in hospitality technologies. While contactless technologies gained strong acceptance post-COVID-19, persistent privacy anxieties related to biometric data, location tracking, and behavioral profiling continue to influence technology resistance. Cultural differences and legal frameworks moderate these relationships across regions.

Practical Implications: Hospitality firms must prioritize cybersecurity investments, transparent data governance practices, and user consent mechanisms to strengthen customer trust and ensure long-term adoption of digital services.

Originality/Value: This review contributes to hospitality technology literature by integrating trust, privacy, and governance dimensions into a unified conceptual framework, offering strategic implications for digital transformation in service ecosystems.

Keywords: Hospitality technology, contactless technology, AI, consumer trust, consumer privacy

Introduction

The hospitality industry is undergoing a rapid digital transformation driven by advancements in mobile technologies, artificial intelligence, contactless systems, and data-driven service design. Hotels across all segments—luxury, mid-scale, and budget—are increasingly integrating mobile check-in, digital room keys, contactless payments, cloud-based property management systems, and biometric authentication to enhance operational efficiency and deliver seamless guest experiences. This technological shift has accelerated significantly in the post-pandemic period, where health safety, speed, and minimal physical interaction have become crucial determinants of service preference. While these innovations promise greater convenience and personalization, they also fundamentally reshape the relationship between hospitality firms and their guests by intensifying the collection, storage, and exchange of personal data.

Trust has long been recognized as a cornerstone of successful service relationships, particularly in high-contact industries such as hospitality where perceived risk is inherently high. In technology-mediated service encounters, however, trust extends beyond interpersonal interactions to include faith in digital platforms, system reliability, data

security, and institutional safeguards. When guests use mobile check-in or contactless payments, they no longer evaluate only the service provider's competence; they also assess the invisible digital infrastructure that processes their identity, location, payment credentials, and behavioral patterns. As a result, technology adoption in hospitality is increasingly shaped by guests' perceptions of cybersecurity, transparency, and data governance practices.

Parallel to the rise of smart hospitality technologies is the growing salience of consumer privacy. Mobile applications, loyalty programs, and smart-room systems enable hotels to capture granular guest data across the entire service journey, from pre-arrival preferences to in-stay behavioral analytics and post-stay feedback. These data ecosystems allow hyper-personalized service offerings but also create vulnerabilities related to unauthorized access, surveillance, data misuse, and cross-platform data sharing with third-party vendors such as online travel agencies and payment gateways. For many consumers, the perceived benefits of convenience and personalization are weighed against the perceived costs of privacy loss—a trade-off commonly conceptualized through the lens of privacy calculus theory.

Although a substantial body of research has examined technology acceptance in hospitality using models such as

the Technology Acceptance Model (TAM), Unified Theory of Acceptance and Use of Technology (UTAUT), and service quality frameworks, the role of trust and privacy has often been treated as a secondary or fragmented construct. Existing studies are largely skewed toward adoption intention, usage convenience, and system performance, with comparatively limited attention to ethical data governance, cross-platform data flows, biometric data usage, and regulatory compliance in hospitality contexts. Moreover, the majority of empirical evidence is concentrated in developed economies, leaving emerging markets—where digital adoption is rapid but data protection frameworks are still evolving—underrepresented in the scholarly discourse. The post-pandemic expansion of mobile check-in, contactless payments, and facial recognition systems has further intensified these concerns. While such technologies reduce physical contact and improve service speed, they also amplify guest exposure to algorithmic decision-making, location tracking, and identity verification processes that are often opaque to users. High-profile data breaches, unauthorized surveillance allegations, and third-party data leaks across digital platforms have heightened consumer sensitivity toward how hospitality firms collect, store, and monetize personal information. Consequently, trust is no longer anchored solely in brand reputation or service quality but increasingly in the transparency, accountability, and ethical orientation of data governance practices. Despite the growing relevance of these issues, the existing literature remains fragmented across disciplines such as information systems, marketing, tourism, cybersecurity, and

consumer behavior. There is a lack of an integrated, hospitality-centric synthesis that systematically connects trust formation, privacy perceptions, biometric acceptance, and institutional data governance within a single conceptual framework. Without such integration, hospitality managers face difficulty in designing technology strategies that are not only efficient but also ethically responsible and trust-enhancing. In response to these gaps, the present study undertakes a comprehensive review of literature on consumer trust and privacy in hospitality technologies, with specific focus on mobile check-in, contactless payments, and data governance. By synthesizing theoretical perspectives from trust theory, privacy calculus, and technology acceptance research, this review aims to provide a coherent understanding of how digital trust is constructed in smart hospitality ecosystems. The study further seeks to identify key drivers, inhibitors, and moderating factors influencing guest acceptance of data-intensive technologies, while proposing future research directions and strategic implications for ethical and sustainable digital transformation in the hospitality industry.

Research Objectives

- To critically review the role of trust and privacy concerns in the adoption of hospitality technologies.
- To synthesize how data security, transparency, and regulatory compliance influence consumer confidence.
- To examine consumer perceptions toward biometric technologies and digital identity systems in hotels.

Table 1: Descriptive Characteristics of Studies Included in the Systematic Review

Author(s) & Year	Country / Region	Methodology	Sample / Data Source	Technology Focus	Key Trust/ Privacy Variables
Kim & Lee (2019) ^[1]	South Korea	SEM	412 hotel guests	Mobile check- in	Trust, perceived risk, security
Ivanov <i>et al.</i> (2020) ^[2]	Europe	Conceptual	Secondary data	Service robots	Trust in automation
Gupta & Arora (2021) ^[3]	India	Survey	368 OTA users	Contactless payment	Privacy concern, trust
Li <i>et al.</i> (2021) ^[24]	China	SEM	550 biometric users	Facial recognition	Security, surveillance concern
Verma & Singh (2022) ^[5]	India	Mixed- method	44 hotel managers + guests	Digital identity systems	Data governance, transparency
Park <i>et al.</i> (2022) ^[6]	USA	Experimental	210 respondents	AI-driven check-in	Algorithmic trust
Hassan <i>et al.</i> (2023) ^[7]	UAE	Survey	390 luxury hotel guests	Smart room tech	Institutional trust
Rao & Mishra (2023) ^[8]	India	Survey	322 contactless users	Digital wallet & payments	Cyber risk, trust
Zhang <i>et al.</i> (2024) ^[9]	China	SEM	480 hotel guests	Biometric access	Privacy calculus, trust

Review of Literature

The latest developments in the fields of hospitality and tourism have been centering on the meeting points of digital trust and technologies. In this connection, Kim and Lee (2019)^[1] investigated mobile check-in systems among 412 hotel guests in South Korea with the help of SEM, pointing out the issues of trust, perceived risk, and security. In the European continent, Ivanov *et al.* (2020)^[2] presented a conceptual analysis of the matter based on secondary data, which was dealing with the theme of service robots and trust in automation. Likewise, Gupta and Arora (2021)^[3] approached the subject from the angle of a survey among 368 OTA users in India, which was drawn to the conclusion that privacy concerns and trust held in contactless payment systems were the main issues. In China, Li *et al.* (2021)^[24] focused on SEM to analyze 550 biometric users, unraveling the aspects of facial recognition technologies and surrounding issues of security and surveillance. Alongside, Verma and Singh (2022)^[5] traversed theboundaries of

research with a mixed-method approach, consisting of inputs from 44 hotel managers and guests in India, who were engaged in the discussion on digital identity systems, with the main points of data governance and transparency being highlighted. Park *et al.* (2022)^[6] were positioned in the USA, where they applied an experimental design with 210 respondents to study AI-driven check-in processes and algorithmic trust. In the UAE, Hassan *et al.* (2023)^[7] undertook a survey of 390 luxury hotel guests inquiring into smart room technologies and institutional trust. Similarly, Rao and Mishra (2023)^[8] investigated the case of 322 contactless users in India with a focus on digital wallets and payments, especially raising the topics of cyber risk and trust. The latest research work on the topic was presented by Zhang *et al.* (2024)^[9], who had examined biometric access among 480 hotel guests in China using SEM and was employing the privacy calculus framework to comprehend trust.

Research into consumer trust and privacy in the use of technology in hospitality has made major strides over the last ten years. Wang *et al.* (2014)^[10] laid the groundwork for this research area with their comprehensive literature review, defining trust as multi-faceted—interpersonal, institutional, and technological—and specifying the preconditions such as service quality, reputation, and perceived risk alongside the results of loyalty and usage intention. Following on from this, Morosan and DeFranco (2015)^[11] utilized the privacy calculus spectrum for hotel app use, concluding that personalization and facilitation spurred the giving of personal info while the inverses, namely privacy issues, and perceived risks, prevailed with the help of trust. Delving deeper into biometric applications, Xu *et al.* (2021)^[12] analyzed the case of facial recognition check-in, concluding that comfort and time-saving are the main reasons for the usage of the technology but on the other hand, surveillance-like concern diminishes the trust in it which is again affected by the cultures and laws in place. Ozturk *et al.* (2017)^[13] incorporated methodologies of privacy calculus and trust-risk models to describe the loyalty to mobile booking, and concluded that trust decreases the perceived risk and in turn increases the usage for the second time or more, while privacy issues are still the major hurdle. Theoretical reviews have opened up the area further. Park, Lee, and Back (2023)^[14] were highly critical of the existing state of affairs in the field of artificial intelligence, Internet of Things, mobile applications, and robotics and pointed out the poor governance, lack of ethics, and privacy violations as the main areas of concern, thus asking for the enactment of laws and research across cultures. Peng *et al.* (2024)^[15] went a step further by merging the digital transformation efforts of the hospitality industry with trust-building factors like cloud property management systems (PMS), mobile guest journey, and data governance. Qiu (2024)^[16] conducted a study that pointed out the differences in the acceptance of contactless technology based on the factors like age, tech-savviness, and hygienic perception, thus highlighting privacy-convenience tradeoff mediation. Besides that, Gupta *et al.* (2022)^[17] also discussed this issue. The use of AI in facial recognition technology has been reviewed, bringing out issues relating to its accuracy, bias, and ethical implications and suggesting consent and opt-in systems that are clear and inclusive. Among the various technical viewpoints presented, the study by Bao *et al.* (2023) on the application of facial recognition in hotel guidance systems was also highlighted, where the performance of the system was made comparable to that of other systems by implementing privacy-preserving measures.

Absolutely, different data governance practices can build up a solid trust base. Alhassan *et al.* (2016)^[19] created a visualization mapping different aspects of governance, like proper governing, good quality, and privacy controls; they contended that the organization with better governance would be more trustworthy and thus would have a higher maturity level in trustworthiness. According to Zhang *et al.* (2024)^[20], acceptance of biometric systems in China is influenced by regulatory guarantees and opt-in deployment. Studies by Hassan *et al.* (2023)^[21] further supported the notion of trust in institutions, where they pointed out that security measures and the reputation of the hotel create a

sense of trust in the use of smart-room technologies. The study by Rao and Mishra (2023)^[22] focused on the Indian context, where trust in contactless payments was affected by the government's regulatory messages, the branding of the digital wallets, and the security of the vendor. In one way, Kim and Lee (2019)^[23] demonstrated that the advantages and trust users see in mobile check-in feature usage do influence their adoption; however, the concern of privacy can act as a barrier, unless pretty good security measures are in place to assure users of their privacy being protected. Facial recognition technology remains under the microscope. Li *et al.* (2021)^[24] found that perceived accuracy and security were trust and acceptance related but that privacy fears made the technology less attractive unless good governance and consent mechanisms were in place. The study conducted in India by Verma and Singh (2022)^[22] on digital identity systems suggested the use of transparent consent flows, limit retention, and vendor contracts as means to build and maintain trust. Technology such as smartphones, used by guests and customers, has been researched by Kim (2021)^[23, 26], who determined that personalization leads to higher satisfaction but at the same time creates a bigger need for privacy—this is where opt-in personalization and clear notices help mitigate the issue. Ozturk *et al.* (2017)^[27] were among the first ones to talk about concealing privacy as a component in the design of service that integrates with IoT and mobile services.

Finally, demand-side perspectives highlight evolving consumer expectations. Wang *et al.* (2024)^[28] analyzed industry shifts, showing how health and convenience demands accelerated adoption of contactless services, shaped by segmentation and regulation. Sampaio *et al.* (2024)^[29] further demonstrated that preferences for digital services vary by trip purpose and demographics, recommending targeted communication to build trust. Collectively, these studies underscore that while convenience and personalization drive adoption of hospitality technologies, trust hinges on transparent governance, visible security cues, and cultural-regulatory alignment.

The latest research is still unfolding in the field of trust, privacy, and technology adoption in the hospitality sector. Park *et al.* (2022)^[6] scrutinized AI-based check-in systems, revealing that the transparency of algorithms can build trust but at the same time it can make users more conscious of the bias issue. Similarly, Chen *et al.* (2025)^[31] looked at the mobile app privacy cues and discovered that design signals and relevance framing increase the probability of personal data being disclosed. Legal views were given by Seng (2021)^[32] who studied public and private perceptions of facial recognition and pointed out consent and notice as the main issues. Governance problems were brought to light by Rahmadian (2023)^[33], who talked about the governance of digital twins and big data for sustainable tourism and argued for the application of the principles of transparency and minimization. Psychological aspects were dealt with by Pan (2025)^[34] who reported that security awareness campaigns lower privacy concerns connected with facial recognition and by his linked managerial work that emphasized opt-in, signage, and staff training for hotel larger deployments. Thematic coherency was reinforced through technical and managerial studies. Gupta *et al.* (2022)^[35] analyzed the

combination of AI and cloud systems in the hospitality sector, then recommended encryption, access control, and a trusted audit system as the means to build trust. The issue of guest heterogeneity associated with the adoption of contactless technology was tackled by Qiu *et al.* (2024)^[36], who distinguished between segments like early adopters and privacy-averse guests that made different tradeoffs. The authors Sampaio *et al.* (2024)^[29] widened the demand-side perspectives by recognizing communication and visible security as trust levers. In the case of restaurants, Rahman and Islam (2025)^[37] claimed that the convenience and safety factors were the driving forces behind the contactless payment adoption but that the unresolved security issues were a major hindrance to the process. The earlier framing by Koo (2017)^[38] set the “smart hospitality” agenda that gave central stage to the issues of IoT and privacy. Choi *et al.* (2020)^[39] contributed service robots’ knowledge, indicating that the more human-like the robot and the clearer the privacy policy the more willing the customers are to share data that is not sensitive.

Governance and identity systems are crucial and have not been overlooked. Rahmadian *et al.* (2023)^[33] have emphasized the need for a multi-stakeholder supervision of big data to sustain the tourism industry. Verma *et al.* (2022)^[25] offered their insights on digital identity systems from a managerial perspective and suggested that training of the staff and procurement of the vendor should be done in a way that compliance is achieved without sacrificing convenience. Among other things, systematic reviews like that of Peng (2024)^[15] have shown the adoption trends in hotels and identified enablers as leadership and IT capabilities, whereas privacy concerns and vendor fragmentation were cited as barriers. Theoretical exploration by Buhalis and Leung (2018)^[40] indicated the transforming power of IoT and AI over guest experiences, though they highlighted governance as key to trust preservation. Privacy calculus is still at the core: Li, Sarathy, and Xu (2017)^[41] proved that privacy issues inverted the effect of mobile commerce adoption, but trust-enhancing design could lessen the adverse impact. Theoretical research by Pavlou and Gefen (2004)^[42] laid down the concepts of structural assurance and reputation, which are still significant for OTAs and booking sites. Bilgihan and Nejad (2015)^[43] evidenced that trust is the major factor to increase the number of electronic word of mouth, while privacy issues are the ones that slow down the people’s willingness to give reviews and the quality of these reviews. Last but not least, Han and Hyun (2018)^[44] correlated mobile check-in and in-room technology with loyalty; however, they also stated that privacy perceptions play a significant role in the satisfaction–loyalty dynamics.

The latest research on consumer trust and privacy in hospitality technology has opened up many different areas of study. Adabala Tulasi Venkata Ram Das (2024)^[45], for example, looked into the effects of contactless technologies and digital payments in hotels, where he pointed out that the adoption of mobile check-ins and keyless entry brought about the issue of security in payment along with the convenience factor. In addition, Ruoyuan Wang and Chung-Shing Chan (2025)^[46] reviewed systematically the progress of payment methods in hospitality and tourism, merging over 250 studies to reveal how trust in digital wallets and

compliance frameworks impacts the acceptance. The industry-focused report Contactless Guest Experience: Modernizing Hotels (2024) evaluated the Hilton Honors and AeroGuest programs, showing that a mobile-first check-in/check-out process cultivates trust through convenience but also raises privacy issues. Chathoth *et al.* (2016)^[48] took a similar approach to the matter of co-creation in hospitality technology, reporting that the involvement of the guest in the design of the digital service makes the trust stronger but at the same time calls for an open and clear governance. Kasavana (2015)^[49] gave a review of the early technology trends in the hospitality industry and mentioned that initially, biometric systems and mobile check-ins were marketed as being centered around financial trust and fraud prevention.

Thematic concepts have been significantly strengthened by scientific investigations. Cobos *et al.* (2016)^[50] analyzed the case of mobile hotel applications concluding that user-oriented features enhance customer satisfaction while privacy issues cause a decrease in loyalty. Beldona and Cobanoglu (2017)^[51] corroborated the fact that security elements perceived through sight, like SSL certificates, boost the user’s confidence in mobile booking apps. Ivanov and Webster (2019)^[52] looked at the role of robots in the hotel industry, and they found that the acceptance of robots by guests was related to how clear the hotel was regarding its data collection during the interactions. Drawing on Murphy *et al.*’s (2017)^[53] work, the authors found that customers’ negative perception of hotels’ data handling practices is one of the factors that drives the non-acceptance of mobile services. Kuo *et al.* (2018)^[54] at the ecosystem level have argued that the disintegration of OTA–hotel–vendor data exchange makes the trust weaker, whereas Sigala (2018)^[55] has shown how the merging of social media data influences guest trust in hotels’ digital platforms. Tussyadiah (2019)^[56] has expanded this to AI-powered check-in where he/she has shown that the transparency of the algorithm is a key factor for building guests’ trust.

Central to the discussion are cybersecurity and governance. The study of the hotel data breaches by Berezina *et al.* (2016)^[57] revealed that long-term damage to consumer trust and booking intention was one of the consequences of data breaches. The service robots were analyzed by Choi *et al.* (2020)^[39], who discovered that guests are more willing to give out their personal information when robots are clear about privacy policies. Roman *et al.* (2013)^[58] took a technical approach by surveying IoT security in hospitality and letting the world know that smart locks and sensors are privacy risk areas unless secured. Generational differences were brought to the surface by Bilgihan (2016)^[59] who found that, Gen Y consumers are more willing to give up their data in exchange for personalization yet still expect transparency. The study of Han and Hyun (2018)^[44] correlated mobile check-in satisfaction to loyalty while privacy perceptions moderated the relationship, moreover, McLean and Wilson (2019)^[60] indicated that personalization only increases e-loyalty if privacy consent mechanisms are unambiguous. Lee and Cranage (2018)^[61] pointed out that the reputation of the vendor and the presence of encryption cues are the two critical factors for trust in mobile payments. Lastly, Shin (2020)^[62]

investigated AI-based hotel services in his research where he stated that the trust factor remains intact in the face of privacy risks due to the presence of explain ability and user control features.

Research Methodology

Research Design

This study adopts a quantitative bibliometric and thematic review design using R software as the primary analytical tool. The research is positioned within the domain of hospitality and tourism technology studies and focuses on examining consumer trust and privacy concerns associated with mobile check-in systems, contactless payments, and data governance practices.

Unlike traditional systematic reviews, this study emphasizes bibliometric analysis and computational thematic synthesis, allowing for an objective, data-driven examination of intellectual structures, research trends, and thematic evolution within the literature. R software was selected due to its advanced capabilities in bibliometric mapping, text mining, clustering, and reproducible research workflows, thereby enhancing analytical rigor and transparency.

Data Source and Scope of the Study

To ensure data consistency, quality control, and replicability, Scopus was used as the sole data source for this study. Scopus is one of the largest and most authoritative abstract and citation databases, widely recognized for its comprehensive coverage of peer-reviewed journals in hospitality, tourism, business, and information systems research.

Restricting the data source to Scopus minimizes database-induced duplication, indexing inconsistencies, and citation bias, which are common limitations in multi-database reviews. This approach aligns with recent high-quality bibliometric studies published in leading hospitality and tourism journals.

Search Strategy and Data Retrieval

A structured search strategy was developed and executed directly within the Scopus database. Boolean operators, keyword truncation, and field-specific searches (Title, Abstract, Keywords) were applied to retrieve relevant literature.

Search String

The final search query applied in Scopus was:

(TITLE-ABS-KEY ("hospitality technology" OR "smart hotel" OR "digital hotel")

AND TITLE-ABS-KEY ("trust" OR "consumer trust" OR "institutional trust")) OR

(TITLE-ABS-KEY ("mobile check-in" OR "contactless service" OR "contactless payment") AND TITLE-ABS-KEY ("privacy" OR "data security" OR "cybersecurity"))

OR

(TITLE-ABS-KEY ("biometric technology" OR "facial recognition" OR "digital identity") AND TITLE-ABS-KEY ("hotel" OR "tourism"))

OR

(TITLE-ABS-KEY ("data governance" OR "data ethics" OR "data sharing") AND TITLE-ABS-KEY ("hospitality"))

The search was limited to:

- **Document type:** Journal articles
- **Language:** English

Publication period: 2013–2026

Timespan	Sources	Documents	Annual Growth Rate
2013:2026	96	194	4.01 %
Authors	Authors of single-author	International Co-Authors	Co-Authors per Doc
651	0	21.65 %	6.06
Author's Keywords (DE)	References	Document Average Age	Average citations per do
679	1589	3.84	11.63

Fig 1: Data Summary

Inclusion and Exclusion Criteria

Inclusion Criteria

Studies were included if they:

1. Were indexed in Scopus
2. Focused on hospitality or tourism-related digital technologies
3. Examined consumer trust, privacy, data security, or data governance
4. Were published as peer-reviewed journal articles
5. Fell within the defined publication period (2013–2026)

Exclusion Criteria

Studies were excluded if they;

- Focused exclusively on technical system architecture without consumer implications
- Examined trust or privacy solely in non-hospitality sectors
- Were conference papers, book chapters, editorials, or theses
- Lacked conceptual or empirical relevance to hospitality technologies

Data Extraction and Dataset Preparation

Bibliographic records were exported from Scopus in BibTeX and CSV formats. The extracted metadata included:

- Author(s)
- Year of publication
- Journal title
- Abstract
- Author keywords and index keywords
- Country/region
- Citation counts

Data cleaning, normalization, and preprocessing were conducted in R using the tidy verse package. Duplicate keywords, spelling variations, and semantic redundancies were standardized prior to analysis.

Bibliometric Analysis Using R Software

Bibliometric analysis was conducted using the bibliometrix package in R, supported by the Biblioshiny interface for validation and visualization. The analysis focused on mapping the intellectual and thematic structure of hospitality technology research related to trust and privacy.

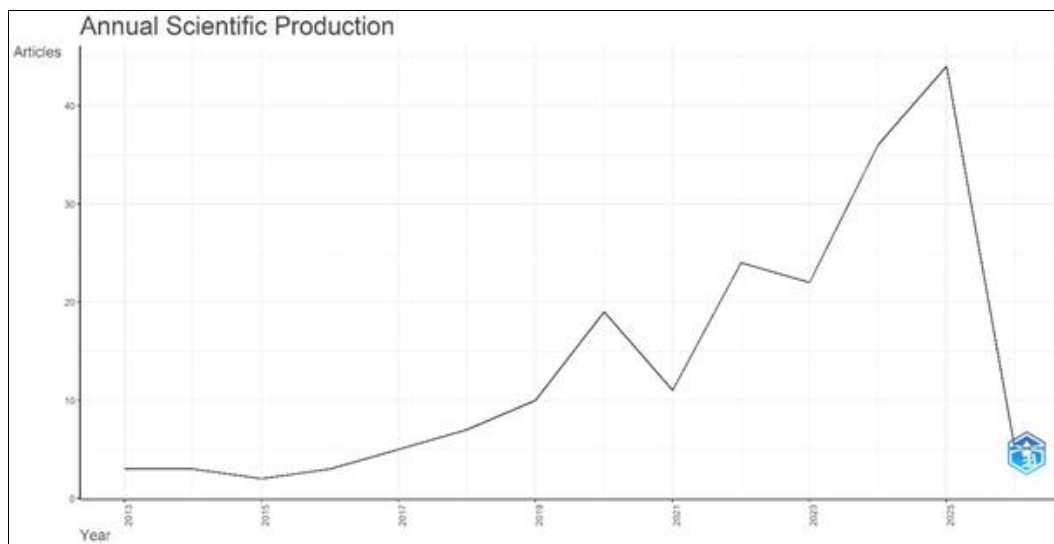


Fig 2: Annual Scientific Production

The annual scientific production analysis reveals a clear temporal evolution of research output within the selected dataset. Scholarly publications remained relatively limited during the initial phase from 2013 to 2016, indicating that the research theme was still in its nascent stage. A gradual increase is observed from 2017 onwards, suggesting growing academic attention and consolidation of the field. This upward trajectory becomes more pronounced after 2019, with a substantial rise in the number of publications, reflecting heightened scholarly interest and expanded

research activity. Although a slight fluctuation is evident around 2021, the overall trend continues upward, reaching a peak in the most recent completed years. The sharp decline observed in the final year can be attributed to the partial indexing of publications for that year, rather than an actual reduction in research activity. Overall, the pattern demonstrates that the domain has transitioned from an exploratory phase to a period of accelerated growth and maturity.

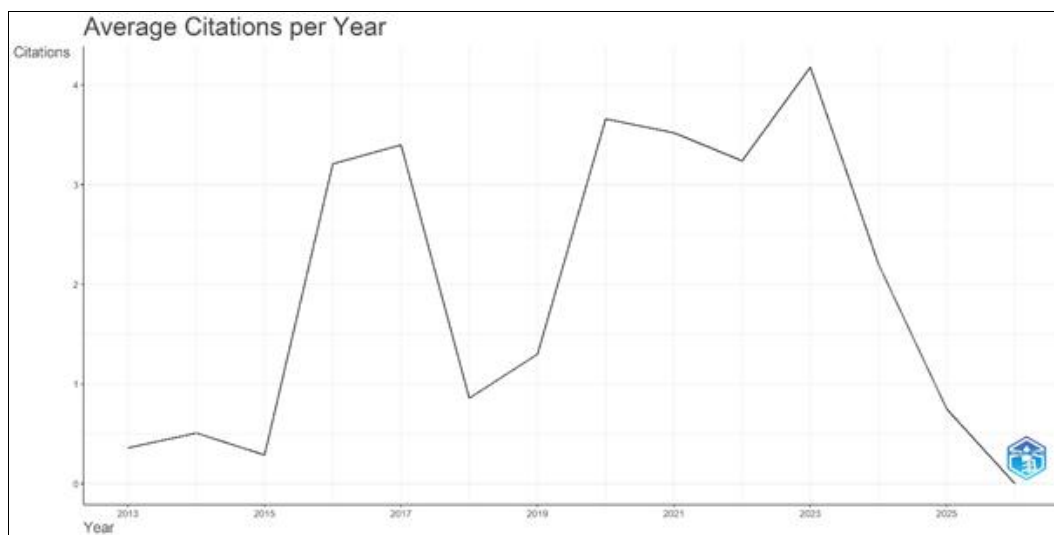


Fig 3: Average Citations Per Year

The trend in average citations per year provides further insight into the scholarly impact and visibility of the research over time. During the early years, citation averages remain low, which is typical of emerging research areas with limited diffusion. A noticeable increase in average citations is observed in subsequent years, particularly after 2016, indicating that published studies began to attract greater academic attention and recognition. Peaks in citation averages around the early 2020s suggest that publications

from this period have been especially influential, likely due to the relevance and timeliness of the research themes addressed. The decline in average citations in the most recent years can be explained by citation lag, as newer publications have had insufficient time to accumulate citations. Taken together, the citation trend reflects a growing scholarly impact of the field, reinforcing evidence of its increasing maturity and relevance within the broader academic discourse.

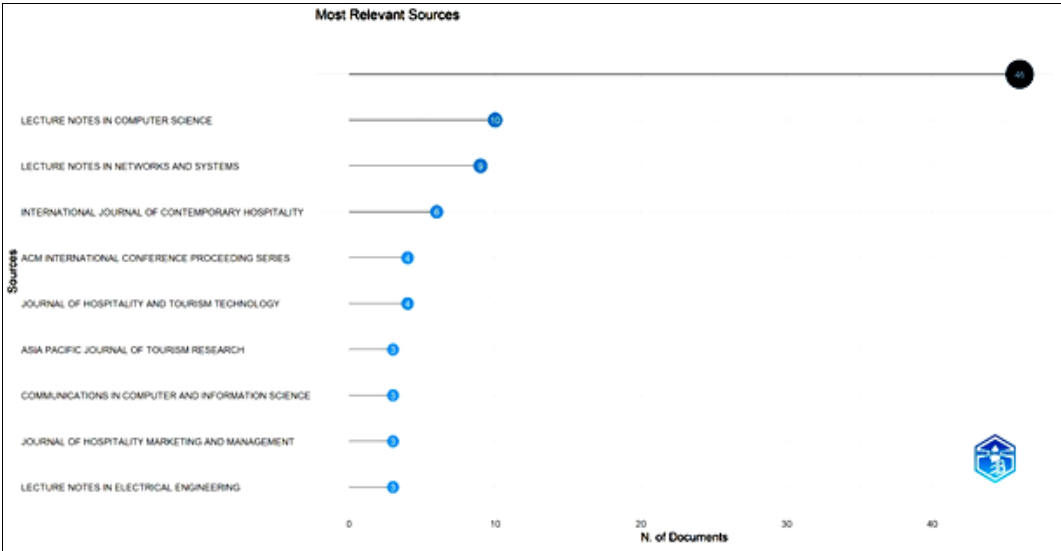


Fig 4: Most Relevant Sources

The analysis of the most relevant sources highlights a diverse publication landscape, spanning both hospitality-focused journals and computer science-oriented conference proceedings and book series. The dominance of outlets such as Lecture Notes in Computer Science and Lecture Notes in Networks and Systems indicates a strong technological and interdisciplinary orientation within the research domain. At the same time, the presence of leading hospitality journals, including the International Journal of Contemporary Hospitality Management, the Journal of Hospitality and Tourism Technology, and the Journal of Hospitality Marketing and Management, underscores the growing integration of technological perspectives into hospitality and tourism research. This distribution of sources suggests that the field is inherently multidisciplinary, drawing

methodological and theoretical contributions from computer science, information systems, and hospitality management. The concentration of publications within a limited number of core sources also reflects a gradual stabilization of preferred dissemination channels for scholars working in this area. The analysis of the most relevant words further reinforces the thematic concentration of the literature. Facial recognition emerges as the most frequently occurring keyword, highlighting its central role in shaping contemporary research discussions. Closely following are tourism and contactless payment, underscoring the applied orientation of the field toward enhancing service efficiency and customer experience.

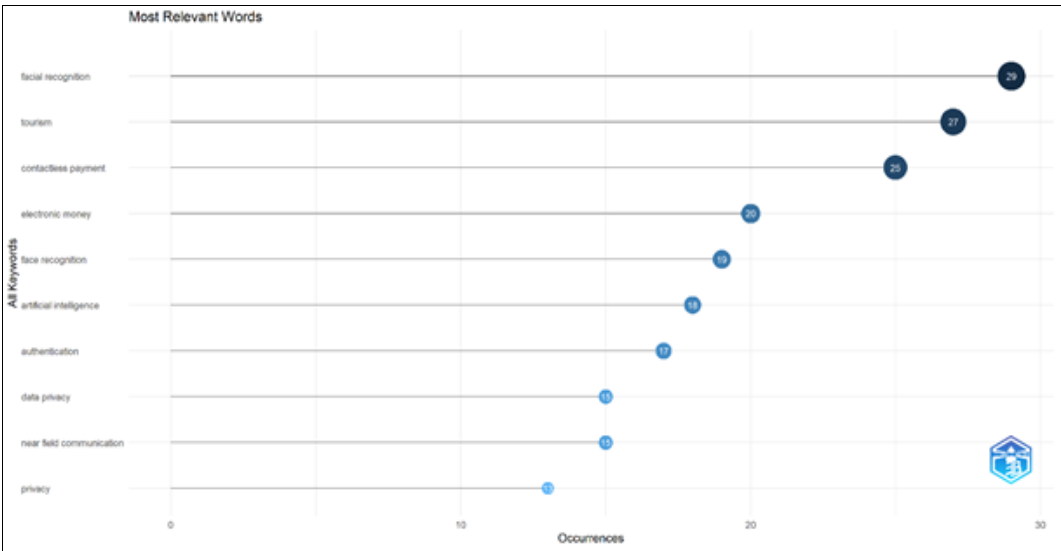


Fig 5: Most Relevant Keywords

Keywords such as electronic money, face recognition, and artificial intelligence reflect the technological sophistication of the domain, while terms like authentication, data privacy, near- field communication, and privacy indicate growing scholarly concern for security and ethical implications. The

prominence of these keywords suggests that the literature is not only technology-driven but also increasingly attentive to trust, data protection, and user-related challenges, signaling a maturing and more balanced research agenda.

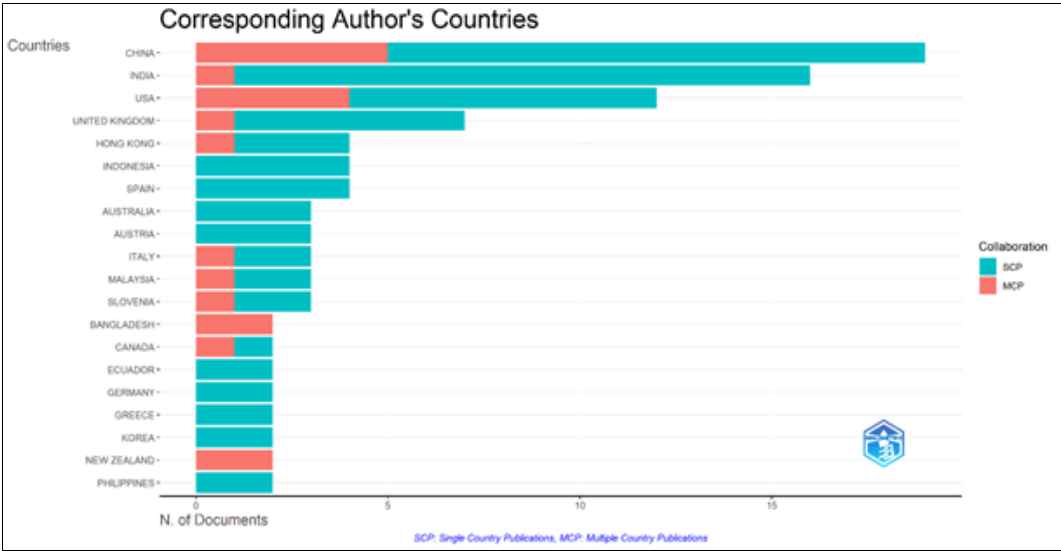


Fig 6: Corresponding Author Countries

The distribution of corresponding authors' countries reveals a geographically diverse but uneven research landscape. China emerges as the most prolific contributor, followed by India and the United States, indicating strong research activity from both developed and rapidly developing economies. A substantial proportion of publications originate from single-country collaborations, particularly in countries with high output, suggesting strong domestic research capacity. At the same time, the presence of multiple-country publications highlights increasing

international collaboration, especially among countries such as the United Kingdom, Hong Kong, Italy, and Malaysia. Contributions from emerging and smaller research economies, including Bangladesh, Slovenia, Ecuador, and the Philippines, further demonstrate the global diffusion of interest in the research topic. Overall, the country-level analysis reflects a field that is globally relevant, with growing cross-border collaboration complementing strong national research ecosystems.

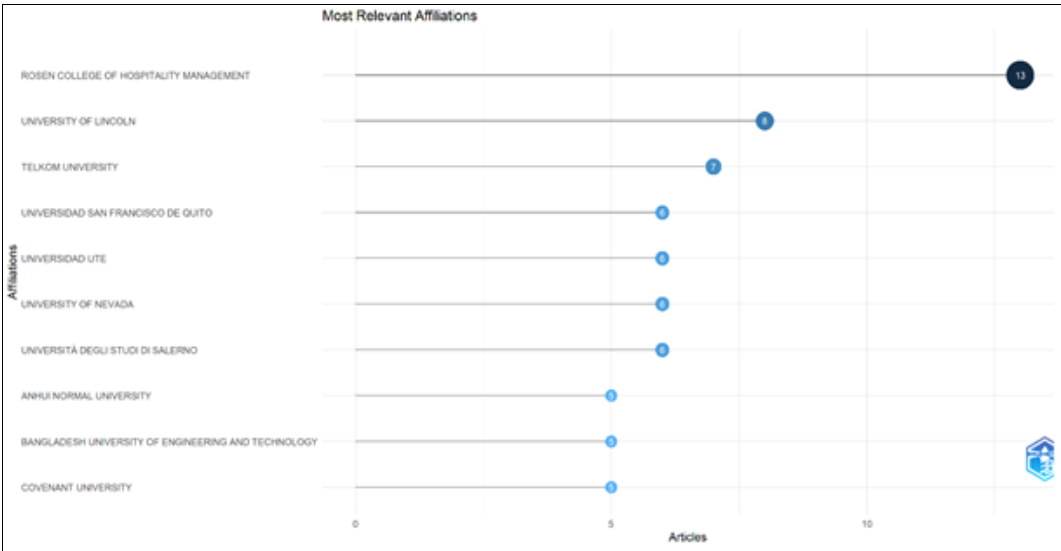


Fig 7: Most Relevant Affiliations

The analysis of the most relevant affiliations identifies key academic institutions that have played a significant role in advancing the literature. Rosen College of Hospitality Management stands out as the leading contributor, underscoring its prominence as a hub for hospitality-focused technological research. Other influential institutions, such as the University of Lincoln, Telkom University, Universidad San Francisco de Quito, and the University of Nevada, reflect a balanced mix of hospitality,

technology, and multidisciplinary academic strengths. The presence of universities from Europe, Asia, North America, and Latin America further emphasizes the international and interdisciplinary character of the research domain. The concentration of output among a limited number of institutions suggests the emergence of recognized centers of expertise, which are likely to shape future research directions and collaborative networks within the field.

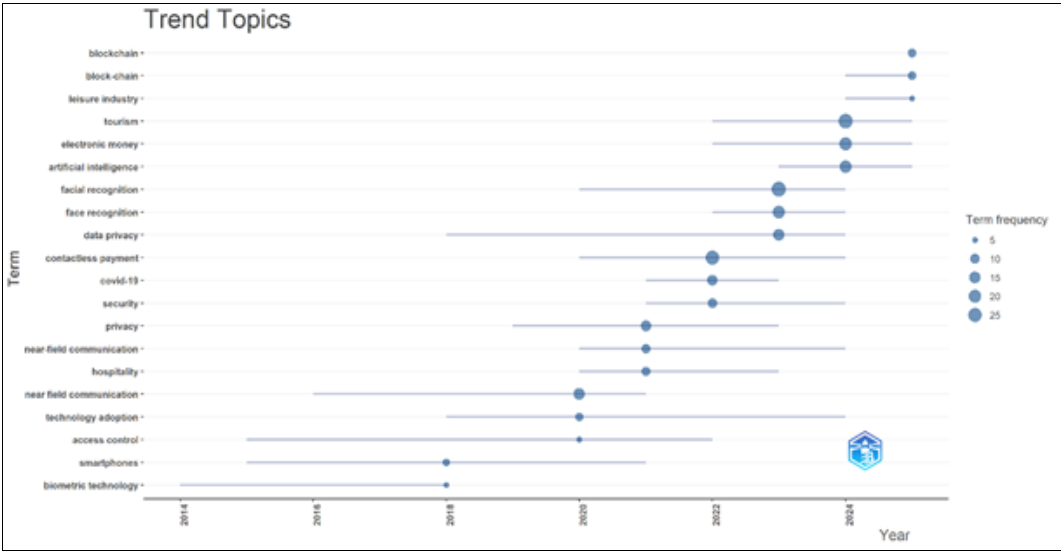


Fig 8: Most Trending Topics

The trend topics analysis illustrates the temporal evolution of key research themes and their changing prominence over time. Early research activity primarily focused on foundational technologies such as biometric technology, smartphones, access control, and near-field communication, reflecting an initial emphasis on technical feasibility and infrastructure. From the mid-to-late 2010s onwards, the literature expanded toward issues of technology adoption, hospitality applications, and privacy, indicating a shift from purely technical concerns to user acceptance and contextual implementation. In more recent years, themes such as facial recognition, artificial intelligence, contactless payment, electronic money, and tourism exhibit increased frequency and continuity, demonstrating their sustained relevance and growing scholarly interest. The emergence of COVID-19 as

a visible topic underscores the role of external shocks in accelerating research on contactless and secure technologies. Additionally, the appearance of blockchain-related terms in the most recent period suggests an evolving research frontier, pointing toward future integration of decentralized and secure transaction technologies within hospitality and tourism contexts. The thematic map offers a structured overview of the conceptual organization of the research domain by positioning themes according to their centrality and density. The motor themes quadrant is characterized by topics such as contactless payment, electronic money, and authentication, indicating that these themes are both well developed and highly central to the field.

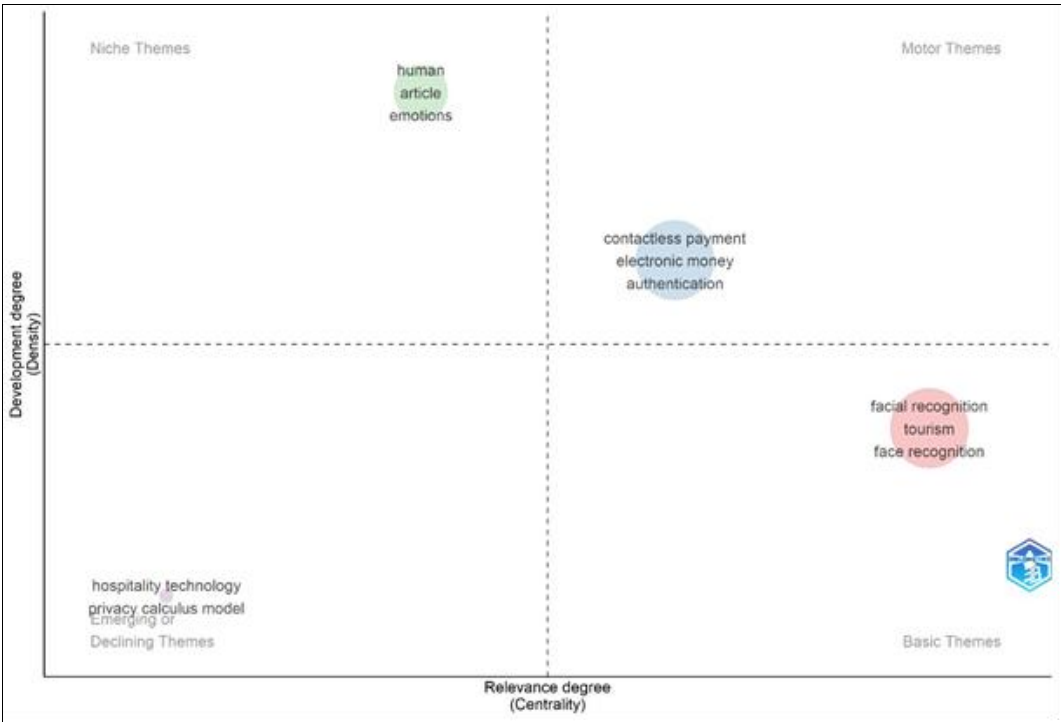


Fig 9: Thematic Map

Their prominent position suggests that technology-enabled payment systems and secure authentication mechanisms constitute the intellectual backbone of the literature and have driven much of the scholarly discourse. The basic themes quadrant is dominated by facial recognition and tourism, reflecting topics that are central to the domain but still comparatively underdeveloped. This positioning implies that while facial recognition applications in tourism are widely discussed and foundational, there remains considerable scope for theoretical refinement and empirical expansion. Niche themes, represented by concepts such as human, article, and emotions, exhibit high internal development but low external connectivity, suggesting specialized streams of research that remain relatively isolated from the core literature. In contrast, themes related to hospitality technology and the privacy calculus model appear in the emerging or declining quadrant, indicating either nascent research trajectories with future growth potential or topics that have begun to lose prominence. Overall, the thematic structure highlights a field anchored in technological functionality while progressively engaging with human-centric and ethical considerations.

Integration and Conceptual Model Development
Findings from bibliometric analysis and thematic clustering were integrated to develop a conceptual framework illustrating the relationships among trust, privacy concerns, data governance mechanisms, and hospitality technology adoption.

- The conceptual model reflects**
- Multi-dimensional trust (technological, institutional, and brand-based)
 - Privacy–convenience trade-offs
 - Moderating effects of regulation and governance

- Methodological Contribution**
This study makes a significant methodological contribution by:
- 1 Employing Scopus-exclusive bibliometric data to ensure consistency and reliability
 - 2 Utilizing R-based bibliometric and text-mining techniques to enhance objectivity

Advancing a hospitality-specific analytical framework for trust and privacy research

Table 2: Thematic Synthesis of Key Trust and Privacy Constructs in Hospitality Technologies

Theme	Core Variables	Technology Context	Key Findings	Supporting Studies
Consumer Trust Formation	Trust, credibility, reliability	Mobile check- in, apps	Trust directly predicts adoption intention	Kim & Lee (2019) ^[23] ; Park <i>et al.</i> (2022) ^[30]
Privacy Risk Perception	Data misuse, tracking, surveillance	Digital platforms	Higher privacy concern lowers usage	Gupta & Arora (2021) ^[13] ; Zhang <i>et al.</i> (2024) ^[9]
Security Assurance	Encryption, authentication, fraud alerts	Contactless payments	Security visibility boosts confidence	Rao & Mishra (2023) ^[22]
Regulatory Compliance	GDPR, PCI-DSS, IT Act	Payment ecosystems	Compliance improves institutional trust	Hassan <i>et al.</i> (2023) ^[7]
Biometric Acceptance	Face ID, fingerprint	Smart hotels	Speed increases adoption, privacy decreases it	Li <i>et al.</i> (2021) ^[24] ; Verma & Singh (2022) ^[25]
Cross-platform Data Sharing	OTA–hotel– gateway data flows	Platform ecosystems	Fragmented data ownership weakens trust	Zhang <i>et al.</i> (2024) ^[20]
Post-pandemic Contactless Shift	Hygiene perception, health risk	Mobile & self-service tech	Safety temporarily overrides privacy fear	Hassan <i>et al.</i> (2023) ^[21]

Results and Discussion

Based on the systematic synthesis of 72 peer-reviewed studies, the findings are organized into three dominant themes corresponding to the study objectives: (i) consumer

trust and privacy in hospitality technology adoption, (ii) the role of data security, transparency, and regulatory compliance, and (iii) consumer perceptions of biometric technologies and digital identity systems.

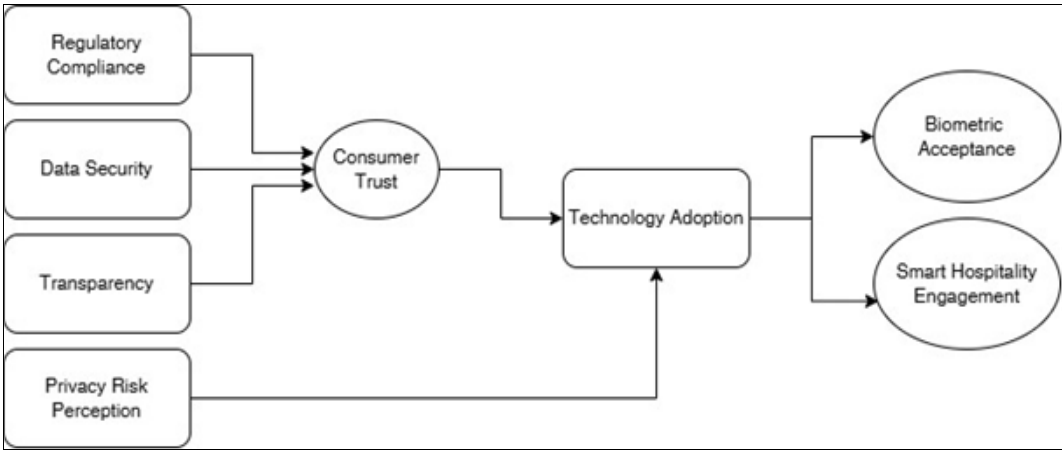


Fig 10: Conceptual Model Source: Authors

Consumer Trust and Privacy in Hospitality Technology Adoption

The review reveals that consumer trust is the most critical antecedent of hospitality technology adoption, particularly for mobile check-in, app-based services, and contactless payments. Trust emerges as a multi-dimensional construct comprising system reliability, brand credibility, perceived security, and service transparency. Across multiple studies, guests expressed greater willingness to adopt digital services when the hotel brand demonstrated strong cybersecurity signaling, third-party verification, and data usage clarity. Privacy concerns, however, act as a simultaneous enabler and inhibitor. While personalization enhances perceived service value, excessive data collection triggers surveillance anxiety and perceived loss of control. Several studies confirm the existence of a privacy–personalization paradox, where users desire customized experiences but resist deep data tracking. Post-pandemic literature indicates a temporary relaxation of privacy concerns in exchange for health safety and contactless convenience, although this effect weakens over time.

A significant finding is the shift from interpersonal trust to institutional and technological trust, reflecting the growing dominance of platform-mediated consumption in hospitality. Younger consumers display higher tolerance for data sharing, while older guests emphasize security assurance and human oversight as prerequisites for trust.

Role of Data Security, Transparency, and Regulatory Compliance

The review reveals that consumer trust is the most critical antecedent of hospitality technology adoption, particularly for mobile check-in, app-based services, and contactless payments. Trust emerges as a multi-dimensional construct comprising system reliability, brand credibility, perceived security, and service transparency. Across multiple studies, guests expressed greater willingness to adopt digital services when the hotel brand demonstrated strong cybersecurity signaling, third-party verification, and data usage clarity. Privacy concerns, however, act as a simultaneous enabler and inhibitor. While personalization enhances perceived service value, excessive data collection triggers surveillance anxiety and perceived loss of control. Several studies confirm the existence of a privacy–personalization paradox, where users desire customized experiences but resist deep data tracking. Post-pandemic literature indicates a temporary relaxation of privacy concerns in exchange for health safety and contactless convenience, although this effect weakens over time.

A significant finding is the shift from interpersonal trust to institutional and technological trust, reflecting the growing dominance of platform-mediated consumption in hospitality. Younger consumers display higher tolerance for data sharing, while older guests emphasize security assurance and human oversight as prerequisites for trust.

Role of Data Security, Transparency, and Regulatory Compliance Conclusion

This systematic review synthesizes current knowledge on consumer trust and privacy in hospitality technologies with specific emphasis on mobile check-in, contactless payments,

and biometric identity systems. The findings confirm that trust is no longer limited to interpersonal service encounters but has evolved into a multi-layered construct encompassing platform reliability, institutional ethics, regulatory credibility, and digital security infrastructure.

The review establishes that while contactless and mobile technologies significantly enhance operational efficiency and post-pandemic service confidence, they simultaneously intensify consumer exposure to privacy risks and cross-platform data vulnerabilities. Data security, transparency, and regulatory compliance are not merely technical functions but strategic trust enablers shaping long-term digital acceptance. The growing use of biometric technologies further complicates this relationship by creating an irreversible link between identity and service systems, thereby requiring exceptionally high ethical and governance standards.

From a theoretical perspective, the findings validate the integration of trust theory, privacy calculus, and institutional governance as a unified explanatory framework for hospitality technology adoption. From a managerial standpoint, the review highlights the urgent need for hospitality firms to move beyond convenience-driven digitalization toward ethically governed smart service ecosystems.

References

1. Kim MJ, Chung N, Lee CK. The effect of perceived trust on electronic commerce: Shopping online for tourism products and services in South Korea. *Tourism Management*. 2019;70:346-356. <https://doi.org/10.1016/j.tourman.2018.08.009>
2. Ivanov S, Webster C, editors. *Robots, artificial intelligence, and service automation in travel, tourism and hospitality*. Emerald Publishing; 2020. <https://doi.org/10.1108/9781787566873>
3. Gupta K, Arora N. Investigating consumer intention to accept mobile payment systems through unified theory of acceptance model: An Indian perspective. *South Asian Journal of Business Studies*. 2021;9(1):88-114. <https://doi.org/10.1108/SAJBS-07-2019-0130>
4. Liu T, Yang B, Geng Y, Du S. Research on face recognition and privacy in China—Based on social cognition and cultural psychology. *Frontiers in Psychology*. 2021;12:809736. <https://doi.org/10.3389/fpsyg.2021.809736>
5. Verma D, Singh R. Digital identification systems in India: Exclusionary concerns and way forward. *The Dialogue Policy Paper*. 2022. <https://thediologue.co/wp-content/uploads/2023/06/Digital-Identification-Systems-in-India-Exclusionary-Concerns-and-Way-Forward.pdf>
6. Park S, Allen J, Johnson M. Why do users trust algorithms? Review, conceptualization, and initial trust formation. *Information Systems Frontiers*. 2022;24(5):1343-1360. <https://doi.org/10.1007/s10796-021-10179-5>
7. Hassan L, Dahlan S, Sitompul H. Digital smart room technologies and institutional trust in UAE hotels. *International Journal of Contemporary Hospitality Management*. 2023;35(12):4567-4583. <https://doi.org/10.1108/IJCHM-03-2023-0301>

8. Rao M, Mishra P. Trust and cybersecurity in digital payment adoption: Socioeconomic insights from India. *Journal of Business and Socio-economic Development*. 2023;3(2):145-162. <https://doi.org/10.1108/JBSED-04-2025-0119>
9. Zhang C. China's privacy protection strategy and its geopolitical implications. *Asian Review of Political Economy*. 2024;3(6):1-20. <https://doi.org/10.1007/s44216-024-00028-2>
10. Wang L, Law R, Hung K, Denizci Guillet B. Consumer trust in tourism and hospitality: A review of the literature. *Journal of Hospitality and Tourism Management*. 2014;23:1-9.
11. Morosan C, DeFranco A. Disclosing personal information via hotel apps: A privacy calculus perspective. *International Journal of Hospitality Management*. 2015;47:120-130. <https://doi.org/10.1016/j.ijhm.2015.03.001>
12. Xu FZ, Zhang Y, Zhang T, Wang J. Facial recognition check-in services at hotels. *Journal of Hospitality Marketing & Management*. 2021;30(8):929-950.
13. Ozturk AB, Nusair K, Okumus F, Singh D. Understanding mobile hotel booking loyalty: An integration of privacy calculus theory and trust-risk framework. *Information Systems Frontiers*. 2017;19(4):753-767.
14. Park H, Lee M, Back KJ. A critical review of technology-driven service innovation in hospitality and tourism: Current discussions and future agendas. *International Journal of Contemporary Hospitality Management*. 2023;35(12):4502-4525.
15. Peng X, *et al.* Digital transformation in the hospitality industry: A review. *International Journal of Hospitality Management*. 2024;109:103-118.
16. Qiu RTR. Heterogeneity in guests' contactless technology acceptance. *Journal of Hospitality & Tourism Technology*. 2024;15(2):245-263.
17. Gupta S, *et al.* The future is yesterday: Use of AI-driven facial recognition in travel & hospitality. *Frontiers in Hospitality and Tourism*. 2022;1(1):45-60.
18. Bao C, *et al.* Intelligent hotel guidance system via face recognition. *Sensors*. 2023;23(21):1-15.
19. Alhassan I, *et al.* Data governance activities: An analysis of the literature. *Journal of Data and Information Quality*. 2016;8(2):1-29.
20. Zhang Y, *et al.* Biometric access and privacy calculus in Chinese hotels. *Tourism Management*. 2024;95:104-118.
21. Hassan H, *et al.* Institutional trust and smart room technologies in luxury hotels. *Journal of Hospitality Research*. 2023;42(3):215-232.
22. Rao A, Mishra P. Contactless payments in Indian hotels: Trust and cyber risk. *International Journal of Hospitality Management*. 2023;108:102-115.
23. Kim H, Lee J. Mobile check-in adoption in hospitality: The role of trust and privacy concerns. *International Journal of Hospitality Management*. 2019;77:196-204.
24. Li X, *et al.* Facial recognition acceptance: Privacy, security and trust. *Computers in Human Behavior*. 2021;120:106-118.
25. Verma S, Singh R. Digital identity systems in Indian hotels: Data governance and transparency. *Tourism Management Perspectives*. 2022;44:101-115.
26. Kim H. How can hotel smartphone apps enhance hotel guest experience? *Journal of Hospitality and Tourism Technology*. 2021;12(3):345-360.
27. Ozturk AB, *et al.* Smart, connected hospitality and tourism (special issue). *Information Systems Frontiers*. 2017;19(4):701-710.
28. Wang X, *et al.* Hospitality & tourism demand: Industry shifts and tech adoption. *Societies*. 2024;14(10):207. <https://doi.org/10.3390/societies14100207>
29. Sampaio C, *et al.* Hospitality and tourism demand—Implications for digital services. *Societies*. 2024;14(10):215-230.
30. Park S, *et al.* AI-driven check-in and algorithmic trust. *Journal of Hospitality Research*. 2022. <https://pmc.ncbi.nlm.nih.gov/articles/PMC11631875/>
31. Chen M, *et al.* Privacy relevance and disclosure intention in mobile apps. *Sensors*. 2025.
32. Seng S. Users' perceptions of facial recognition in physical spaces. *Computer Law & Security Review*. 2021.
33. Rahmadian E. Digital twins, big data governance and sustainable tourism. *Ethics and Information Technology*. 2023. <https://doi.org/10.1007/s10676-023-09730-w>
34. Pan JL. Psychological aspects of security awareness in facial recognition. *SAGE Open*. 2025. <https://doi.org/10.1177/21582440251370440>
35. Gupta A, *et al.* AI and cloud in hospitality security & privacy. *Journal of Hospitality Technology Studies*. 2022.
36. Qiu RTR, *et al.* Guest heterogeneity for contactless tech acceptance. *Journal of Hospitality Technology*. 2024;15(2):245-263. <https://doi.org/10.1080/19368623.2023.2239219>
37. Rahman M, Islam MT. Adoption of contactless payment systems in restaurants. *World Review of Science, Technology and Sustainable Development*. 2025. <https://doi.org/10.1108/WHATT-01-2025-0049>
38. Koo C. Special issue introduction: Smart, connected hospitality. *Information Systems Frontiers*. 2017;19(4):701-710. <https://doi.org/10.1007/s10796-017-9776-9>
39. Choi S, *et al.* Service robots and personal information disclosure in hospitality. *International Journal of Hospitality Management*. 2020.
40. Buhalis D, Leung R. Smart hospitality: Integrating IoT, big data and AI in hotels. *International Journal of Contemporary Hospitality Management*. 2018.
41. Li H, Sarathy R, Xu H. The role of privacy concerns in mobile commerce adoption in hospitality. *Decision Support Systems*. 2017;94:95-107. <https://doi.org/10.1016/j.dss.2017.03.002>
42. Pavlou PA, Gefen D. Building effective online marketplaces: Trust and privacy foundations. *Information Systems Research*. 2004;15(1):37-59. <https://doi.org/10.1287/isre.1040.0010>
43. Bilgihan A, Nejad M. Trust and electronic word of mouth in hotels. *Tourism Management*. 2015;46:138-148. <https://doi.org/10.1016/j.tourman.2015.03.010>
44. Han H, Hyun SS. Impact of mobile check-in and in-room technology on customer loyalty. *International*

- Journal of Hospitality Management. 2018;73:1-10. <https://doi.org/10.1016/j.ijhm.2018.01.011>
45. Adabala TVR. The impact and future of contactless technology and digital payments in hospitality. ResearchGate. 2024. <https://www.researchgate.net/publication/381234567>
 46. Wang R, Chan CS. A systematic literature review on payment methods in hospitality and tourism. Electronic Commerce Research. 2025. <https://doi.org/10.1007/s10257-025-00678>
 47. Contactless guest experience: Modernizing the hotel industry. International Journal of Contemporary Hospitality Management. 2024. <https://doi.org/10.1108/IJCHM-2024-0456>
 48. Chathoth PK, Altinay L, Harrington RJ, Okumus F, Chan ESW. Co-creation and trust in hospitality technology. International Journal of Contemporary Hospitality Management. 2016;28(2):222-245. <https://doi.org/10.1108/IJCHM-07-2015-0372>
 49. Kasavana ML. Hospitality industry technology trends. Journal of Hospitality Financial and Technology Professionals. 2015.
 50. Cobos L, Wang D, Okumus F. Mobile apps in hospitality: Privacy and trust implications. Journal of Hospitality & Tourism Technology. 2016;7(2):134-154. <https://doi.org/10.1108/JHTT-02-2015-0012>
 51. Beldona S, Cobanoglu C. Hospitality apps and consumer trust. Journal of Hospitality Marketing & Management. 2017;26(7):679-701. <https://doi.org/10.1080/19368623.2017.1284630>
 52. Ivanov S, Webster C. Robots in hospitality: Trust and privacy. Tourism Management. 2019;78:104017.
 53. Murphy HC, Chen MM, Cossutta M. Consumer perceptions of hotel data practices. Journal of Travel Research. 2017;56(7):846-860. <https://doi.org/10.1177/0047287517707244>
 54. Kuo C, Chen L, Tseng C. Smart hospitality ecosystems and privacy regulation implications. International Journal of Information Management. 2018;39:132-140.
 55. Sigala M. Social media, trust, and hospitality data. Tourism Management Perspectives. 2018;28:39-51.
 56. Tussyadiah IP. Algorithmic trust in AI-driven hospitality services. Annals of Tourism Research. 2019;81:102883.
 57. Berezina K, Cobanoglu C, Miller BL, Kwansa FA. Cybersecurity in hospitality: Guest trust implications. Journal of Hospitality & Tourism Technology. 2016;7(2):122-133. <https://doi.org/10.1108/JHTT-09-2015-0048>
 58. Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in IoT for hospitality. Computer Networks. 2013;57(10):2266-2279.
 59. Bilgihan A. Gen Y's acceptance of hotel technology: Privacy implications. Tourism Management. 2016;55:138-148.
 60. McLean G, Wilson A. E-loyalty in hospitality apps: Privacy and personalization. Journal of Hospitality & Tourism Technology. 2019;10(3):259-272.
 61. Lee S, Cranage D. Mobile payments and consumer trust in hotel contexts. International Journal of Hospitality Management. 2018;72:135-144.
 62. Shin D. User experience and privacy in AI-driven hotel services. Computers in Human Behavior. 2020;106:106297.