

BEYOND TECHNOLOGY: HOW ORGANIZATIONAL CULTURE TRANSLATES BIG DATA CAPABILITIES INTO CLOUD SECURITY IN HOSPITALITY SETTINGS

Ahmad Mohammad HERZALLAH ^{1*}, Osama Mohammad AL-RAWASHDEH ²,
Ahmed K. ELNAGAR ³, Salwa A.L. BARGHOUTHI ¹, Mohamed M. SHOAIB ³

¹ Al-Quds University, Faculty of Business and Economics, Department of Business Administration, Jerusalem, Palestine; ahirzallah@staff.alquds.edu (A.M.H.); sbarghouthi@staff.alquds.edu (S.A.L.B.)

² Al-Balqa Applied University, Aqaba University College, Hotel Management and Tourism Science, Salt, Jordan; osama.rawashdeh@bau.edu.jo (O.M.A.R.)

³ Taibah University, Applied College, Administrative and Financial Sciences, Madinah, Saudi Arabia; Hotel Management Department, Faculty of Tourism & Hotels, Suez Canal University, Ismailia, Egypt; Akelnagar2020@gmail.com (A.K.E.); malam@taibahu.edu.sa (M.M.S.)

Citation: Herzallah, A.M., Al-Rawashdeh, O.M., Elnagar, A.K., Barghouthi, S.A.L., & Shoaib, M.M. (2026). Beyond technology: How organizational culture translates big data capabilities into cloud security in hospitality settings. *Geojournal of Tourism and Geosites*, 66(2spl), 1758–1772. <https://doi.org/10.30892/gtg.662spl45-1806>

Abstract: Egypt's hospitality sector, vital to the country's economy, is rapidly adopting cloud computing for operational efficiency and personalization of guests. However, this digital transition introduces significant data security vulnerabilities, including the risk of breaches and ransomware. Big Data Analytics (BDA) presents a potential solution to strengthen cloud computing data security (CCDS), but mechanisms to effectively utilize BDA for this purpose have not been explored. This study examines the relationship between BDA capabilities and CCDS within the Egyptian hotel sector, and proposes organizational culture (OC) as a key mediating mechanism. Based on the resource-based view (RBV) and dynamic capability theory (DCT), the research examines the direct and indirect effects of big data technological capabilities (BDTC) and big data personal capabilities (BDPC) on CCDS. Data were collected through a structured questionnaire from 215 IT managers and directors in mid-scale and high-end Egyptian hotels and analyzed using partial least squares structural equation modeling (PLS-SEM). The results confirm that BDTC and BDPC both directly and indirectly significantly improve CCDS via OC. This study provides a clear, actionable framework for hotel and IT managers in Egypt and similar emerging economies to strategically align their technology investments and organizational practices to reduce cloud-related risks and protect valuable data assets.

Keywords: Big data analytics, cloud computing security, organizational culture, hospitality industry, PLS-SEM

* * * * *

INTRODUCTION

Egypt's hospitality sector is crucial to its economy, as it is closely tied to the country's rich cultural heritage and key geographic locations (Aboushouk & Tamamm, 2023; Ahmed et al., 2025; Herzallah et al., 2025). Millions of international travelers are drawn to Cairo, Luxor, Aswan, and the Red Sea resorts every year. Recently, the tourism sector has taken significant steps to utilize new technologies, particularly cloud computing, for more efficient operations, enhanced guest personalization, and the flexibility required to handle a growing number of tourists (Ahmed et al., 2025; Carneiro et al., 2023; Elnagar & Derbali, 2020; Zaki et al., 2025; Herman et al., 2016; Herman, 2009). Using cloud platforms promises hotels lower operational costs for their IT infrastructure, as well as simple access to data for making fast decisions and introducing new services quickly. Additionally, hotels generate substantial amounts of data, which includes guests' preferences, booking patterns, key performance indicators, and comments left at various touchpoints (Noby et al., 2022). Hotels in Egypt can gain a strong position in the industry by leveraging BDA to deliver hyper-personalized marketing, manage profits through data-driven means, utilize advanced analytics for preventive maintenance, and select resources more effectively (Aziz et al., 2024; Elnagar et al., 2022).

The aspect of adopting cloud technology systems within the hospitality industry for the processing of personal customer information, financial information, and business documents raises key information security risks, such as information breaches and violations (Ahmadi, 2024 ; Popescu et al., 2022). A recent research discussed the risks posed to Egyptian hotels, where the use of the cloud system risks financial and customer profile information to cyber threats, owing to the absence of appropriate infrastructural capabilities within the country (Aboushouk & Tamamm, 2023). Preserving confidentiality, ensuring data integrity, and providing access to data (the CIA triad) are the most important considerations (Ernest Chang & Lin, 2007).

* Corresponding author

<http://gtg.webhost.uoradea.ro/>

Like in many similar emerging markets, hotels in Egypt may have limited resources, new rules coming into effect (such as Egypt's Personal Data Protection Law), and noticeable skill shortages that increase the possibility of cyber-attacks, including data breaches, ransomware, and intrusion. Achieving absolute security in the cloud is vital for businesses today, ensuring that guests, regulations, and the brand's reputation remain secure. BDA not only provides businesses with important information, but it can also be used to actively identify and mitigate security risks in the cloud by analyzing usage patterns, detecting unusual activity, and predicting potential attacks (Noby et al., 2022).

However, this digital transformation and reliance on cloud platforms introduce significant security vulnerabilities. Moving sensitive data, including personal guest details, payment information and proprietary company files, to the cloud presents a new set of risks (Aboushouk & Tamamm, 2023). For hotels in Egypt, which may operate with limited resources, face new regulations such as Egypt's Privacy Law, and experience a lack of expertise, these risks are heightened, increasing susceptibility to cyber-attacks such as data breaches, ransomware, and intrusions. In this context, ensuring data confidentiality, integrity and availability (CIA Triad) is not just a technical issue, but a fundamental business imperative to protect guest security, regulatory compliance and brand reputation (Ernest Chang & Lin, 2007).

Cloud computing and BDA are increasingly crucial in the hospitality industry; however, research specifically on the combined advantages they offer to enhance data security in Egyptian hotels is lacking. While studies are available on BDA's impact on performance (Carneiro et al., 2023) and innovation (Aziz et al., 2024), as well as on security culture, without contextualizing the findings (Ernest Chang & Lin, 2007). There is a notable absence of dedicated research focusing on the interplay between BDA capabilities and OC, particularly regarding their effects on cloud security. Among the primary risks facing Egyptian hotels are inadequate cybersecurity systems, evolving regulations, and the challenge of integrating modern technology with traditional operational methods (Gómez-Talal et al., 2024). Due to these vulnerabilities, such establishments present appealing targets for hackers, resulting in significant losses, reputational damage, and potential legal implications (Noby et al., 2022). Many hotels are unaware of how to better leverage their investments in BDA (tools and skills) to enhance their cloud data security. Furthermore, the influence of OC, characterized by cooperativeness, support for innovative ideas, consistency, and encouragement of progress, in translating these capabilities into tangible security achievements remains unexplored, mainly in this domain. While cloud computing and BDA are increasingly crucial, research specifically examining their combined role in fortifying data security within the context of Egyptian hotels is notably absent (Abdelhamied, 2024; Noby et al., 2021). Though these two terms, cloud computing and BDAC, are critically explained in digital infrastructure across several service-centered industries, existing studies have largely examined them on an individual basis, particularly in showing the nexus of operational efficiency and firm performance, where data security and its presence or essence are underexplored (Vesterinen et al., 2024; Zizic et al., 2022; Carneiro et al., 2023) and innovation (Aziz et al., 2024), or discussed security culture in isolation (Ernest Chang & Lin, 2007). However, a critical gap exists in understanding the interplay between BDA capabilities (both technological and personal) and OC, and their subsequent combined effect on cloud security outcomes. Many Egyptian hotels struggle with how to strategically leverage their investments in BDA tools and skills to enhance cloud data security effectively. Existing studies focused on the influence of OC on BDAC or BDPC and cybersecurity, but few studies have examined the mediating role of capabilities such as BDTC or BDPC towards outcomes such as CCDS in hotels managing guests' information. The literature indicates the role of OC's characteristics in instilling security awareness, but does not capture innovativeness as the moderator in routing employees' talent towards encryption and threats in cloud technology (Willie, 2023; Leso et al., 2022; Alsheikh et al., 2018). Global hospitality studies relate big data to performance or cloud separately to efficiency, but no empirical models, typically PLS-SEM on 215 IT managers-test OC's mediation (6a & 6b) in emerging markets that face tourism-driven data surges. Egyptian contexts discuss security challenges without culture-capability linkages, and thus leave IT directors without actionable frameworks.

The novelty of the model is based on the dual mediation hypotheses, positioning OC as the mediator of technological capability (H1 & H2) and human capability (H3 & H4)-into security, H5, in a context that fits mid/high-end Egyptian hotels' realities, such as legacy systems and cyber risks. The sample size of 215 enables the conduct of a robust PLS-SEM analysis that extends the BDAC theory to hospitality security while validating Egypt-specific validates through practical insights for managers. This goes beyond descriptive studies by quantifying the indirect effects of informing policy amidst Vision 2030 tourism goals (Almasoudi et al., 2025; Nche et al., 2022). This research aims to bridge this gap by proposing that a strong OC is the pivotal trigger that enables hotels to harness their big data analytics potential for superior cloud CCDS (Figure 1).

Theoretically, this study contributes to RBV and DCT by integrating perspectives from information systems (BDTC, CCDS), human resource management (BDPC), and organizational behavior (OC). It goes beyond examining direct impacts to uncover the mechanisms-OC through which technical and human resources are translated into improved security outcomes, providing new insights into cybersecurity in the hospitality sector. Practically, it enables managers, IT leaders, and cybersecurity professionals in Egyptian hotels to make more effective decisions about how to focus and coordinate their current and future investments in BDA, thereby improving efficiency, guest satisfaction, and protecting their cloud data against risks. Recognizing that infrastructure, the workforce, and proper culture are essential enables the creation of stronger and more reliable information security (Busulwa et al., 2025).

This theory contributes to research on hospitality technology adoption by integrating information systems constructs (BDTC, CCDS), human resource principles (BDPC), and organizational behavior concepts (OC). It highlights the importance of conducting further research in various emerging economies (Aziz et al., 2024). It focuses on the mechanisms by which technological and human resources contribute to improved security outcomes, primarily through the influence of OC. It gives new insights into the RBV and Dynamic Capabilities as applied to cybersecurity. Its results will help other businesses in the region, as well as in other developing countries, with related digitalization and security issues.

REVIEW OF LITERATURE

1. Theoretical underpinnings

1.1. Big data technological capabilities

BDTC comprises the infrastructure, systems, and components required for organizations to handle and analyze large and diverse datasets at high speed. In cloud-based security in hotels, the main points to remember are Connectivity, Modularity, and Compatibility. Allowing various systems (such as PMS, POS, CRM, IoT sensors, guest Wi-Fi, and social media) to connect provides a more comprehensive way to maintain overall security (Nadkarni et al., 2019). Because the stack is built of scalable, changeable components (such as cloud storage buckets, data processing clusters, and analytics tools), hotels can handle data growth or update security features without having to rebuild the system from scratch. Ensuring these solutions are compatible enables various platforms and data to work together, which is necessary for integrating specialized security tools into a hotel's cloud system and databases (Lee et al., 2020). Prior research highlights the transformative role of BDTC in the hospitality industry. According to research, its influence is apparent, as studying what customers say online has helped hotels provide more suitable services to their guests and improve their satisfaction (Lee et al., 2020). Due to the internet and data integration in the hotel industry, a concept called the "Hotel of Things" is being developed, which relies heavily on practical and up-to-date BDTC (Nadkarni et al., 2019). Since there are few similar studies in Egypt, research in other comparable markets helps demonstrate how BDTC can be improved operationally. Yet, effectively applying the components of BDTC, especially their ability to catch unusual activities in the cloud (such as strange access or data movement), is understudied and highly crucial for protecting Egyptian hotels' data. Most of the literature highlights benefits like serving customers faster or running operations smoothly, but security is often not given sufficient attention. Literature discusses BDAC adoption barriers, such as infrastructure and privacy issues in Egyptian hospitality (Aziz et al., 2024; Horng et al., 2022; Noby et al., 2021), but does not take into account the direct and indirect routes of BDTC or BDPC to CCDS via OC, although cloud transitions are exposing guest payment data to breaches (Ilieş et al., 2017).

1.2 Big data personal capabilities

BDPC encompasses the knowledge and skills of individuals within an organization, enabling them to utilize big data effectively. Security of cloud data in the hotel industry is divided into two essential domains: acquiring technical skills and gaining business knowledge. To possess technology skills, one must be efficient in data management, programming (for instance, with Python and SQL), statistical analysis, machine learning that identifies irregularities, utilizing cloud systems (mainly AWS and Azure), and be familiar with cloud security principles. Knowledge of the hotel industry involves learning how the business is run, managing earnings, serving guests, and being familiar with various types of sensitive information (like guests' and inventory details). Both sets of skills are essential; staff are expected to utilize data and understand security threats to address what may impact guests or the hotel the most in its daily operations (Jiang et al., 2019).

Human-centric challenges significantly hinder the development and utilization of BDPC. More people interested in data science and security work are needed in the hospitality industry, but there are not enough (Nadkarni et al., 2019). Both big data and cybersecurity are constantly evolving, which requires large organizations to invest in regular training. Additionally, ensuring that people understand how to handle data involves more than just technical classes; it also consists of making data literacy accessible to everyone and helping them comprehend the intersection between their work and data protection (Nosrati et al., 2024). When organizations resist change, keep teams separated into departments, and fail to clarify security roles, it is more difficult for BDPC to be carried out effectively. Overcoming these problems enables Egyptian hotels to leverage technology in their cloud systems by implementing security intelligence and best practices.

1.3 Organizational culture

OC refers to the shared values, beliefs, practices, and standards that determine how technology is used and secured within an organization (Al-Ali et al., 2017). Effective use of big data in cloud security relies greatly on cooperativeness (collaboration), innovativeness (exploring new security technologies), Consistency (applying established security standards), and Effectiveness (meeting security goals efficiently). A workplace that prioritizes these elements will see employees view themselves as responsible for security, not just IT specialists (Nosrati et al., 2024).

It is widely recognized that OC supports better success in adopting technology and in using security practices. Rapid sharing of security information and efficient incident response become possible when teams are cooperative. An innovative organization explores ways to use BDA instead of waiting to solve problems through standard fixing. Applying data-driven security teams uniformly minimizes the possibility of inconsistent actions that lead to weaknesses. Such a culture concentrates resources on security efforts, and data analysis proves to yield the most significant payoff in terms of safety (Jiang et al., 2019). A good security culture, founded on these factors, helps employees stay motivated to comply, report rare incidents, work safely with cloud tools, and increase the strength of the human firewall, which is highly susceptible to risks and is usually more vulnerable than modern technologies.

2 Research hypothesis & model

2.1 Influence of big data technological capabilities

RBV believes that companies achieve a competitive advantage through valuable and scarce resources (Barney, 1991). BDTC, as a tangible technological resource, can be a source of such benefits (Shamim et al., 2021). Furthermore, sociotechnical systems theory emphasizes that technical systems (the "technical" subsystem) inevitably interact with and shape the social structures and practices of an organization (the "social" subsystem).

While BDTC is often studied for its operational benefits, its role as a shaper of organizational norms is underexplored. A core tenet of socio-technical systems theory is that technology is not neutral; it imposes structures that necessitate new forms of work, communication, and decision making (Lunde et al., 2019). For instance, the connectivity facet of BDTC requires IT, security, and operational departments to collaborate on integrated data flows, thereby actively fostering a culture of cooperativeness (Nadkarni et al., 2019). BDTC also entails the application of highly advanced technologies such as data storage systems, machine learning software, and big data analytics software that enable organizations to analyze large amounts of data (Topcu et al., 2025; Lyu et al., 2022). The implementation of these technologies in an organizational setup may warrant a change in OC. Organizational circumstances that embrace BDTC may hence experience an organizational culture change towards an environment that emphasizes data-driven decision-making, collaborative work, and an openness to advancing technologies. Generally, the application of big data software may transform organizational values, practices, and behaviors, hence shifting an organizational culture towards a more digital environment. A recent empirical study among 260 respondents of Malaysian hotels validated that BDAC aspects, including technology, make a direct positive impact upon innovation capabilities, thereby embedding analysis into the organization's culture and practices through technology enablers (Aziz et al., 2024; Naz et al., 2022). BDTC impacts adaptive hospitality cultures during the adoption of the cloud, thereby establishing strategic BDMCs (like management and technology integration) to create data-driven environments resulting in service innovation and excellence during this pandemic period (Song et al., 2025; Liu et al., 2022; Chen et al., 2022). The very presence of a sophisticated data infrastructure signals organizational commitment, legitimizing data-driven decisions and cultivating a culture of consistency and effectiveness. Therefore, we formally hypothesize:

H1: BDTC have a significant influence on OC.

The technology BDTC offers enables the enhancement of cloud-based data security by improving Confidentiality, Integrity, and Availability (CIA). When networks are advanced, security-related logs and events can be collected from various sources (e.g., the cloud, network, applications, and devices) into a single location for enhanced monitoring (Rasool et al., 2025). Because of modularity, hotels can easily deploy updated versions of security analytics programs (such as SIEM, UEBA, or IDS/IPS) in their cloud environment when new types of threats emerge. With compatibility, these security solutions can integrate with cloud providers' security offerings (such as AWS Guard Duty and Azure Security Center) and existing hotel software, forming a unified protection layer. Most importantly, BDTC enables the instant monitoring of suspicious events, the identification of threats promptly by analyzing large security logs, the triggering of a rapid response to security risks through automation, and the prediction of outcomes based on collected data (Shamim et al., 2021). BDTC integrated into an organization's operations contributes much toward the improvement of CCDS. This BDTC incorporates real-time analytics, advanced encryption protocols, anomaly detection, and automated response systems have helped organizations to get better means of identifying and mitigating potential security threats in cloud environments (Pour et al., 2022; Makhloufi et al., 2023). The use of predictive capabilities of big data not only improves the security of clouds, but it also keeps organizations ahead of all the risks and potential vulnerabilities. The higher the BDTC is, the robust the CCDS will be, hence making it one of the important relationships in the context of secure cloud computing. Research papers identify big data tools that support machine learning algorithms, which may be used to detect fraudulent patterns in bookings and payments, reinforcing the barriers against data breaches within the hospitality industry, where sensitive guest profiles are being managed using cloud platforms (Hornig et al., 2022). A reliable approach to BDTC also facilitates the management of data encryption, access rules, and security updates in multi-server cloud systems, thereby directly protecting both data integrity and confidentiality (Nosrati et al., 2024). Thus, the BDTC infrastructure at a hotel plays a crucial role in securing its cloud data assets. Thus, we hypothesize a direct path:

H2: BDTC have a significant direct influence on CCDS.

2.2. Influence of big data personal capabilities

The Knowledge-Based View (KBV), an extension of the RBV, identifies knowledge as the most strategically significant resource. BDPC represents this critical human capital. Organizational Learning Theory further clarifies that for knowledge to be impactful; it must be shared and embedded into the organization's routines and culture.

People with strong BDPC skills help make the organization alive and vibrant. Thanks to their tech abilities, they can experiment with and start using new methods in security analysis and threat identification, which helps spark innovativeness (Shamim et al., 2021). Because of their business background, they can connect technical problems with specific actions for each department (for instance, describing a payment data weakness to the finance team or talking about access control with the front desk). This approach enables different groups to work more effectively together by fostering understanding and agreement on common objectives (Nadkarni et al., 2019). It also makes the strategy more effective by allowing staff to identify exact weaknesses using data and suggest solutions that maximize security investments. Because they manage even the most minor details with accuracy, APM supports consistency in everything. Proactive personnel search for areas to improve, which leads to a culture of ongoing advancement rather than just compliance. BDPC constitutes the human engine that drives the effective use of technological resources. According to the KBV, the knowledge and skills of individuals are primary determinants of an organization's ability to perform complex tasks. Employees with strong Technology Knowledge are not just operators; they are change agents who can identify opportunities for innovation in security analytics, thereby actively promoting an Innovative culture. Their Business Knowledge is equally critical, as it allows them to translate technical risks into business-impacting terms, facilitating cooperation between technical and non-technical units and ensuring security policies are understood and consistently applied (Nadkarni et al., 2019). This combination of skills embeds data proficiency into the fabric of the organization, shaping a culture that is both Consistent in its processes and Effective in its outcomes (Lunde et al., 2019b). Consequently, we propose:

H3. BDPC have a significant influence on OC.

The direct effect of BDPC on security is a function of applied expertise. While BDTC provides the tools, BDPC provides the intelligence to wield them effectively. Technically skilled personnel are required to correctly configure complex cloud security settings (IAM roles, encryption keys), write scripts for automated threat response, and accurately interpret the outputs of security analytics to distinguish false positives from genuine threats (Gupta & George, 2016). The business acumen within BDPC ensures that these technical efforts are strategically directed, prioritizing the protection of the most critical assets, such as guest databases and payment systems, thereby making the security posture both robust and efficient (Nosrati et al., 2024). This leads to the hypothesis:

H4. BDPC have a significant influence on CCDS.**2.3 Influence of organizational culture on cloud security**

CCDS in hotels is believed to benefit from OC, characterized by cooperativeness, innovativeness, consistency, and effectiveness. Although tools are essential, the effectiveness and regularity with which confidentiality, integrity, and data availability are protected rely heavily on the organization's culture. A culture of cooperativeness is paramount for robust CCDS. Security does not depend entirely on the IT team; all parts of the organization need to cooperate. As guest data, financial information, and IoT data are present across the roles of the staff, everyone is involved in handling sensitive material. A culture of cooperation removes organizational barriers, ensures the sharing of security problems, and enables people to act quickly by reporting phishing attacks and participating in quick incident response efforts (Nadkarni et al., 2019). Having departments support one another means a greater understanding and acceptance of security policies, which reduces confusion and the likelihood of new vulnerabilities. Innovativeness within the OC drives proactive security enhancement. A company with an innovative culture tests various security analytics tools, examines advanced threats using big data, and applies the latest security practices in cloud environments. Instead of waiting for problems, innovative hotels work to strengthen their systems by using BDTC and BDPC (Shamim et al., 2021). The fact that cyber threats are constantly evolving means that this forward approach is crucial. Consistency is the bedrock of reliable CCDS. Ensuring that security policies, procedures, and protocols are consistently and accurately applied across all levels and departments is the purpose of this dimension (Nosrati et al., 2024). Not adhering to password policies or using the same multiple authentication steps across the company provides attackers with easy opportunities to compromise the system. When security policies are regularly followed, organizations have fewer vulnerabilities and a robust, comprehensive security framework.

Finally, by focusing on Effectiveness, organizations verify that their security actions are meaningful and bring results. Having an effectiveness-oriented culture means Security initiatives are led by risk assessments and data analysis, which allows the best use of time, money, and staff. This approach centers on determining outcomes, such as fewer security events, by focusing more on performance results than on simply tracking actions (Rasool et al., 2025).

The fact that the approach is centered on results means that the security actions taken are effective in protecting cloud data. Essentially, having a positive security culture built on these four points turns security into something the whole organization supports. It enables employees to monitor data closely, requires robust and up-to-date security systems, and focuses on proper protection, which enhances the hotel's defense against a range of cloud-based threats.

H5: OC has a significant influence on CCDS.**2.4 Organizational culture as a mediator**

Although BDTC and BDPC make essential contributions to CCDS in technology and human expertise, respectively, the way they help is largely guided and enhanced by OC. The mediation hypothesis posits that OC provides the essential environment that enables technology and people to develop successful security practices (Alsheikh et al., 2018). A synthesis of relevant studies supports this mediating role. Due to its BDTC (connectivity, modularity, and compatibility), sophisticated cloud environments can implement top-level security monitoring and threat detection (Nadkarni et al., 2019). However, this opportunity will not arise unless there is a culture that supports its use for security purposes. An innovative OC seeks ways to leverage new technology in security, such as linked data streams, which can be used to monitor unusual activity in real time. Using the effectiveness of BDTC helps make sure efforts contribute mainly to key security outcomes. If there is no common cultural understanding, BDTC may not be utilized effectively, leading to misconfiguration or inconsistent use, which in turn weakens its primary protective effects (H2) and renders capabilities ineffective. As a result, OC determines how BDTC is utilized for security purposes (Shamim et al., 2021).

While BDTC provides the techno-platform foundation for cloud security, it is the organization's culture that will define how these technologies will be put into practice. A strong organizational culture concerning security and integrity of data can enhance the BDTC to lead to a highly improved cloud security outcome. Organizational culture acts as a mediator of the BDTC and CCDS association through the channeling of such advanced tools as analytics platforms and scalable infrastructure into appropriate security practices through supportive norms, having priority on innovation, data sharing, and awareness of risk in hospitality (Horani et al., 2025; Leso et al., 2022). Recent findings based on recent studies of 183 firms using PLS-SEM demonstrate that digital and adhocratic cultures facilitate a vital mediation role in linking the antecedents of BDAC to the secure deployment of analytics by developing an enabling environment where technological investments translate into privacy-compliant processes (Orero-Blat et al., 2024). Such mediation has intensified the concept of hospitality, whereby data-driven OC helps hotels leverage BDTC in real-time threat monitoring and encryption during cloud migration, as evidenced in five-star hotels in Turkey, where digital transformation mediates BDAC to innovation outcomes (Demir et al., 2025). Empirical models in emerging markets in turn continue to validate the indirect effects of OC

in magnifying the strategic effects of BDTC on protective measures such as anomaly detection in the flow of customer data. This is a copyright-free work, and upon completion, this publication can be cited and even distributed freely (Arshad et al., 2022; Leso et al., 2022). Hence, the hypothesis is as:

H6a: OC has a significant mediating effect on the relationship between BDTC and CCDS.

Similarly, BDPC represents hidden expertise. OC is the enabling environment that determines whether this expertise is isolated or utilized throughout the organization. A collaborative culture enables data professionals to effectively communicate risks and solutions. A consistent culture ensures that the processes they design are universally adopted. Employees possessing superior skills regarding data capabilities can also help to enhance the data security and cloud storage, whereas the impact of these skills may differ depending upon the organizational culture.

Perspectives of the employees concerning the security of the data will help to capitalize on the capabilities of the employees to overcome the challenges in the clouds (Mosqueda, 2023; Ebert et al., 2021). Research validates the mediating role of organizational culture on big data work and decision-making, including storage, analytics, and data visualizations, and by extension, within cloud security, as a stimulating culture fosters qualified IT personnel to devise effective security measures such as access controls and encryption techniques (Horani et al., 2025; Orero-Blat et al., 2024). The Egyptian hospitality industry contexts validate the role of organizational cultures, where skilled personnel can have a greater impact on high data security, as adhocratic and digital cultures can effectively integrate personnel capabilities to support analytics security within growing tourist data (Li & Zhang, 2025).

An effective culture values and rewards their contribution to safety results. In the absence of such a culture, even highly skilled individuals may face resistance, covert operations, and lack of support, which greatly limits their impact on the overall security of the organization (Almeida et al., 2024; Wang et al., 2020). Therefore:

H6b: OC has a significant mediating effect on the relationship between BDPC and CCDS.

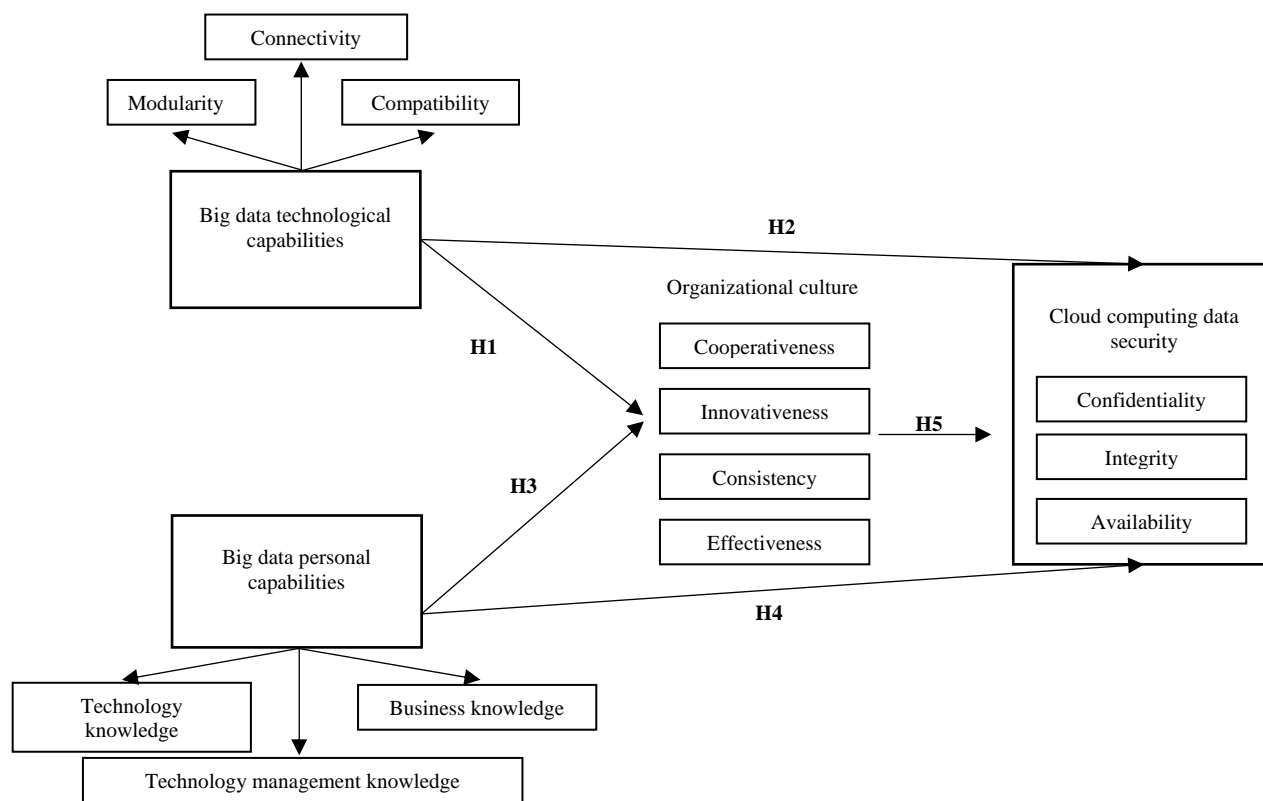


Figure 1. Theoretical framework and research hypotheses

METHODOLOGY

1 Sampling procedure

To determine the study population, this research focused on the Egyptian hotel sector, particularly midscale and upscale hotels operating in Cairo and Sharm El-Sheikh, which are the regions known for their significance in Egypt's hospitality and tourism industry, and currently employ the use of cloud information systems. A purposive sampling technique was employed to identify hotels utilized in order to guarantee that the surveyed individuals had decision-making capacities in the areas of Information Technology or information security. The list of the targeted hotels was taken from official membership rosters of the Egyptian Hotel Association (EHA) (Stephens, 2023). The key respondents targeted were IT managers, data analysts, and departmental directors. These individuals were selected based on their strategic roles in technology management, OC development, and data security practices—core themes of this research. From March to June 2025, data were collected using a structured questionnaire administered both physically and electronically, depending on the respondent's accessibility and preference. A total of 300 questionnaires were distributed across the selected hotels. With follow-up efforts and managerial

cooperation, 215 valid (135 were from Cairo and the rest from Sharm El-Sheikh) and complete responses were received by the data collection cut-off date, yielding a response rate of approximately 72%. All respondents participated voluntarily and provided informed consent. Ethical guidelines regarding anonymity and confidentiality were strictly followed. Although we did not claim representativeness of the Egyptian hotel sector in general, the existing sample can sufficiently represent the segment of the organization under which cloud data security risks lie, which corresponds with our research goals. The survey was conducted in English, the predominant business language used in multinational and upscale hotel chains operating in Egypt. Clarification was provided when necessary to ensure accurate comprehension of the items.

The Egyptian hotel sector was selected due to its dynamic and technology-driven environment, offering a relevant context for investigating BDA, OC, and CCDS. However, the findings may reflect specific contextual characteristics unique to Egypt; therefore, future studies are encouraged to validate the results in different geographical or industry settings.

The sample size of 215 was evaluated for sufficiency for Partial Least Squares Structural Equation Modeling (PLS-SEM). A common heuristic for minimum sample size in PLS-SEM is the '10-times rule' (Elnagar & Aljuwaiber, 2026; Hair et al., 2019, 2017; Zaki & Elnagar, 2025). It is critical to note that this rule refers to the larger of two criteria: (1) ten times the largest number of formative indicators for any single construct, or (2) ten times the largest number of structural paths directed at any latent variable in the structural model. This study uses reflective indicators, so the first criterion is not applicable. We must apply the second criterion. In the proposed structural model (Figure 1), the construct OC is predicted by two paths (from BDTC and BDPC), and CCDS is predicted by three paths (from BDTC, BDPC, and OC). Therefore, the maximum number of paths pointing at any construct is three. Applying the 10-times rule yields an absolute minimum sample size of $10 * 3 = 30$. While the sample of 215 is vastly larger than this heuristic minimum, a more robust approach is a power analysis. Using G*Power software (Faul et al., 2009) for a linear multiple regression test with three predictors, an effect size f^2 of 0.15 (medium), an alpha of 0.05, and a power of 0.80, the recommended minimum sample size is 77. Our final sample of 215 far exceeds this requirement, providing strong assurance of the statistical power for the PLS-SEM analysis conducted in this study. The demographic profile of the 215 respondents revealed that 73.5% were male and 26.5% were female, indicating a male-dominated respondent pool. In terms of age distribution, the majority (58.6%) were aged 35 years or below, followed by 34.4% between 36 and 45 years, suggesting a predominantly young workforce in the sampled hotels. Regarding education, 42.3% held an intermediate qualification, while 22.3% had completed university degrees, and another 22.3% possessed a master's or Ph.D. qualification, reflecting a relatively educated sample. Concerning professional experience, 41.4% had 5 years or less, and 37.7% had between 5 to 10 years, highlighting that most respondents were in the early to mid-stages of their careers.

2 Measurement items

Following an extensive literature review, this study adopted and adapted established measurement scales to align with the study's conceptual framework and research objectives. The scale for BDA was adapted from Anwar et al. (2018), which distinguishes between technological and personal capabilities. The technological capabilities dimension included three subdimensions: Connectivity (CONN1 to CONN4), Computability (COM1 to COM4), and Modularity (MOD1 to MOD4), each measured using four items. The personal capabilities dimension comprised Technology Knowledge (TK1 to TK4), Technology Management Knowledge (TMK1 to TMK4), and Business Knowledge (BK1 to BK4), also with four items per subdimension. All items were adapted to reflect the organizational context under investigation and pre-tested for clarity and relevance. The OC scale was adapted from Ernest Chang & Lin (2007), capturing four key cultural dimensions essential for managing information effectively. The construct included Cooperativeness (COOP1 to COOP8), Innovativeness (INN1 to INN6), Consistency (CONS1 to CONS6), and Effectiveness (EFF1 to EFF6). Academic experts in organizational behavior reviewed these items to ensure cultural and contextual appropriateness before field administration.

To measure CCDS, this study adopted the scale developed by Wang et al. (2020), which captures security affordances from a cloud management perspective. The three subdimensions—Confidentiality (CONF1 to CONF5), Integrity (INT1 to INT5), and Availability (AVA1 to AVA3)—were each operationalized with three to five items. The items were slightly revised to align with the broader scope of enterprise-level cloud deployments and subsequently verified through expert validation and a pilot study. All survey items were measured using a 7-point Likert scale ranging from 1 ("Strongly Disagree") to 7 ("Strongly Agree"). Pre-testing involved 10 subject matter experts and 15 professionals from the target population to assess the clarity and relevance of the items. The final instrument demonstrated strong content validity and internal consistency, confirmed through Cronbach's alpha and confirmatory factor analysis.

FINDINGS

1. Measurement model analysis

In the two-stage structural equation modeling (SEM) procedure, both the measurement model and the structural model were evaluated. The analysis was conducted using SmartPLS version 4 (Ringle et al., 2024; Khalifa et al., 2025; Zaki & Elnagar, 2025). To assess the reliability and convergent validity of the constructs in the measurement model, several criteria were examined, including factor loadings, Cronbach's alpha (α), composite reliability (CR), and average variance extracted (AVE). As recommended by Hair et al. (2019) and Iriqat et al. (2025), all Cronbach's alpha (α) and CR values exceeded the threshold of 0.70, indicating satisfactory internal consistency reliability. Additionally, factor loadings for all items were above the acceptable level of 0.70, and all AVE values were greater than the recommended minimum of 0.50, confirming convergent validity. Therefore, the constructs used in the study demonstrated strong reliability and convergent validity, justifying their inclusion in the structural model (Table 1).

Table 1. Construct reliability and validity (Notes: All factor loadings were standardized and were significant at the 0.001 level; AVE = average variance extracted; CR = composite reliability; α = Cronbach's alpha)

Latent Variable	Items	Factor Loading	α , CR, AVE
Connectivity (CONN)	CONN1: As Compared to rivals within our industry, our organization has the foremost available analytics systems.	0.927	0.959, 0.970, 0.891
	CONN2: All remote, branch, and mobile office are connected to the central office for analytics.	0.954	
	CONN3: Our organization utilizes open system network mechanisms to boost analytics connectivity.	0.946	
	CONN4: There are no identifiable communication bottlenecks within our organization when sharing analytics insights.	0.948	
Computability (COM)	COM1: Software applications can be easily transported and used across multiple analytics platforms.	0.957	0.957, 0.969, 0.886
	COM2: Our user interfaces provide transparent access to all platforms and applications.	0.927	
	COM3: Analytics-driven information is shared seamlessly across our organization, regardless of the location.	0.934	
	COM4: Our organization provides multiple analytics interfaces or entry points for external lend users.	0.946	
Modularity (MOD)	MOD1: Reusable software modules are widely used in new analytics model development.	0.952	0.955, 0.967, 0.880
	MOD2: End-users utilize object-oriented tools to create their own analytics applications.	0.937	
	MOD3: Object-oriented technologies are utilized to minimize the development time for new analytics applications.	0.941	
	MOD4: Applications can be adapted to meet a variety of needs during analytics tasks.	0.922	
Technology Knowledge (TK)	TK1: Our analytics personnel are very capable in terms of programming skills.	0.940	0.938, 0.956, 0.844
	TK2: Our analytics personnel are very capable in terms of managing project lifecycles.	0.919	
	TK3: Our analytics personnel are very capable in the areas of data and network management and maintenance.	0.915	
	TK4: Our analytics personnel create very capable decision support systems driven by analytics.	0.901	
Technology Management Knowledge (TMK)	TMK1: Our analytics personnel show superior understanding of technological trends.	0.923	0.931, 0.951, 0.828
	TMK2: Our analytics personnel show superior ability to learn new technologies.	0.922	
	TMK3: Our analytics personnel are very knowledgeable about the critical factors for the success of our organization.	0.893	
	TMK4: We are very knowledgeable about the role of BDA as a means, not an end.	0.901	
Business Knowledge (BK)	BK1: Our analytics personnel understand our organization's policies and plans at a very high level.	0.938	0.946, 0.961, 0.861
	BK2: We are very capable in interpreting business problems and developing proper technical solutions.	0.925	
	BK3: Our analytics personnel are very knowledgeable about business functions.	0.919	
	BK4: Our analytics personnel are very knowledgeable about the business environment.	0.930	
Cooperativeness (COOP)	COOP1: Managers empower their staff.	0.899	0.971, 0.975, 0.832
	COOP2: Managers treat all staff as their big family members.	0.907	
	COOP3: Employees are loyal and trust one another.	0.931	
	COOP4: Your company encourages employees to actively participate all company activities and events.	0.917	
	COOP5: Employees are devoted to protecting their organization.	0.939	
	COOP6: Employees are trusted by their managers and can participate in the decision-making process.	0.902	
	COOP7: It is very harmonious amongst employees, and your company is treated like a big family.	0.894	
	COOP8: Your company pays attention to human resource development, employees' morale, and teamwork.	0.906	
Innovativeness (INN)	INN1: Managers have courage to make innovation and take risk.	0.912	0.961, 0.968, 0.836
	INN2: Managers actively lead the staff to grow and innovate.	0.909	
	INN3: Managers have vision and insights to create new business opportunities.	0.914	
	INN4: Employees always must face challenges, and they can learn and grow from the challenges.	0.917	
	INN5: Your company pays attention to the uniqueness of employees and encourages the innovation from employees.	0.913	
	INN6: Your company is willing to take risks, and it is indeed an ambitious and energetic organization.	0.922	
Consistency (CONS)	CONS1: Managers set up clear goals and demand employees to carry out the goals strictly.	0.910	0.965, 0.972, 0.852
	CONS2: Your company always has formal and strict rules for employees to follow.	0.912	
	CONS3: The operation of your company emphasizes stability and conservative culture. It does not allow any confusion.	0.922	
	CONS4: Your company pays attention to efficiency and performance for achieving the goals.	0.917	
	CONS5: Your company is stable and offers job security to employees.	0.945	
	CONS6: Your company is a systematic organization where each employee has clear duty, and its operations are well defined with clear rules to follow.	0.930	
Effectiveness (EFF)	EFF1: Managers emphasize working efficiency and acts effectively.	0.918	0.970, 0.976, 0.869
	EFF2: Managers pay attention to achieve good work performance and reach the goal, regardless of personal feelings.	0.948	
	EFF3: The critical success factor of your company is its good productivity.	0.938	
	EFF4: Your company pays attention to work efficiency. Every department and employee must compete with its peer for better efficiency.	0.926	
	EFF5: Your company pays attention to maintaining its competition advantages.	0.924	
	EFF6: Your company pays attention to employees in terms of increasing their efficiency and pursuing their accomplishment.	0.939	

Confidentiality (CONF)	CONF1: Your company enforces security controls (such as the cryptographic system) to protect sensitive information and proprietary/business secrets.	0.935	0.966, 0.973, 0.879
	CONF2: Unauthorized employees are prohibited from accessing company's information resources.	0.919	
	CONF3: Employees must follow company policy and regulations when releasing or transmitting information.	0.950	
	CONF4: Your company has well implemented security practices to protect important information from stolen by malicious intrusions (such as break-in, Trojans, and spy-wares).	0.951	
	CONF5: Information security measures are implemented in your company to prevent sensitive information from unauthorized disclosure.	0.934	
Integrity (INT)	INT1: Your company constantly updates information resources and regularly creates information backups.	0.930	0.966, 0.974, 0.881
	INT2: Your company regularly conducts risk assessment and updates security plans to reduce the probability of loss of information.	0.931	
	INT3: When acquiring important information from the information sources or business partners, employees will store it into the company's database.	0.956	
	INT4: Your company has security controls (such as change management procedures) in place to prevent unauthorized information changes (creation, alternation, and deletion).	0.929	
	INT5: The database is periodically reconciled and regularly maintained in your company to increase the accuracy and reliability of information.	0.948	
Availability (AVA)	AVA1: Your company pays attention to lower down the probability of information system breakdown and information service disruption.	0.922	0.924, 0.952, 0.868
	AVA2: There are well established information access control procedures in your company, to make sure that for any information resource only authenticated users with right privileges can access such resource.	0.947	
	AVA3: A legitimate user with business needs can access company information at any time and at anyplace.	0.926	

A discriminant validity investigation was conducted using both the Fornell-Larcker criterion and the heterotrait-monotrait ratio (HTMT). According to Fornell & Larcker (1981), discriminant validity is established when the square root of each construct's AVE is greater than its correlations with other constructs. The results supported this condition, as all diagonal values (square roots of AVEs) exceeded the inter-construct correlations. Additionally, HTMT values for all construct pairs were found to be below the conservative threshold of 0.85 (Elnagar et al., 2026; Henseler et al., 2015; Khalifa et al., 2025), further confirming the distinctiveness of the constructs. Together, (Table 2) these findings demonstrate that discriminant validity was adequately established in the measurement model.

Table 2. Discriminant validity

HTMT	1	2	3	4	5	6	7	8	9	10	11	12	13
Availability													
Business Knowledge	0.787												
Computability	0.844	0.755											
Connectivity	0.782	0.780	0.804										
Confidentiality	0.887	0.803	0.807	0.741									
Consistency	0.865	0.802	0.788	0.796	0.798								
Cooperativeness	0.747	0.724	0.743	0.797	0.745	0.763							
Effectiveness	0.821	0.826	0.753	0.784	0.799	0.784	0.750						
Innovativeness	0.809	0.820	0.777	0.791	0.802	0.771	0.762	0.799					
Integrity	0.862	0.802	0.845	0.755	0.845	0.773	0.660	0.791	0.754				
Modularity	0.823	0.778	0.826	0.830	0.815	0.760	0.753	0.829	0.785	0.788			
Technology Knowledge	0.815	0.776	0.809	0.821	0.804	0.771	0.709	0.749	0.768	0.819	0.766		
Technology Management Knowledge	0.807	0.782	0.812	0.761	0.802	0.783	0.771	0.768	0.746	0.781	0.762	0.829	
Fornell-Larcker	1	2	3	4	5	6	7	8	9	10	11	12	13
Availability	0.932												
Business Knowledge	0.736	0.928											
Computability	0.793	0.720	0.941										
Connectivity	0.736	0.744	0.770	0.944									
Confidentiality	0.838	0.769	0.776	0.714	0.938								
Consistency	0.817	0.766	0.758	0.766	0.771	0.923							
Cooperativeness	0.708	0.695	0.716	0.769	0.722	0.739	0.912						
Effectiveness	0.777	0.791	0.726	0.757	0.773	0.759	0.729	0.932					
Innovativeness	0.763	0.782	0.745	0.760	0.773	0.743	0.736	0.771	0.915				
Integrity	0.815	0.768	0.813	0.727	0.817	0.747	0.640	0.766	0.727	0.939			
Modularity	0.773	0.740	0.790	0.795	0.782	0.729	0.725	0.798	0.752	0.758	0.938		
Technology Knowledge	0.759	0.732	0.767	0.779	0.766	0.734	0.677	0.715	0.730	0.780	0.726	0.919	
Technology Management Knowledge	0.748	0.735	0.767	0.719	0.762	0.742	0.733	0.730	0.706	0.741	0.719	0.775	0.910

2. Structural Model Analysis

The structural model was assessed using Partial Least Squares Structural Equation Modeling (PLS-SEM) in SmartPLS. The model's explanatory power was evaluated using the R-squared (R²) value. The results revealed a substantial amount of variance explained in both the endogenous constructs, with CCDS (R² = 0.834) and OC (R² = 0.828). These values indicate that the model explains 83.4% of the variance in CCDS and 82.8% in OC, which are considered high according to thresholds suggested by Elnagar et al. (2025) and Hair et al. (2019). Figure 2 and Table 3 present the results of the direct path relationships. All

hypothesized paths or direct effects (H1 to H5) were statistically significant at 1% level of significance, indicating strong support for the proposed relationships. Specifically, BDPC had the most substantial direct effect on OC ($\beta = 0.659, t = 16.163, p < .001$), followed by BDPC on cloud computing data security (CCDS) ($\beta = 0.449, t = 6.053, p < .001$). Hence, although five straightforward hypotheses were accepted but two (H3 and H4) were strongly influenced. Two mediation analyses were conducted to examine whether organizational culture mediates the relationship between independent and dependent constructs.

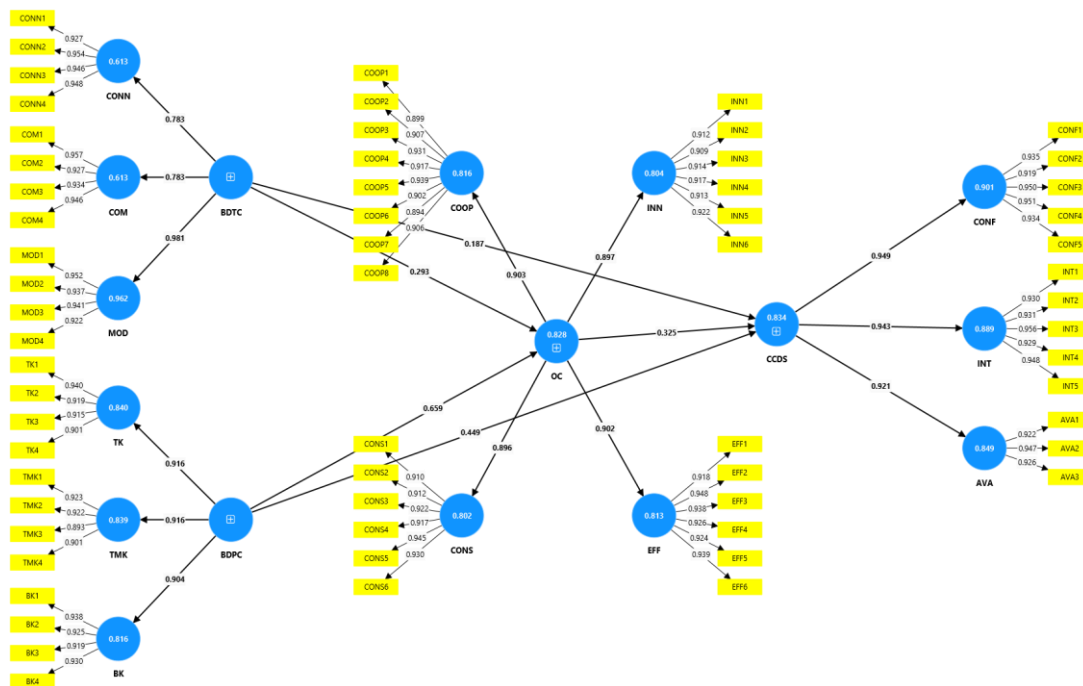


Figure 2. Measurement model diagram (Notes: Big Data Technological Capabilities (BDTC), Big Data Personal Capabilities (BDPC) Organizational Culture (OC), Cloud Computing Data Security (CCDS), Availability (AVA), Business Knowledge (BK), Computability (COM), Connectivity (CONN), Confidentiality (CONF), Consistency (CONS), Cooperativeness (COOP), Effectiveness (EFF), Innovativeness (INN), Integrity (INT), Modularity (MOD), Technology Knowledge (TK), Technology Management Knowledge (TMK))

As shown in Figure 2 and Table 3, both indirect effects were significant at $p < .001$, confirming the mediating role of OC in the relationships between BDTC and CCDS (H6a) and BDPC and CCDS (H6b).

Table 3. Results of the structural model

Direct paths	Beta	T statistics	P values	Supported?
H1. BDTC -> OC	0.293	6.869	0.000	Yes
H2. BDTC -> CCDS	0.187	3.784	0.000	Yes
H3. BDPC -> OC	0.659	16.163	0.000	Yes
H4. BDPC -> CCDS	0.449	6.053	0.000	Yes
H5. OC -> CCDS	0.325	3.934	0.000	Yes
Indirect paths				
H6a. BDTC -> OC -> CCDS	0.095	3.509	0.000	Yes
H6b. BDPC -> OC -> CCDS	0.214	3.740	0.000	Yes

DISCUSSION

The adoption of big data has become an emerging aspect of digital transformation in the hospitality and tourism sectors. In the twenty-first century, cloud technologies are ideal for enhancing management and customer expectations in the hospitality sector, as they can boost security, privacy, and management effectiveness (Busulwa et al., 2025; Wiboonrat, 2014). Our study aims to demonstrate the effect of big data personal and technological capabilities on OC and CCDS (H1, H2, H3, H4), as well as the effect of OC on CCDS (H5) in Egyptian hotels. The study formulates several hypotheses, which also include the OC as a mediator. The study supports all hypotheses, specifically the direct influence of BDC on OC and the mediating effect of OC on the relationship between BDC and CCDS (H6a, H6b).

The personal and technological capabilities of big data have a significant positive effect on OC in Egyptian hotels (H1, H3). Previous research has indicated that organizational preparedness and a competitive environment encourage the use of big data analytics, which in turn raises business profitability by strengthening the foundations of the hotel sector's reputation and performance (Carneiro et al., 2023; Yallop & Seraphin, 2020). BDPC is a cumulative factor of several personnel skills in multi-factor authentication, SIEM solutions, and role-sensitive access on cloud PMS, and the analysis of big data output by trained analysts to close vulnerabilities in IoT room controls (Bala & Gnanavel, 2025). Hotel IT administrators use BDPC to parameterize encryption algorithms (AES-256) and perform simulation tasks, which can also reduce the plausible rate of malware threats (Li & Zhang, 2025). On the other side, BDTC is deployed with ML-based algorithms in cloud computing to detect fraudulent activities in the CCTV footage, access logs, and booking system records in order to reduce the time (Ilha,

2022). The relationship between OC and big data capabilities in the travel and hospitality sector has not been explicitly stated in earlier studies. Our study fills this gap by suggesting that both big data personal and technological capabilities have a significant influence on OC. In the tourism industry, leveraging big data effectively is closely tied to revenue optimization. Hotel administrators can enhance decision-making processes within their organizations by utilizing big data analytics (Yallop & Seraphin, 2020). The culture within an organization plays a vital role in effectively leveraging big data analytics (Lunde et al., 2019b). Administrators need to promote a data-driven culture and integrate data to make informed decisions that enhance the organization's capabilities (Shamim et al., 2021). Prior studies indicated that the outcome of big data analytics within service-based sectors relies heavily on both technological and personal capabilities (Carneiro et al., 2023; Wamba et al., 2017). Notably, the findings show that the BDPC has the greatest influence on OC, which confirms that human capability plays a fundamental role in influencing the collective values and norm systems in data usage.

In this way, it can be argued that the analytical capability of employees plays a crucial role in promoting a data security culture in the cloud computing environment as a result of their data handling expertise and security knowledge. Contrary to expectations that suggested otherwise, our results show that BDPC makes a contribution towards the data security aspect of cloud computing indirectly through the promotion of a data security-oriented culture within organizations as a means of improving their business development and analysis capabilities. Research on the Malaysian hospitality sector has shown that data-driven skills and organizational culture in IT sector are crucial factors in enhancing BDAC (Aziz et al., 2024). These capabilities also affect hotels' ability to develop innovative features that enhance management and service.

BDTC and BDPC have a significant influence on CCDS in Egyptian hotels (H2, H4). Data management and ethics in the tourism sector suggest that for organizations to leverage data for a competitive edge, they must enhance regulatory frameworks to incorporate more robust privacy and ethical data solutions (Yallop & Seraphin, 2020). The potential for a revolutionary shift toward a new era of organizational design and industry-optimized decision-making is demonstrated by the broad applications of the Internet of Things in the hotel sector, alongside its interaction with big data (Nadkarni et al., 2019). Although big data can be considered advantageous for the hospitality and tourism sectors, it is associated with widespread ethical, privacy, and security issues. To effectively manage the tourism sector, it is essential to build and uphold customer trust while adhering to principles that strengthen the organization's reputation. Data security in cloud computing is crucial in this situation. Tourism and hospitality organizations must prioritize understanding consumer behavior while safeguarding privacy, ensuring that both goals are equally valued (Blakesley & Yallop, 2019; Yallop & Seraphin, 2020).

Our study demonstrates that OC has a significant influence on CCDS (H5). Security-conscious culture in an organization inspires its members to comply with security measures, practice safe data management, and stay cautious about cyber threats. In the hotel industry, where cloud technology is largely employed for operations such as customer reservations, data management, and payments, the role of employee behavior and awareness cannot be overlooked in offsetting potential cloud security threats associated with such technology. From a theoretical viewpoint, the result is supportive of socio-technical systems theory because it validates that the results of technology are contingent on the congruence of technology and social structures. It further validates the former studies on the scope of information security that organizational culture does shape the domain of security compliance, risk assessment, and decision-making. OC is identified as the enabling environment that converts cloud security tools and security policies into an immutable culture of CCDS.

Strong organizational cultures are more likely to get widespread support, while data-driven cultures facilitate the utilization of business analytics. A previous study focusing on information value chain theory demonstrated the significance of a data-driven culture as crucial for managing CCDS through business analytics (Wang et al., 2020). To enhance data security, earlier research has emphasized the importance of aligning data capabilities with an organization's values and standards (Sun et al., 2020; Yallop et al., 2023). Our study demonstrates that OC has a significant mediating effect on the relationship between both BDTC and personal capabilities and CCDS (H6a, H6b). A prior study revealed that the association between cloud computing data security decision-making and business analytics affordances is positively mediated by a data-driven culture and IT-based business integrity (Wang et al., 2020). Another survey of business firms found that the association between business performance and big data analytics capabilities is mediated by OC, indicating how culture can be leveraged to optimize technology outcomes (Upadhyay & Kumar, 2020). BDPC is stronger than BDTC via OC for some causal reasons. As human resource skills in data analysis and threat understanding cultivate cultural values such as sharing knowledge, it permeates hotel operations to incorporate security procedures. This is consistent with the idea of RBV Theory, where human capital complements physical capital in a dynamic hospitality environment (Horani et al., 2025). In Egyptian hotels, IT managers' BDPC-driven mediation by means of their competence is reflected in tailored cloud settings, such as dynamic IAM policies, outperforming purely technological implementations, where cultural acceptance is needed for their effectiveness. Empirical evidence suggests human factors account for extra additional variance in security achieved by innovative OC (Arshad et al., 2024; Orero-Blat et al., 2024).

Implications

1 Practical implications

Our study provides several important recommendations for hotel managers, IT managers and cybersecurity professionals in the Egyptian hospitality sector on how to strategically leverage BDA to strengthen CCDS. Firstly, we suggest that investments in big data analysis should be holistic, targeting both technical infrastructure and human capital. The findings indicate that although BDTC is important, BDPC has a greater impact on the design of safety-oriented OC. Therefore, hotel managers should not only allocate budgets to advanced analytics platforms and cloud security tools, but also prioritize the recruitment, training and retention of data-savvy personnel. Investing in continued skills development in areas such as computer programming, cloud security principles and business analytics ensures that the workforce has the expertise needed to

properly configure systems, accurately interpret security alerts and translate technical risks into actionable business terms (Gupta & George, 2016; Nadkarni et al., 2019). Second, our results underscore that OC is not a peripheral concern but the central mechanism for achieving robust security. Managers must actively cultivate a culture characterized by cooperativeness, innovativeness, consistency, and effectiveness to bridge the gap between technological potential and security outcomes.

This involves breaking down departmental silos to foster collaboration between IT, security, and operational teams, enabling rapid threat information sharing and coordinated incident response. Leaders should incentivize innovative uses of BDA for proactive threat hunting and reward consistent adherence to security protocols. By embedding these cultural values, managers can transform security from a mere IT function into a shared organizational responsibility, thereby strengthening the human firewall against cyber threats (Ernest Chang & Lin, 2007; Wang et al., 2020). Third, our study shows that cloud CCDS is a strategic outcome that can be achieved by aligning big data capabilities with a supportive culture. Therefore, hotel managers should integrate their BDA and cybersecurity strategies. This means that decisions regarding new analytics software or cloud services should be evaluated not only for their operational benefits, but also for their compatibility with the existing IT ecosystem and their potential to improve security monitoring (for example, through improved connectivity and modularity).

In addition, security objectives should be clearly communicated and woven into performance management systems to ensure that all employees, from front desk staff to management, understand their role in protecting guest data. Such strategic alignment ensures that investments in technology and people are directly aimed at mitigating cloud-related risks, protecting the hotel's reputation and ensuring compliance with evolving regulations such as Egypt's Personal Data Protection Law.

In conclusion, our study provides a clear actionable framework for practitioners: To build a resilient cloud security posture, Egyptian hotels need to invest strategically in both technology and people, and intentionally foster an OC that enables effective translation of these capabilities into concrete security performance.

2 Theoretical implications

The results of our study offer three primary implications for advancing management and information systems theory. First, this study significantly contributes to and extends the RBV (Barney, 1991) and the DCT (Iriqat et al., 2025; Teece et al., 1997) by integrating them with perspectives from information systems, human resource management, and organizational behavior. While the RBV posits that valuable and rare resources are the source of competitive advantage, our findings demonstrate that BDTC and BDPC represent such critical technological and human resources, respectively. We advance this view by showing that these resources alone are not sufficient; their true value in achieving superior security outcomes (CCDS) is unlocked through the mediating mechanism of OC. This aligns with and extends the DCT, which emphasizes a firm's ability to integrate, build, and reconfigure resources. Our study illustrates that OC is the fundamental dynamic capability that allows firms to absorb and effectively reconfigure their BDTC and BDPC to fortify their security posture in a rapidly evolving digital threat landscape (Lunde et al., 2019b; Shamim et al., 2021). Second, our research clarifies the important mediating role of OC in the relationship between technical/human resources and safety performance. Previous literature has often treated technology, people and culture in isolation or been vague about their interactions. Our findings definitively establish OC not as a mere precursor or mediator, but as the central mediating mechanism by which BDTC and BDPC are translated into robust CCDS. We propose that a culture characterized by collaboration, innovation, continuity and efficiency functions as the essential "social fabric" that determines whether technological tools and human expertise are fully utilized or underutilized (Wang et al., 2020). This provides a more nuanced understanding than direct effect models, which show how and why investments in big data analysis ultimately lead to increased data security. Third, we establish an important link between human capital and technology deployment in the cybersecurity sector. By decomposing big data capabilities into technical (BDTC) and personal (BDPC) dimensions, and demonstrating that BDPC had the strongest direct impact on shaping OC, our study emphasizes that human expertise is the primary engine for enabling a security-oriented culture.

This finding resonates with RBV's extension, the knowledge-based view (KBV), which emphasizes that employees' knowledge, skills and professional insight are the most strategic resources for dealing with complex security challenges. It is human capital that fosters an innovative and collaborative environment, ensuring that technological capabilities are effectively targeted to protect critical assets (Gupta & George, 2016; Nadkarni et al., 2019).

CONCLUSIONS

Limitations and scope for further research

While this study provides valuable insights, it is not without limitations, which also offer opportunities for future research. First, this research was conducted in the specific context of the Egyptian hotel sector, focusing on mid- and high-end hotels in key tourist areas. This geographic and region-specific focus may limit the generalizability of our findings to other countries with different technological infrastructure, regulatory environments, or cultural norms. Therefore, we recommend that future studies replicate and validate our conceptual model in other geographical settings, such as in other countries in the Middle East and North Africa (MENA), or in different sub-sectors of hospitality, such as restaurants or travel agencies, to increase the external validity of the findings. Second, our study focused on the mediating role of OC, but did not examine potential moderating variables that might strengthen or weaken the proposed relationships. Factors such as top management support, regulatory pressure or a hotel's technical preparedness can significantly influence how big data capabilities are translated into security results. We suggest that future research include these variables as moderators to provide a more nuanced understanding of the boundary conditions that influence the BDA-CCDS relationship. Third, the data for this study were collected at a single point in time using a cross-sectional design. While this allows investigation of relationships, it prevents definitive conclusions regarding causation. The dynamic nature of technology, cybersecurity threats, and OC suggests that

these relationships are evolving. Therefore, we suggest that future longitudinal studies be conducted to explore how the development of BDA abilities and changes in OC affect CCDS over time, thereby establishing stronger causal inferences. Finally, our data were collected from management perspectives (IT managers, department directors) within hotels.

Although these respondents are knowledgeable, their views may not fully illuminate challenges on the ground or safety culture as understood by non-executive staff. To provide a more holistic and balanced view of the organizational phenomenon under investigation, future research could adopt a multi-source data collection approach, collecting responses from both managers and operational staff. In addition, using objective measures of data security performance along with perceptual survey data can further strengthen the validity of the findings. To strengthen the transparency of this study, this research was potentially affected by gender bias and recommends that future research explore more insights to explore gender dominance or diversity in IT leadership as a significant moderator between BDAC, OC, and cloud security outcomes.

Author Contributions: Conceptualization, A.K.E, A.M.H, and O.M.A; methodology, M.M.S, S.A.B, and O.M.A; software, M.M.S, S.A.B, and O.M.A, validation, formal analysis, A.M.H, M.M.S., and O.M.A; investigation, A.K.E, A.M.H, and S.A.B; data curation, M.M.S, S.A.B, and O.M.A; writing - original draft preparation, A.K.E, A.M.H, and S.A.B; writing - review and editing, A.K.E, and A.M.H; visualization, A.K.E, A.M.H, O.M.A and S.A.B; supervision, A.M.H, A.K.E; project administration, A.K.E.; resources, M.M.S, S.A.B, and O.M.A; funding acquisition, A.M.H All authors have read and agreed to the published version of the manuscript.

Funding: Not applicable.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study may be obtained on request from the corresponding author.

Acknowledgements: The research undertaken was made possible by the equal scientific involvement of all the authors concerned.

Conflicts of Interest: The authors declare no conflict of interest.

REFERENCES

- Abdelhamied, F. (2024). Digital transformation in the Egyptian hotels: Benefits, drivers and challenges. *International Journal of Tourism and Hospitality Management*, 7(2), 275-298. <https://doi.org/10.21608/ijthm.2024.393775>
- Aboushouk, M., & Tamamm, M. (2023). Big Data in Egyptian Travel Agencies: Enabling Factors (TOE), Adoption Readiness and Adoption Intention. *Int. J. Tour. Archaeol. Hosp.* 3, 71-92. <https://doi.org/10.21608/ijtah.2023.178344.1020>
- Ahmadi, S. (2024). Systematic Literature review on cloud computing security Threats and mitigation Strategies. *SCIRP*. <https://doi.org/10.4236/jis.2024.152010>
- Ahmed, H. A. M., Zaki, K., Abdelghani, A. A. A., Abdelfadel, T. A., Abusalim, E., & Elnagar, A. K. (2025). Leveraging corporate social responsibility for sustainable performance: The mediating roles of green organizational culture and employee engagement under regulatory pressure. *Geoj. Tour. Geosites*, 62, 1950-1970. <https://doi.org/10.30892/gtg.62414-1580>
- Al-Ali, A. A., Singh, S. K., Al-Nahyan, M., & Sohal, A. S. (2017). Change management through leadership: the mediating role of organizational culture. *International Journal of Organizational Analysis*, 25(4), 723-739. <https://doi.org/10.1108/ijoa-01-2017-1117>
- Almasoudi, A., Bhatti, A. Q., Alluqmani, A. E., & Alotaibi, A. (2025). Investigation of enhancing heritage preservation utilizing heritage building information modeling (HBIM). *Journal of Umm Al-Qura University for Engineering and Architecture*, 16(2), 414-442. <https://doi.org/10.1007/s43995-025-00116-1>
- Almeida, J., Franco Junior, A., Battistelle, R. A. G., & Bezerra, B. S. (2024). Dynamic Capabilities: Unveiling Key Resources for Environmental Sustainability and Economic Sustainability, and Corporate Social Responsibility towards Sustainable Development Goals. *Resources* 13, 22. <https://doi.org/10.3390/resources13020022>
- Alsheikh, G. A. R. A., Halim, M. S. B. A., Alremawi, M. S. A. A., & Tambi, A. M. B. A. (2018). The Mediating Role of Organizational Culture on the Relationship between Employee Performance and Antecedents in the Hotel Sector. *Journal of Reviews on Global Economics*, 6, 489-497. <https://doi.org/10.6000/1929-7092.2017.06.49>
- Anwar, M., Khan, S. Z., & Shah, S. Z. A. (2018). Big Data Capabilities and Firm's Performance: A Mediating Role of Competitive Advantage. *J. Inf. Knowl. Manag.* 17, 1850045. <https://doi.org/10.1142/S0219649218500454>
- Arshad, M., Qadir, A., Ahmad, W., & Rafique, M. (2024). Enhancing organizational sustainable innovation performance through organizational readiness for big data analytics. *Humanities and Social Sciences Communications*, 11(1), 950. <https://doi.org/10.1057/s41599-024-03424-4>
- Arshad, M., Yu, C. K., Qadir, A., Ahmad, W., & Rafique, M. (2022). The impact of big data analytics on organizational sustainability: The influencing factors of autonomous research and development and absorptive capacity. *International Journal of Engineering Business Management*, 14. <https://doi.org/10.1177/18479790221141537>
- Aziz, N. A., Al Mamun, A., Reza, M. N. H., & Naznen, F. (2024). The impact of big data analytics on innovation capability and sustainability performance of hotels: evidence from an emerging economy. *J. Enterp. Inf. Manag.* 37, 1044-1068. <https://doi.org/10.1108/JEIM-07-2023-0354>
- Bala, R. G., & Gnanavel, S. (2025). BC2P-1305: enhanced data security in cloud computing network using blockchain based ChaCha20-Poly1305 cryptography. *Frontiers in Blockchain*, 8. <https://doi.org/10.3389/fbloc.2025.1636056>
- Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. *J. Manag.* 17, 99-120. <https://doi.org/10.1177/014920639101700108>
- Blakesley, I. R., & Yallop, A. C. (2019). What do you know about me? Digital privacy and online data sharing in the UK insurance sector. *J. Inf. Commun. Ethics Soc.* 18, 281-303. <https://doi.org/10.1108/JICES-04-2019-0046>
- Busulwa, R., Pathiranage, N. W., & Pickering, M. E. (2025). Integration of critical digital technologies into hospitality and tourism curricula: evidence from QS-ranked universities. *J. Hosp. Tour. Technol.* <https://doi.org/10.1108/JHTT-06-2024-0388>
- Carneiro, T., Picoto, W. N., & Pinto, I. (2023). Big Data Analytics and Firm Performance in the Hotel Sector. *Tour. Hosp.* 4, 244-256. <https://doi.org/10.3390/tourhosp4020015>

- Chen, L., Liu, H., Zhou, Z., Chen, M., & Chen, Y. (2022). IT-business alignment, big data analytics capability, and strategic decision-making: Moderating roles of event criticality and disruption of COVID-19. *Decision Support Systems*, *161*, 113745. <https://doi.org/10.1016/j.dss.2022.113745>
- Demir, M., Tajeddini, K., & Gamage, T. C. (2025). Big data analytical capabilities and tech-business model innovation: a moderated mediation model. *Journal of Hospitality and Tourism Technology*. <https://doi.org/10.1108/jhtt-12-2024-0852>
- Ebert, I., Wildhaber, I., & Adams-Prassl, J. (2021). Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy protection. *Big Data & Society*, *8*(1), 1-14. <https://doi.org/10.1177/205395172111013051>
- Elnagar, A., & Derbali, A. (2020). The importance of tourism contributions in Egyptian economy. *Int. J. Hosp. Tour. Stud.* *1*, 45–52. <https://doi.org/10.31559/IJHTS2020.1.1.5>
- Elnagar, A. K., Abdelkawi, A., Elshaer, I., & Salama, S. (2022). The Effect of Organizational Culture on Financial Performance: Based on Cameron and Quinn Model (CVF). *Manag. Econ. Res. J.* *4*, 38–53. <https://doi.org/10.48100/merj.2022.181>
- Elnagar, A. K., & Aljuwaiber, A. (2026). The nexus of green intellectual capital and sustainable performance: leadership commitment and knowledge sharing as influences. *J. Intellect.* 1–29. <https://doi.org/10.1108/JIC-09-2024-0290>
- Elnagar, A. K., Khalifa, G. S. A., Herzallah, A. M., Derbali, A. M., Elgabrony, S. A. A., & Iriqat, R. A. M. (2025). Exploring the Link between Self-Leadership and Innovative Work Behaviours in Luxury Hotels: Validating a Moderated Mediation Model. *Afr. J. Hosp. Tour. Leis.* https://www.ajhtl.com/uploads/7/1/6/3/7163688/article_7_14_1_63-73.pdf
- Elnagar, A. K., Zaki, K., Salama, W. M. E., & Suliman, M. A. (2026). Customer Incivility Spillover into Kitchen Staff Deviance and Withdrawal in Multigenerational Workplaces: The Moderating Function of Moral Disengagement. *Administrative Sciences*, *16*(6), 253. <https://doi.org/10.3390/admsci16060253>
- Ernest Chang, S., & Lin, C. (2007). Exploring organizational culture for information security management. *Ind. Manag. Data Syst.* *107*, 438–458. <https://doi.org/10.1108/02635570710734316>
- Faul, F., Erdfelder, E., Buchner, A., & Lang, A. G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behav. Res. Methods* *41*, 1149–1160. <https://doi.org/10.3758/BRM.41.4.1149>
- Fornell, C., & Larcker, D. F. (1981). Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics. *J. Mark. Res.* *18*, 382–388. <https://doi.org/10.1177/002224378101800313>
- Gómez-Talal, I., González-Serrano, L., Rojo-Álvarez, J. L., & Talón-Ballester, P. (2024). Avoiding food waste from restaurant tickets: a big data management tool. *J. Hosp. Tour. Technol.* *15*, 232–253. <https://doi.org/10.1108/JHTT-01-2023-0012>
- Gupta, M., & George, J. F. (2016). Toward the development of a big data analytics capability. *Inf. Manage.* *53*, 1049–1064. <https://doi.org/10.1016/j.im.2016.07.004>
- Hair, J. F., Black, W. C., Babin, B. Y., & Anderson, R. E. (2019). *Multivariate data analysis*, Eighth Edition. ed. Springer International Publishing, Cengage.
- Hair, J. R., Matthews, L. M., Matthews, R. L., & Sarstedt, M. (2017). PLS-SEM or CB-SEM: updated guidelines on which method to use. *Int. J. Multivar. Data Anal.* *1*, 107. <https://doi.org/10.1504/IJMDA.2017.087624>
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *J. Acad. Mark. Sci.* *43*, 115–135. <https://doi.org/10.1007/s11747-014-0403-8>
- Herman, G. V. (2009). *Omul și modificările antropice din Câmpia Someșului*. Editura Universității din Oradea.
- Herman, G. V., Dorina, C., Ilieș, Baias, Ș., Măduța, M., Ilieș, A., Wendt, J., & Josan, I. (2016). *The tourist map, scientific tool that supports the exploration of protected areas, Bihor County, Romania*. https://geosport.uroadea.ro/2016_1/2016_12_GSS_Herman_Ilies_16.04.02.013.pdf
- Herzallah, A. M., Iriqat, R. A. M., Hamed, M. H., Zaki, K., & Elnagar, A. K. (2025). Green synergy in hospitality: Unveiling the nexus between environmentally sustainable practices and hotel green performance. *Int. J. Hosp. Manag.* *131*, 104301. <https://doi.org/10.1016/j.ijhm.2025.104301>
- Horani, O. M., Al-Adwan, A. S., Al-Rahmi, W. M., & Alkhalifah, A. (2025). Enabling innovation with big data analytics capabilities: the moderating role of organizational learning culture. *Data Science and Management*. <https://doi.org/10.1016/j.dsm.2025.06.006>
- Hornig, J., Liu, C., Chou, S., Yu, T., & Hu, D. (2022). Role of big data capabilities in enhancing competitive advantage and performance in the hospitality sector: Knowledge-based dynamic capabilities view. *Journal of Hospitality and Tourism Management*, *51*, 22–38. <https://doi.org/10.1016/j.jhtm.2022.02.026>
- Ilieș, A., Ilieș, D.C., Tătar, C., Ilieș, M. (2017). Geography of Tourism in Romania. In: Widawski, K., Wyrzykowski, J. (eds), *The Geography of Tourism of Central and Eastern European Countries*. Springer, Cham. https://doi.org/10.1007/978-3-319-42205-3_9
- Ilha. (2022). *Securing guest Data: The argument for Cloud-Based PMS*. International Luxury Hotel Association. <https://ilha.org/securing-guest-data-the-argument-for-cloud-based-pms/>
- Iriqat, R. A., Shkairat, R., Herzallah, A. M., & Elnagar, A. K. (2025). Enhancing corporate sustainability in SMEs through smart technologies: supply chain flexibility and agility as mediator. *Ind. Manag. Data Syst.* <https://doi.org/10.1108/IMDS-10-2024-1000>
- Jiang, Y., Ritchie, B. W., & Verreynne, M. (2019). Building tourism organizational resilience to crises and disasters: A dynamic capabilities view. *Int. J. Tour. Res.* *21*, 882–900. <https://doi.org/10.1002/jtr.2312>
- Khalifa Gamal, S. A., Derbali, A. M. S., Herzallah, A. M., Elshaer, A. M., & Elnagar, A. K. (2025). Greening Strategies: Interweaving Strategic Vigilance, Digital Transformation, and Corporate Strategic Foresight for Green Innovative Performance. *Int. J. Hosp. Tour. Adm.* 1–36. <https://doi.org/10.1080/15256480.2025.2539723>
- Khalifa Gamal, S. A., Elshaer, A. M., Hussain, K., & Elnagar, A. K. (2025). What drives customers' participation behaviour? Unveiling the drivers of affective satisfaction and its impacts in the restaurant industry. *J. Hosp. Tour. Insights* *8*, 612–636. <https://doi.org/10.1108/JHTI-01-2024-0100>
- Lee, M., Cai, Y. (Maggie), DeFranco, A., & Lee, J. (2020). Exploring influential factors affecting guest satisfaction: Big data and business analytics in consumer-generated reviews. *J. Hosp. Tour. Technol.* *11*, 137–153. <https://doi.org/10.1108/JHTT-07-2018-0054>
- Leso, B. H., Cortimiglia, M. N., & Ghezzi, A. (2022). The contribution of organizational culture, structure, and leadership factors in the digital transformation of SMEs: a mixed-methods approach. *Cognition Technology & Work*, *25*(1), 151–179. <https://doi.org/10.1007/s10111-022-00714-2>
- Li, P., & Zhang, L. (2025). Application of big data technology in enterprise information security management. *Scientific Reports*, *15*(1), 1022. <https://doi.org/10.1038/s41598-025-85403-6>
- Liu, C., Hornig, J., Chou, S., Yu, T., Huang, Y., & Lin, J. (2022). Integrating big data and marketing concepts into tourism, hospitality operations and strategy development. *Quality & Quantity*, *57*(2), 1905–1922. <https://doi.org/10.1007/s11135-022-01426-5>
- Lunde, T. Å., Sjusdal, A. P., & Pappas, I. O. (2019). Organizational Culture Challenges of Adopting Big Data: A Systematic Literature Review, in: Pappas, I.O., Mikalef, P., Dwivedi, Y.K., Jaccheri, L., Krogstie, J., Mäntymäki, M. (Eds.), *Digital Transformation for a Sustainable Society in the 21st Century*, Lecture Notes in Computer Science. Springer International Publishing, Cham, 164–176. https://doi.org/10.1007/978-3-030-29374-1_14

- Lyu, J., Khan, A., Bibi, S., Chan, J. H., & Qi, X. (2022). Big data in action: An overview of big data studies in tourism and hospitality literature. *Journal of Hospitality and Tourism Management*, 51, 346–360. <https://doi.org/10.1016/j.jhtm.2022.03.014>
- Makhloufi, L., Vasa, L., Rosak-Szyrocka, J., & Djermani, F. (2023). Understanding the impact of big data analytics and knowledge management on green innovation practices and organizational performance: the moderating effect of government support. *Sustainability*, 15(11), 8456. <https://doi.org/10.3390/su15118456>
- Mosqueda, J. (2023). *Perceptions and knowledge of Information Security Policy compliance in Organizational Personnel - ProQuest*. <https://www.proquest.com/openview/4de5271690e7e75bbcf7c62d26ed0c51/1?pq-origsite=gscholar&cbl=18750&diss=y>
- Nadkarni, S., Kriechbaumer, F., Rothenberger, M., & Christodoulidou, N. (2019). The path to the Hotel of Things: Internet of Things and Big Data converging in hospitality. *J. Hosp. Tour. Technol.* 11, 93–107. <https://doi.org/10.1108/JHTT-12-2018-0120>
- Naz, S., Haider, S. A., Khan, S., Nisar, Q. A., & Shehnaaz Tehseen. (2023). Augmenting hotel performance in Malaysia through big data analytics capability and artificial intelligence capability. *Journal of Hospitality and Tourism Insights*, 7(4), 2055–2080. <https://doi.org/10.1108/jhti-01-2023-0017>
- Nche, G. C., Ugwueze, M. I., & Ugwu, C. I. (2022). “As the Israelites in the Land of Egypt, So are We in Nigeria”: The Significance of the Exodus Event for Biafra Secessionist Movement. *Journal of Church and State*, 65(1), 1–24. <https://doi.org/10.1093/jcs/csac023>
- Noby, O., Rady, A., & Eljalil, S. A. (2021). Big Data Analytics’ Utilization in Egyptian Hotels’ Decision-Making. What are The Challenges of Applying BDA? *Journal of Association of Arab Universities for Tourism and Hospitality*, 0(0), 0. <https://doi.org/10.21608/jaauth.2021.106301.1265>
- Noby, O., Rady, A., & Gaber Abd Eljalil, S. (2022). The influence of big data analytics on hotel performance efficiency in Egyptian hotels. 567–535, 11. *مجلة كلية السياحة والفنادق جامعة المنصورة*. <https://doi.org/10.21608/mkaf.2022.253846>
- Nosrati, S., Altinay, L., & Darvishmotevali, M. (2024). Multiple mediating effects in the association between hotels’ eco-label credibility and green WOM behavior. *J. Hosp. Mark. Manag.* 33, 917–942. <https://doi.org/10.1080/19368623.2024.2356524>
- Orero-Blat, M., Rodríguez, A. L. L., & Palacios-Marqués, D. (2024). The strategic advantage of innovative organizational culture: An exploratory analysis in digital transformation and big data analytics capabilities. *Journal of Management & Organization*, 31(2), 443–462. <https://doi.org/10.1017/jmo.2024.74>
- Popescu, O., Tache, A., & Petrișor, A. (2022). Methodology for Identifying Ecological Corridors: A Spatial Planning perspective. *Land*, 11(7), 1013. <https://doi.org/10.3390/land11071013>
- Pour, M. J., Abbasi, F., & Sohrabi, B. (2022). Toward a Maturity Model for Big Data Analytics: A Roadmap for Complex Data Processing. *International Journal of Information Technology & Decision Making*, 22(01), 377–419. <https://doi.org/10.1142/s0219622022500390>
- Rasool, M., Murtza, M. H., Rasheed, M. I., Leong, A. M. W., Okumus, F., & Bai, J. (2025). Information technology competency and supply chain performance: role of risk management orientation and supply chain agility. *J. Hosp. Tour. Technol.* 16, 158–173. <https://doi.org/10.1108/JHTT-08-2023-0240>
- Ringle, C. M., Wende, S., & Becker, J. M. (2024). SmartPLS 4 (Version 4).
- Shamim, S., Yang, Y., Zia, N. U., & Shah, M. H. (2021). Big data management capabilities in the hospitality sector: Service innovation and customer generated online quality ratings. *Comput. Hum. Behav.* 121, 106777. <https://doi.org/10.1016/j.chb.2021.106777>
- Song, Y., Yu, W., Jacobs, M. A., & Chavez, R. (2025). Pandemic-related inventory management practices and financial performance: exploring the roles of pandemic-related production uncertainty and big data analytics capability. *International Journal of Production Research*, 63(17), 6319–6338. <https://doi.org/10.1080/00207543.2025.2470990>
- Stephens, M. (2023). *Egyptian Hotel Association (EHA) program*. HSMIAI Global. <https://global.hsmia.org/event/egyptian-hotel-association-eha-program/>
- Sun, S., Hall, D. J., & Cegielski, C. G. (2020). Organizational intention to adopt big data in the B2B context: An integrated view. *Ind. Mark. Manag.* 86, 109–121. <https://doi.org/10.1016/j.indmarman.2019.09.003>
- Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strateg. Manag. J.* 18, 509–533. [https://doi.org/10.1002/\(SICI\)1097-0266\(199708\)18:7<509::AID-SMJ882>3.0.CO;2-Z](https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z)
- Topcu, I., Karpak, B., Ülengin, F., & Aktas, E. (2025). Big data analytics in supply chain management: uncovering emerging trends through a bibliometric network analysis and a systematic literature review. *Journal of Enterprise Information Management*, 1–34. <https://doi.org/10.1108/jeim-07-2024-0374>
- Upadhyay, P., & Kumar, A. (2020). The intermediating role of organizational culture and internal analytical knowledge between the capability of big data analytics and a firm’s performance. *Int. J. Inf. Manag.* 52, 102100. <https://doi.org/10.1016/j.ijinfomgt.2020.102100>
- Vesterinen, M., Mero, J., & Skippari, M. (2024). Big data analytics capability, marketing agility, and firm performance: a conceptual framework. *The Journal of Marketing Theory and Practice*, 33(2), 310–330. <https://doi.org/10.1080/10696679.2024.2322600>
- Wamba, S. F., Gunasekaran, A., Akter, S., Ren, S. J., Dubey, R., & Childe, S. J. (2017). Big data analytics and firm performance: Effects of dynamic capabilities. *J. Bus. Res.* 70, 356–365. <https://doi.org/10.1016/j.jbusres.2016.08.009>
- Wang, Z., Wang, N., Su, X., & Ge, S. (2020). An empirical study on business analytics affordances enhancing the management of cloud computing data security. *Int. J. Inf. Manag.* 50, 387–394. <https://doi.org/10.1016/j.ijinfomgt.2019.09.002>
- Wiboonrat, M. (2014). *Cloud computing in budget hotel management*, in: 2014 IEEE International Conference on Management of Innovation and Technology. Presented at the 2014 IEEE International Conference on Management of Innovation and Technology (ICMIT), IEEE, Singapore, Singapore, 327–332. <https://doi.org/10.1109/ICMIT.2014.6942447>
- Willie, M. M. (2023). The role of Organizational culture in Cybersecurity: Building a Security-First Culture. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4564291>
- Yallop, A., & Séraphin, H. (2020). Big data and analytics in tourism and hospitality: opportunities and risks. *J. Tour. Futur.* 6, 257–262. <https://doi.org/10.1108/JTF-10-2019-0108>
- Yallop, A. C., Gică, O. A., Moiescu, O. I., Coroș, M. M., & Séraphin, H. (2023). The digital traveller: implications for data ethics and data governance in tourism and hospitality. *J. Consum. Mark.* 40, 155–170. <https://doi.org/10.1108/JCM-12-2020-4278>
- Zaki, K., Abdelghani, A. A. A., Ahmed, H. A. M., Abdelfadel, T., Abusalim, E., Ahmed, K., Abuzaid, A. E., & Elnagar, A. K. (2025). Work decently: AI-driven marketing strategies for a competitive edge in tourism. *Res. J. Adv. Humanit.* 6, 1–18. <https://royalliteglobal.com/advanced-humanities/article/view/1970/894>
- Zaki, K., & Elnagar, A. K. (2025). Unpacking talent management: a moderated mediation analysis of team dynamics and competitive performance in luxury hotels. *Empl. Relat. Int. J.* 47, 48–77. <https://doi.org/10.1108/ER-02-2024-0114>
- Zizic, M. C., Mladineo, M., Gjeldum, N., & Celent, L. (2022). From Industry 4.0 towards Industry 5.0: A Review and Analysis of Paradigm Shift for the People, Organization and Technology. *Energies*, 15(14), 5221. <https://doi.org/10.3390/en15145221>