

IoT Security Maturity and Resilience in the Saudi Smart Tourism Ecosystem

Ali Abu Abid¹, Sultan Algarni²

Department of Information Technology, Prince Musaid bin Abdulrahman University, Saudi Arabia¹

Department of Information Systems-Faculty of Computing and Information Technology,
King Abdulaziz University, Jeddah 21589, Saudi Arabia²

Abstract—As Internet of Things (IoT) technologies become more deeply embedded in smart tourism, connected infrastructure has grown into a core operational dependency, and service continuity now needs to be treated as a complement to conventional security controls rather than an afterthought. This study evaluates IoT security maturity in the Saudi Smart Tourism Ecosystem (STE) through the Cyber Resilience Readiness Validation (CRRV) framework, drawing on data from 25 governmental and quasi-governmental organizations across eight resilience determinants and seven reported threat categories. The resulting readiness profile is uneven: Confidentiality ($M = 4.13$) and Privacy ($M = 4.08$) achieved the highest scores, while Availability was the weakest determinant overall ($M = 3.28$). This gap is especially notable given that DoS/DDoS attacks were the most frequently reported threat ($n = 13$), pointing to a mismatch between organizations' maturity in data protection and their readiness to keep services running through disruption. IoT Awareness showed the widest spread among the eight determinants ($SD = 1.05$), suggesting that workforce preparedness varies considerably across organizations. Physical-attack exposure was also reported ($n = 5$), underscoring the exposure of IoT assets deployed in remote, open-air, and publicly accessible tourism settings. Together, these results suggest that strong readiness in data-protection domains does not automatically translate into operational resilience, and that strengthening IoT security across large-scale smart tourism ecosystems will require closer attention to service availability, workforce preparedness, physical-layer protection, and continuity planning — alongside, not instead of, established cybersecurity controls.

Keywords—IoT security; cyber resilience; smart tourism; Saudi vision 2030; regulatory alignment; availability; threat taxonomy

I. INTRODUCTION

Vision 2030 has driven a rapid expansion of Internet of Things (IoT) adoption across Saudi Arabia's key service sectors, tourism, transportation, and smart infrastructure, among them [1-3]. Within Smart Tourism Ecosystems (STEs) specifically, IoT is the layer that ties physical assets to digital services: environmental sensors, smart facility controllers, biometric identity systems, mobile tourism platforms, e-visa verification, and real-time crowd management all depend on it [4,5]. As these systems become more tightly interconnected, the question of whether they remain available and functional when something goes wrong takes on growing importance [12, 13].

That requirement pushes the security objective past prevention alone. Conventional cybersecurity is built primarily around preventing, detecting, and mitigating threats through

encryption, authentication, access control, and network segmentation. Cyber resilience asks a related but larger question: can essential services keep operating, absorb disruption, and recover once preventive controls are bypassed or overwhelmed [6,8]? The distinction matters especially in large-scale IoT environments, where DoS/DDoS attacks, Man-in-the-Middle (MiTM) attacks, device failures, and other disruptions can directly affect services that depend on continuous connectivity. Resilience, in this sense, covers both protecting against threats and sustaining critical functions, and restoring normal operations once disruption has occurred [9,10].

Saudi Arabia already has a national cybersecurity governance structure in place, built around the National Cybersecurity Authority (NCA), its Essential Cybersecurity Controls (ECC), and related standards for IoT devices and interoperability [9,11], giving organizations that run connected public services a regulatory baseline to work from. While recent scholarship on the Saudi Smart Tourism Ecosystem (STE) has extensively examined macroeconomic integration and digital transformation drivers [7, 14], technical evaluations focusing specifically on IoT security maturity and operational availability remain limited. Existing cybersecurity studies predominantly concentrate on data protection, confidentiality compliance, and secure communication protocols, and are rarely evaluated against service continuity constraints under high-concurrency conditions. Unlike prior models that treat security as a static compliance check, the CRRV framework explicitly integrates availability and resilience metrics, allowing for a structured comparison between regulatory alignment and operational continuity. That leaves an open question: does maturity in regulated security domains carry over into comparable readiness for service continuity across the heterogeneous IoT environments that make up the Saudi Smart Tourism Ecosystem?

To investigate this gap empirically, the present study applies the Cyber Resilience Readiness Validation (CRRV) framework to data collected from 25 governmental and quasi-governmental organizations. CRRV organizes readiness around eight resilience determinants: Privacy, Confidentiality, Data Integrity, Access Control, Availability, Trust, Regulatory and Policy Alignment, and IoT Awareness, interpreted alongside seven reported threat categories [4,15-17]. Throughout the study, the term compliance-resilience gap describes the divergence between comparatively strong readiness in data-protection dimensions and weaker readiness in operational service continuity, particularly Availability. Rather than equating IoT

security with the mere presence of technical controls, CRRV offers a structured way of reading organizational readiness against the threat environment in which smart tourism services actually operate.

The main contributions of this study are as follows:

- A standards-anchored resilience assessment: CRRV is applied to examine organizational IoT security maturity across eight resilience determinants, read against national cybersecurity requirements, relevant IoT standards, and the reported threat environment of the Saudi STE.
- Identification of a compliance-resilience gap: the analysis asks whether strong readiness in regulated data-protection domains is matched by comparable readiness in service availability, with particular attention to how Availability relates to reported DoS/DDoS exposure.
- Attention to physical-layer exposure: the assessment extends beyond network-level threats to include reported physical risks facing IoT assets deployed in remote, open-air, and publicly accessible tourism settings.
- Policy and operational implications: by relating organizational readiness to regulatory requirements, reported threats, and deployment conditions, the study points to where service continuity, workforce preparedness, and physical protection warrant greater attention within the Saudi STE.

The remainder of the study proceeds as follows. Section II sets out the research design, the CRRV framework, the survey instrument, the sampling strategy, and the statistical procedures. Section III reports the empirical results and resilience readiness scores. Section IV discusses these findings in relation to regulatory alignment, operational resilience, human factors, physical-layer exposure, and the Saudi smart tourism context. Section V closes with the main implications, limitations, and directions for future research.

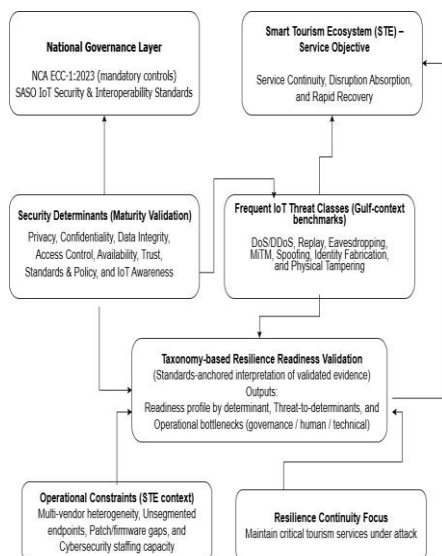


Fig. 1. Standards-anchored taxonomy for IoT cyber-resilience readiness validation in Saudi Smart Tourism Ecosystems (STE).

II. MATERIALS AND METHODS

A. Research Design and Positivist Framework

The study followed a quantitative, cross-sectional design to assess IoT security maturity and cyber-resilience readiness within the Saudi Smart Tourism Ecosystem (STE). Working within a positivist approach, we used the CRRV framework to organize eight security determinants: Privacy, Confidentiality, Data Integrity, Access Control, Availability, Trust, Regulatory and Policy Alignment, and IoT Awareness, and interpreted these alongside seven reported threat categories relevant to IoT environments in the Gulf region. CRRV is used here as an assessment structure, not as a claim that a new latent construct has been fully psychometrically validated.

B. Sampling Strategy and Organizational Profiles

The study was carried out within Saudi Arabia's governmental tourism sector, where IoT integration sits within the wider Vision 2030 digital transformation agenda. The sampling frame consisted of 80 governmental tourism organizations operating across the Kingdom, of which 25 returned valid responses, a response rate of 31.25%. The survey was directed at senior decision-makers and technical leads, so that responses would reflect organization-level assessments of security maturity and resilience readiness rather than individual opinion.

The sampling frame of 80 organizations was identified through national registries of entities executing Vision 2030 tourism and digital infrastructure mandates, encompassing regional development authorities, smart city management teams, and heritage site operators. While the final sample size of 25 organizations is numerically modest, it represents a specialized, organizational-level cohort. Gaining primary data from senior decision-makers concerning sensitive national cybersecurity infrastructure is inherently challenging. Given that the objective of this study is exploratory resilience assessment using the CRRV framework rather than predictive modeling, capturing 31.25% of the targeted governmental ecosystem provides a highly qualified, representative baseline.

- Target Population: The sampling frame consisted of 80 governmental tourism organizations operating across the Kingdom.
- Sample Size: 25 organizations returned valid responses, a response rate of 31.25%.
- Respondent Qualifications: Respondents were senior decision-makers and technical leads. Roughly 40% reported more than ten years of professional experience, 36% held managerial positions, and 24% held director-level roles. This seniority profile makes it more likely that responses reflect actual organizational policy and practice, though the data remain self-reported.

C. Instrument Development and Taxonomy Design

The instrument was designed to capture organizational maturity across several dimensions at once. As Fig. 1 shows, the eight resilience determinants make up the Shield component of the CRRV framework, and the seven reported threat categories provide the corresponding Stress context. The threat data serve

to interpret determinant-level readiness; they are not a formal experimental stress test, nor are they independently verified incident records.

1) *Defining resilience determinants*: The determinants listed in Table I were chosen for their relevance in the regional security literature and their bearing on service continuity in IoT environments. Organizational maturity on each determinant was assessed using a five-point Likert scale, giving a consistent basis for comparing readiness across participating organizations.

To ensure the robustness of the CRRV framework as an assessment structure, the eight resilience determinants and their corresponding survey items were developed through a structured three-phase process. First, the determinants were derived from a comprehensive review of IoT resilience literature and mapped directly to the mandatory controls of the Saudi National Cybersecurity Authority (NCA ECC-1:2018) and relevant SASO IoT standards. Second, individual survey items were adapted from established information security measurement scales and contextualized specifically for smart tourism IoT environments. Finally, to establish content validity, the initial item pool underwent an expert review by a panel of cybersecurity specialists and academic researchers. Based on their feedback, items were refined for technical accuracy and clarity. A preliminary pilot test was subsequently conducted with a small subset of IT professionals to confirm that the target audience correctly interpreted the terminology before finalizing the 24-item instrument.

TABLE I. DEFINITION AND SCOPING OF IoT RESILIENCE DETERMINANTS

Resilience Determinant	Operational Description	Measurement Focus (Items)
Privacy	The capacity to govern how personal visitor data are collected and shared.	Data minimization; consent management; privacy policies.
Confidentiality	Ensuring that sensitive telemetry and user data are accessible only to authorized entities.	Encryption at rest; secure transmission protocols.
Data Integrity	Safeguarding against unauthorized alteration of sensor data or command signals.	Hash functions; digital signatures; secure boot.
Access Control	Managing the identity and privileges of users and interconnected IoT nodes.	Multi-factor authentication; least-privilege access.
Availability	Maintaining the operational uptime of IoT infrastructure under stress.	AID redundancy; strict Service Level Agreements (SLAs) for uptime, response, and repair times.
Trust	The verified reliability of third-party IoT vendors and device hardware.	Confidence in IoT security measures; anticipated future engagement.
Regulatory & Policy Alignment	The organizational governance framework directing IoT security operations.	Internal standard development; clear IoT policies and regulations.
IoT Awareness	The cybersecurity maturity and risk literacy of the organizational workforce.	Staff training frequency; social-engineering resilience.

2) *National governance alignment and threat taxonomy*: To ground the assessment in the Saudi regulatory context, we cross-mapped the resilience determinants against the National Cybersecurity Authority's Essential Cybersecurity Controls (ECC-1:2018), shown in Table II. This cross-mapping was conducted iteratively. Initially, the authors aligned each determinant with the primary ECC sub-domains based on explicit control objectives. To mitigate subjective bias, this preliminary mapping was subsequently evaluated by an independent review panel comprising cybersecurity academics and industry practitioners familiar with Saudi regulatory compliance. Discrepancies regarding primary control alignments were resolved through a consensus-driven review process prior to finalizing the taxonomy, ensuring the standards-anchored aspect of the CRRV framework reflects established professional interpretation rather than subjective authorial judgment alone. This mapping gives a regulatory reference point for interpreting the readiness scores; it does not, on its own, establish that regulatory enforcement causes higher organizational maturity.

TABLE II. TAXONOMY OF IoT RESILIENCE PILLARS AND NCA CONTROL ALIGNMENT

Resilience Determinant	Frequency	Primary NCA Control Alignment (ECC-1:2018)	Description of Alignment
Privacy	15	2-11: Data and Information Protection	Focuses on classifying and protecting personal data according to Saudi laws and regulations.
Confidentiality	11	2-12: Cryptography	Mandates encryption to protect sensitive data in transit and at rest.
Data Integrity	9	2-11: Data and Information Protection	Addresses measures intended to prevent unauthorized alteration of data.
Access Control	7	2-3: Identity and Access Management	Defines least-privilege principles for access to IoT nodes and management interfaces.
Availability	7	2-13: Backup and Recovery Management	Supports redundancy and resilience against service disruptions.
Trust	5	2-1: Asset Management	Supports trusted asset inventories and authorized IoT device management.
Regulatory & Policy Alignment	4	1-1: Cybersecurity Governance	Requires an organizational framework for cybersecurity management.
IoT Awareness	4	1-2: Cybersecurity Risk Management	Addresses the human factor through training and awareness activities.

The study also draws on a taxonomy of seven threat categories, treated as contextual stressors within the Saudi STE. Their reported frequencies provide background for interpreting the resilience determinants in Section III; because the survey captured perceived or reported threat exposure, these counts are treated as reported frequencies rather than independently verified incident totals.

3) *Survey structure*: The finalized instrument, provided in full in Appendix A, comprised three modules:

a) *Organizational profile*: captured entity size, type, and current level of IoT experience.

- Resilience Determinants (24 items): measured the eight resilience dimensions, capturing technical, operational, and governance variables.
- Threat Vector Exposure (7 items): captured respondents' reported/perceived frequency and operational impact for each threat category, including DoS/DDoS and Man-in-the-Middle (MiTM) attacks.

This modular structure was chosen to support resilience assessment rather than descriptive security profiling on its own. Treating resilience as an organizational capability, rather than a checklist of controls, broadens what the instrument can capture. Accordingly, the eight resilience determinants are read together with the reported threat taxonomy to examine service continuity, disruption absorption, and recovery readiness across the participating public-sector Smart Tourism organizations.

D. Statistical Analysis and Reliability

All statistical procedures were conducted using SPSS version 25.0.

- Internal Consistency: Cronbach's alpha for the full instrument was $\alpha = 0.93$, indicating high overall internal consistency. Given that the instrument spans several theoretically distinct determinants, this figure is read as evidence of overall reliability rather than as proof that the instrument is unidimensional.
- Item Consistency: item-total correlations were positive and statistically significant across all 24 items, ranging from $r = 0.413$ ($p < 0.05$) to $r = 0.807$ ($p < 0.01$). These figures support item consistency within the instrument, but on their own they do not establish the full multidimensional construct validity of the CRRV framework.
- Analytical Procedures: readiness levels were summarized through frequencies, percentages, means, and standard deviations, and associations between Regulatory Alignment and the technical determinants were examined through correlation analysis, with significance set at $p < 0.05$.

Ethical standards were observed throughout data collection: participants were informed of the study's purpose before responding, and organizational identities were protected by anonymizing the dataset.

III. RESULTS

A. Socio-Demographic Profile of the Saudi STE

The CRRV framework was applied across 25 governmental and quasi-governmental organizations, 60% of whose respondents held managerial or director-level positions. The results are therefore best read as organization-level assessments provided by senior respondents, not as independently audited measures of cybersecurity performance.

B. Analysis of the IoT Threat Landscape (Stressors)

The reported threat environment provides context for interpreting the resilience determinant scores. Table III summarizes how frequently each of the seven threat categories was reported in the survey; these values are treated as reported exposure frequencies rather than independently verified incident counts.

TABLE III. REPORTED FREQUENCY OF IoT THREAT CATEGORIES IN THE SAUDI STE

Rank	Threat Vector	Reported Frequency (n)	Primary Impact Area
1	Denial of Service (DoS & DDoS) attack	13	Service Availability
2	Replay Attack	8	Data Integrity
3	Eavesdropping Attack	7	Data Confidentiality
4	Man-in-the-Middle (MiTM) Attack	7	Communication Trust
5	Spoofing Attack	6	Access Control
6	Sybil Attack	6	Network Trust
7	Physical Attacks	5	Hardware Integrity

DoS/DDoS was the most frequently reported threat category ($n = 13$), which makes service availability a particularly relevant dimension for interpreting the readiness scores. Physical-attack exposure was also reported ($n = 5$), indicating that device-level and environmental risks are part of the threat context these organizations face.

C. Empirical Readiness Scores of Resilience Determinants

Readiness was evaluated across the eight determinants on a five-point Likert scale, with five representing maximum readiness; Table IV reports the mean scores and standard deviations.

TABLE IV. MEAN READINESS SCORES OF IoT RESILIENCE DETERMINANTS

Resilience Determinant	Mean Score (M)	Std. Dev. (SD)	95% Confidence Interval
Confidentiality	4.13	0.69	[3.86, 4.40]
Privacy	4.08	0.82	[3.76, 4.40]
Access Control	3.96	0.69	[3.69, 4.23]
Data Integrity	3.92	0.81	[3.60, 4.24]
Trust	3.79	0.80	[3.48, 4.10]
Regulatory Alignment	3.65	0.98	[3.27, 4.03]
IoT Awareness	3.51	1.05	[3.10, 3.92]
Availability	3.28	0.91	[2.92, 3.64]

Confidentiality (M = 4.13) and Privacy (M = 4.08) recorded the highest readiness scores, while Availability recorded the lowest (M = 3.28). Given that DoS/DDoS was also the most frequently reported threat category (n = 13), this points to a mismatch between readiness in data-protection domains and readiness for service continuity. IoT Awareness showed the greatest variability of any determinant (SD = 1.05), indicating uneven workforce preparedness across organizations. To improve precision, Table IV reports 95% confidence intervals alongside mean scores and standard deviations. While these dimensions represent distinct theoretical constructs rather than repeated-measures conditions—meaning direct paired hypothesis tests across different determinants are methodologically constrained—the interval estimates illustrate the clear separation between the upper data-protection domains and the lower availability scores.

D. Reliability and Correlation Analysis

Overall internal consistency for the 24-item instrument was high (Cronbach's $\alpha = 0.93$). To examine the relationships between the eight resilience determinants, a bivariate correlation analysis was conducted. Because the determinant scores were calculated as continuous composite means rather than individual ordinal items, Pearson's correlation coefficient (r) was utilized. As detailed in Table V, the analysis identified multiple significant positive relationships across the framework. Notably, Regulatory Alignment (Standards & Policies) demonstrated strong correlations with IoT Awareness (r = 0.802, p < 0.01) and Data Integrity (r = 0.533, p < 0.01). These findings are interpreted as evidence of association rather than causation.

TABLE V. PEARSON CORRELATION MATRIX OF IoT RESILIENCE DETERMINANTS

Determinant	1	2	3	4	5	6	7	8
1. Privacy	1							
2. Confidentiality	0.439*	1						
3. Data Integrity	0.579**	0.635**	1					
4. Access Control	0.424*	0.612**	0.394	1				
5. Trust	0.484*	0.392	0.537**	0.478*	1			
6. Regulatory Alignment	0.592**	0.237	0.533**	0.284	0.704**	1		
7. IoT Awareness	0.641**	0.330	0.623**	0.218	0.632**	0.802**	1	
8. Availability	0.314	0.338	0.403*	0.407*	0.416*	0.523**	0.512**	1

* p < 0.05; ** p < 0.01

IV. DISCUSSION

The results point to an important asymmetry within the Saudi Smart Tourism Ecosystem: comparatively strong readiness in data-protection dimensions sits alongside weaker readiness in service availability. We interpret this pattern as a

compliance-resilience gap, while recognizing that the cross-sectional design cannot establish that regulation caused the differences observed.

A. The Regulatory Paradox: Compliance Vs. Resilience

Confidentiality (M = 4.13) and Privacy (M = 4.08) achieved the highest readiness scores of the eight determinants. This is consistent with the prominence given to data protection and cryptographic controls within the Saudi cybersecurity regulatory environment [18,19], though our design does not allow us to attribute these scores causally to NCA enforcement. We read the finding instead as an alignment: readiness is strongest precisely in the domains where policy emphasis is strongest.

Availability tells a different story. It recorded the lowest readiness score (M = 3.28), even though DoS/DDoS was the most frequently reported threat (n = 13). That divergence suggests that maturity in data protection does not automatically carry over into readiness to sustain service continuity under disruption. The distinction between satisfying defined security controls and actually maintaining operations under adverse conditions sits at the center of how we interpret these findings, and it echoes prior work on availability and resilience limitations in IoT and smart-city infrastructure [20,21]. It is important to note that this "compliance-resilience gap" is presented here as a descriptive interpretation of the ecosystem's overall readiness profile based on mean score variances. While these descriptive differences provide a valuable conceptual heuristic, formal statistical testing of within-organization variance across a larger sample is required to empirically validate this gap as a definitive structural finding.

Furthermore, it should be emphasized that juxtaposing the high frequency of reported DoS/DDoS exposure with the ecosystem's low Availability scores is a descriptive observation of the overarching threat context. This juxtaposition highlights a conceptual alignment of vulnerabilities, but it does not represent a statistically confirmed empirical association at the individual organizational level.

Several Structural Factors Could Plausibly Contribute to This Imbalance: Multi-vendor Device Heterogeneity, Insufficient Network Segmentation, Slow Patch and Firmware Update Cycles, and Limited Cybersecurity Workforce Capacity. We Treat These as Plausible Operational Constraints Rather than Causal Effects Demonstrated by the Survey Itself. Even so, the Findings Support Giving More Attention to Governance-led, Ecosystem-level Resilience in Which Service Continuity Is Treated as a Primary Objective Rather than a Secondary Concern.

B. The Human-Governance Gap

IoT Awareness showed the widest variability of any determinant we assessed (SD = 1.05). That pattern fits uneven workforce preparedness across organizations better than a uniform, sector-wide training deficit. In an interconnected ecosystem, this kind of variation can produce uneven defensive capacity even where technical controls are otherwise mature, a point consistent with prior research on the role of cybersecurity awareness and human factors [22,23].

The positive correlations between Regulatory Alignment and the technical determinants (r ≥ 0.413, p < 0.05) point to an

association between governance alignment and technical security maturity. Because the design is cross-sectional, these correlations should not be read as evidence that governance drives technical performance; rather, they motivate further investigation into how organizational governance, human preparedness, and technical resilience relate to one another [24].

C. Regional Specificity: the Physical Threat Factor

IoT security research tends to emphasize network and software threats more than physical-layer exposure. In this survey, physical-attack exposure was reported with a frequency of $n = 5$. That figure does not make physical threats the dominant resilience constraint, but it does show that they are a real part of the threat environment these organizations operate in.

IoT assets deployed at open-air heritage sites or remote desert locations- sensors, smart lighting, automated kiosks- operate under conditions quite different from controlled indoor settings, which makes physical tampering and environmental degradation genuine operational risks. These findings support building hardware protection and localized monitoring into resilience planning for geographically distributed smart-tourism infrastructure, alongside network and software controls [25].

D. Alignment with Vision 2030

Vision 2030's Substantial Emphasis on Tourism Growth and Regional Competitiveness [12, 13] Raises the Strategic Stakes for Reliable Digital Services, Mirroring Broader Economic Impact Projections for the Sector [14]. Smart Transport, Digital Visa Systems, and Automated Hospitality Infrastructure All Depend on Sustained Availability to Support Visitor-facing Operations, Which Gives the Relatively Low Availability Score ($M = 3.28$) Practical, Not Just Statistical, Relevance, Particularly during Peak-demand Periods When Reliable Digital Services Are a Core Part of Smart-destination Performance [26].

E. Study Scope and Limitations

These findings need to be read within the bounds of the study design. The sample is limited to 25 governmental and quasi-governmental organizations, and the assessments are self-reported and cross-sectional.

Because both the cybersecurity maturity scores and the threat exposure frequencies were collected simultaneously using a single instrument, the findings are inherently susceptible to common-method bias. Furthermore, while targeting senior decision-makers improves the operational relevance of the responses, reliance on self-reporting introduces the potential for social-desirability bias, wherein respondents may inadvertently inflate their organization's regulatory compliance or defensive posture. Consequently, these metrics represent perceived organizational readiness rather than independently audited technical capabilities.

Furthermore, the response rate of 31.25% introduces the potential for non-response bias. Organizations with lower cybersecurity maturity, or those lacking dedicated technical leadership, may have been less likely to participate. As a result, the readiness scores reported in this study—including the notably weak Availability determinant—may represent a conservative estimate, meaning the actual sector-wide

compliance-resilience gap could be more pronounced than captured here.

Additionally, while the bivariate correlations provide valuable insight into determinant relationships, formal adjustments for multiple comparisons (e.g., Bonferroni correction) were not applied. In the context of a small, exploratory organizational sample, such strict adjustments overly inflate Type II error rates. Consequently, the reported correlation significance levels should be interpreted with caution as exploratory associations rather than definitive hypothesis tests.

The analysis is therefore best understood as a context-specific organizational assessment rather than a sector-wide estimate of cybersecurity maturity. Likewise, the reported threat frequencies reflect survey-reported exposure and should not be read as independently verified incident counts. Cronbach's alpha and the item-total correlations provide evidence of reliability and item consistency, but they do not amount to full validation of the eight-dimensional CRRV structure; larger samples and stronger construct-validation procedures would be needed before broader psychometric claims could be made.

Finally, regarding psychometric evaluation, while the global internal consistency of the 24-item survey is high (Cronbach's $\alpha = 0.93$), the study's organizational sample size ($N = 25$) and the limited number of items per determinant (ranging from 2 to 4 items) preclude the calculation of stable, independent reliability coefficients at the subscale level. Complete item wordings are provided in Appendix A for absolute transparency, but the eight determinants should be interpreted as theoretically derived operational dimensions rather than psychometrically isolated subscales. Furthermore, given the small sample size, structural validation via full factor analysis was not statistically viable; instead, construct validity relies on rigorous theoretical mapping to national standards and expert content validation conducted prior to deployment. The analysis is therefore best understood as a context-specific organizational assessment, utilizing the CRRV framework as an exploratory readiness profiling structure rather than a fully psychometrically partitioned diagnostic scale.

V. CONCLUSION

This study applied the CRRV framework to assess IoT security maturity and resilience readiness across 25 governmental and quasi-governmental organizations operating within the Saudi Smart Tourism Ecosystem. Given the sample size and specific governmental focus, these findings are not intended to serve as a definitive, sector-wide baseline for the entire ecosystem. Rather, they provide an exploratory organizational profile of this public-sector cohort. Within this bound, a consistent descriptive pattern emerges: readiness is strongest in Confidentiality and Privacy, and comparatively weaker in Availability, despite frequent reported DoS/DDoS exposure.

First, Confidentiality ($M = 4.13$) and Privacy ($M = 4.08$) recorded the highest readiness scores, indicating comparatively strong maturity in data-protection domains, consistent with the emphasis these controls receive within the Saudi regulatory environment.

Second, Availability recorded the lowest readiness score ($M = 3.28$) even as DoS/DDoS remained the most frequently reported threat category ($n = 13$); this asymmetry between data-protection maturity and service-continuity readiness is the principal compliance-resilience gap this study identifies.

Third, physical-attack exposure was reported ($n = 5$), a reminder that cyber-physical resilience in smart tourism needs to account for device-level risks alongside network and software threats, particularly in geographically distributed, open-air, and publicly accessible tourism settings.

Based on these exploratory findings and the observed threat context, the following recommendations are offered as logical strategic considerations rather than direct empirical proofs:

- Ministry of Tourism and NCA: Future sector-specific cybersecurity guidance could consider placing additional emphasis on high-availability architectures, redundancy, and DDoS resilience for public-facing smart tourism infrastructure, addressing the observed gap between data protection and availability.
- Tourism Organizations: Compliance-oriented controls might be usefully complemented with continuity measures, failover capability, redundant gateways, and recovery planning, where operationally appropriate.
- Heritage Site Management: Given the contextual reporting of physical-attack exposure ($n = 5$) within the threat taxonomy, remote and publicly accessible deployments may benefit from exploring hardware protection and localized monitoring as part of broader, defense-in-depth planning.
- Workforce Development: The variation observed in IoT Awareness ($SD = 1.05$) supports moving toward more consistent workforce training, with content tailored to the operational risks specific to smart hospitality and tourism environments.

The study remains limited by its sample size, its governmental focus, and its cross-sectional design. The measures are self-reported and may carry response and non-response bias, and the threat frequencies reflect reported or perceived exposure rather than independently verified incidents. Future research should extend this analysis to larger samples, private-sector tourism and hospitality providers, independent incident data where feasible, and longitudinal designs capable of tracking how resilience changes over time.

Taken together, the findings suggest that maturity in data protection should not be treated as synonymous with operational resilience. For the Saudi Smart Tourism Ecosystem, strengthening service availability, workforce preparedness, and physical-layer protection alongside established cybersecurity controls offers a more complete foundation for resilience planning.

ACKNOWLEDGMENT

During manuscript preparation, the authors used Claude (Anthropic) for language editing and for reorganizing the framing of the introduction, abstract, and conclusion. All

suggested content was reviewed and edited by the authors, who take full responsibility for the final publication.

AUTHOR CONTRIBUTIONS

Conceptualization, A.A. and S.A.; Methodology, A.A.; Software, A.A. and S.A.; Validation, A.A.; Formal Analysis, S.A.; Investigation, A.A. and S.A.; Resources, S.A.; Data Curation, A.A. and S.A.; Writing—original Draft Preparation, A.A.; Writing—review and Editing, S.A.; Visualization, A.A.; Project Administration, A.A. All Authors Have Read and Agreed to the Published Version of the Manuscript.

FUNDING

This research received no external funding.

A. Institutional Review Board Statement

The study was conducted in accordance with the Declaration of Helsinki. An exemption from full ethical review was granted by the Institutional Research Ethics Committee, as the research methodology was restricted to the collection of non-sensitive, anonymized, organization-level operational assessments and did not involve the collection of personal, medical, or sensitive human-subject data.

B. Informed Consent Statement

Informed consent was obtained from all subjects involved in the study. Participants were briefed on the research objectives, the voluntary nature of their participation, and the measures taken to ensure the anonymity and confidentiality of their organizational data. No identifiable personal or entity-specific information is disclosed in this manuscript.

C. Data Availability Statement

The data presented in this study are available on request from the corresponding author. The data are not publicly available due to the sensitive nature of the cybersecurity maturity profiles and threat exposure data related to the participating governmental tourism organizations in the Kingdom of Saudi Arabia.

CONFLICTS OF INTEREST

The author declares no conflict of interest. The funders or participating organizations had no role in the design of the study; in the collection, analysis, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

ABBREVIATIONS

Abbreviation	Definition
CRRV	Cyber Resilience Readiness Validation
NCA	National Cybersecurity Authority
AI	Artificial Intelligence
STE	Smart Tourism Ecosystem
SASO	Saudi Standards, Metrology and Quality Organization
MiTM	Man-in-the-Middle
IoT	Internet of Things
ECC	Essential Cybersecurity Controls
DDoS	Distributed Denial of Service
DoS	Denial of Service

REFERENCES

- [1] M. Nematpour, M. Khodadadi, A. Azimi, and R. Mohammadkazemi, "IoT-driven smart solutions: transforming urban tourism destinations," *Journal of Hospitality and Tourism Insights*, 2025.
- [2] K. S. Lim, S. Y. Ooi, M. S. Sayeed, Y. J. Chew, and N. M. Ahmad, "Securing the Internet of Things: Systematic Insights into Architectures, Threats, and Defenses," *Electronics*, vol. 14, no. 20, p. 3972, 2025.
- [3] Communications, Space and Technology Commission (CST), Internet Penetration and Digital Indicators Report in Saudi Arabia, CST Knowledge Center, Riyadh, Saudi Arabia, 2025. Available: <https://www.cst.gov.sa/en/knowledge-center/reports> [Accessed: Aug. 18, 2025].
- [4] F. Abdullayeva, "Cyber resilience and cyber security issues of intelligent cloud computing systems," *Results in Control and Optimization*, vol. 12, p. 100268, 2023.
- [5] M. Malatji, A. L. Marnewick, and S. Von Solms, "Cybersecurity capabilities for critical infrastructure resilience," *Information & Computer Security*, vol. 30, no. 2, pp. 255-279, 2022.
- [6] P. Jeehyun, "Book Of Abstracts for 2024 International Conference on Resilient Systems," 5th International Conference on Resilient Systems (ICRS 2024), ETH Zurich, 2024.
- [7] A. T. Rosário and J. C. Dias, "Exploring the landscape of smart tourism: a systematic bibliometric review of the literature of the Internet of Things," *Administrative Sciences*, vol. 14, no. 2, p. 22, 2024.
- [8] H. Sebestyen, D. E. Popescu, and R. D. Zmaranda, "A literature review on security in the Internet of Things: Identifying and analysing critical categories," *Computers*, vol. 14, no. 2, p. 61, 2025.
- [9] National Cybersecurity Authority (NCA), "Policy and Standards," <https://nca.gov.sa/en>. Accessed: Dec. 04, 2023. [Online]. Available: <https://nca.gov.sa/en>
- [10] M. R. Tawffaq et al., "IoT Security in a Connected World: Analyzing Threats, Vulnerabilities, and Mitigation Strategies," 2024 36th Conference of Open Innovations Association (FRUCT), IEEE, 2024, pp. 626-638.
- [11] S. Mohanty, K. Cormican, and C. Dhanapathi, "Analysis of critical success factors to mitigate privacy risks in IoT Devices," *Procedia Computer Science*, vol. 196, pp. 191-198, 2022.
- [12] E. Y. M. Musa, "The impact of tourism in the Kingdom of Saudi Arabia on GDP, 2005-2017: An analytical approach," *Global Journal of Economics and Business*, vol. 10, no. 2, pp. 458-462, 2021.
- [13] B. E. Barakka, "Determinants of Tourism Competitiveness in Emerging Tourist Destinations in the Arab Region: The Case of Saudi Arabia," *International Journal of Hospitality & Tourism Studies*, vol. 2, no. 2, 2021.
- [14] World Travel and Tourism Council (WTTC), Saudi Arabia 2023 Annual Research: Economic Impact and GDP Contribution, WTTC Reports, London, UK, 2023. Available: <https://wtcc.org/> [Accessed: Dec. 04, 2023].
- [15] S. F. Ahmed et al., "Toward a secure 5G-enabled internet of things: A survey on requirements, privacy, security, challenges, and opportunities," *IEEE Access*, vol. 12, pp. 13125-13145, 2024.
- [16] M. Al-Shaer, K. AlShehhi, and S. Abdulla, "The Internet of Things (IoT) Forensic Investigation Process: A State-of-the-Art Review, Challenges and Future Directions," *Journal of Information Security and Cybercrimes Research*, vol. 6, no. 2, pp. 150-161, 2023.
- [17] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations," *Sensors*, vol. 23, no. 15, p. 6666, 2023.
- [18] N. N. Albogami, "Intelligent deep federated learning model for enhancing security in internet of things enabled edge computing environment," *Scientific Reports*, vol. 15, no. 1, p. 4041, 2025.
- [19] R. Parashar, A. Khan, and A. K. Neha, "A survey: The internet of things," *International Journal of Technical Research and Applications*, vol. 4, no. 3, pp. 251-257, 2020.
- [20] B. A. Alkhaleel, "Future Trends and Opportunities of Artificial Intelligence and Machine Learning in the Resilience of Interdependent Critical Infrastructure Networks in the Kingdom of Saudi Arabia," in *Proceedings of the International Conference on Sustainability: Developments and Innovations*, Springer, 2024, pp. 232-239.
- [21] R. Sharma and R. Arya, "Security threats and measures in the Internet of Things for smart city infrastructure: A state of art," *Transactions on Emerging Telecommunications Technologies*, vol. 34, no. 11, p. e4571, 2023.
- [22] M. Zwilling, G. Klien, D. Lesjak, L. Wiecheteck, F. Cetin, and H. N. Basim, "Cyber security awareness, knowledge and behavior: A comparative study," *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 82-97, 2022.
- [23] M. U. Shah, F. Iqbal, U. Rehman, and P. C. K. Hung, "A comparative assessment of human factors in cybersecurity: Implications for cyber governance," *IEEE Access*, vol. 11, pp. 87970-87984, 2023.
- [24] J. He, Y. He, J. Hu, and Y. Guo, "Intelligent Governance: The AI-Driven New Paradigm of Governmental Adaptive Governance," *Journal of US-China Public Administration*, vol. 22, no. 1, pp. 1-27, 2025.
- [25] Z. Yu, H. Gao, X. Cong, N. Wu, and H. H. Song, "A survey on cyber-physical systems security," *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 21670-21686, 2023.
- [26] U. Gretzel and C. Koo, "Smart tourism cities: a duality of place where technology supports the convergence of touristic and residential experiences," *Asia Pacific Journal of Tourism Research*, vol. 26, no. 4, pp. 352-364, 2021.

APPENDIX A. SURVEY TEMPLATE

A. Purpose

This study addresses the objective of investigating the factors and attacks affecting IoT security in the Saudi Governmental Tourism Sector.

Section A: Profile of Responding Employee

Please indicate your job role: ☐ CISO ☐ Director ☐ Manager ☐ Senior ☐ Other: _____

Please indicate your gender: ☐ Male ☐ Female

How many years have you been working for the organization? ☐ < 1 year ☐ 1–5 years ☐ 6–10 years ☐ > 10 years

Section B: Profile of Responding Organization

Please indicate the type of your organization: ☐ Ministry ☐ Authority ☐ Program ☐ Company

Number of employees: ☐ < 200 ☐ 200–500 ☐ > 500

Are you implementing the Internet of Things in your organization? ☐ Yes ☐ No

Do you have a special team or department to manage cybersecurity? ☐ Yes ☐ No

Do you have clear, announced standards and policies for cybersecurity? ☐ Yes ☐ No

Section C: Factors that affect IoT Security in Saudi Governmental Tourism Sector

Please indicate the degree to which the following factors applied in your organization to gain a result of IoT systems security (1 = Strongly Agree, 2 = Agree, 3 = Neutral, 4 = Disagree, 5 = Strongly Disagree) (Table VI).

TABLE VI. SURVEY TEMPLATE I

#	Statement	1	2	3	4	5
1	In our organization, we collect only the necessary data and avoid the unnecessary collection of personal information.					
2	In our organization, we provide clear and concise information about how personal data is collected, used, and shared.					
3	In our organization, we obtain explicit consent from users before collecting or using their personal data.					
4	In our organization, we have clear and comprehensive privacy policies that outline how personal data is collected, used, and shared.					
5	In our organization, we have a list that specifies which users or devices are allowed or denied access to specific resources.					
6	In our organization, we use data encryption mechanisms in such a way that only authorized parties can access them.					
7	In our organization, we verify users' identities before allowing access to sensitive data using biometric authentication or Two-factor authentication (2FA).					
8	In our organization, we validate the accuracy and completeness of the data before it is transmitted or stored.					
9	In our organization, we identify errors in the data and correct them to ensure that it is accurate and consistent.					
10	In our organization, we have audit trails to maintain a record of all actions taken on the data, including who accessed it, when, and for what purpose.					
11	In our organization, we use RAID techniques that store multiple copies of the data in different locations to ensure that it is not lost or corrupted due to hardware failures or other issues.					
12	In our organization, we have a network security system that monitors and controls incoming and outgoing traffic based on predetermined security rules.					
13	In our organization, we authorize users or devices to access specific resources with the ability to do certain actions.					
14	In our organization, we use software that detects and prevents unauthorized access attempts by monitoring network traffic for suspicious activity.					
15	In our organization, we trust the security measures taken in the IoT adoption.					
16	In our organization, we believe that the usage rate and employee engagement with IoT technology will increase in the future.					
17	In our organization, we have built our own standards to adopt IoT.					
18	In our organization, we have a clear IoT policy and regulations.					
19	In our organization, we regularly conduct awareness programs.					
20	In our organization, training that increases knowledge about IoT systems is available at a regular pace.					
21	In our organization, we have SLA that indicate the amount of time an IoT device is operational without any downtime or failure.					
22	In our organization, we have SLA that indicate how quickly an IoT system responds to user requests or commands.					
23	In our organization, we have SLA that indicate the average time between failures of an IoT device or system.					
24	In our organization, we have SLA that indicate the average time it takes to repair a failed IoT device or system.					

Section D: Attacks Targeting IoT Security in Saudi Governmental Tourism Sector

Please indicate the degree to which the following attacks have been experienced as a result of IoT system attacks (1 = Strongly Agree, 2 = Agree, 3 = Neutral, 4 = Disagree, 5 = Strongly Disagree) (Table VII).

TABLE VII. SURVEY TEMPLATE II

#	Challenge / Threat Vector	1	2	3	4	5
1	Our organization has experienced a Denial of Service attack					
2	Our organization have experienced Replay Attack					
3	Our organization have experienced Eavesdropping Attack					
4	Our organization have experienced Man-in-The-Middle (MiTM) Attack					
5	Our organization have experienced Spoofing Attack					
6	Our organization have experienced Sybil attack					
7	Our organization have experienced Physical attacks					