International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

Responsible Smart City Technologies: the Role of Security in Building Citizen Trust and Technology Acceptance

Smit

Abstract

The rise of cities is being driven by the integration of connected digital tools that aim to make city services better and life easier.. The broad use of these connected digital tools brings up worries about security, privacy and whether citizens will use services that rely on technology. This study looks at how feelings of security and trust shape how likely citizensre to use smart-city technologies. We gathered data by surveying 601 people and analysed that data with Partial Least Squares Structural Equation Modelling (PLS-SEM). The results give evidence for the model we proposed and show that both the real visible parts of security and the more subtle invisible parts of security matter a lot when citizens think about technology. Especially the links between trust and perceived security and between security and data privacy are strong inside the model we built. The results say that keeping citizen trust means that organisations and public bodies that run smart-city technologies must meet expectations, about security and privacy and must act openly and quickly when citizens raise concerns. In short how citizens feel is a piece of what makes smart-city projects succeed especially when the success of smart-city tools depends on public confidence on how safe people feel and on how willing people are to use technology-enabled city services.

Keywords: Smart cities; Perceived security; Citizen trust; Technology adoption; Data privacy; Intelligent technologies; PLS-SEM

1. INTRODUCTION

The urbanization of the populations and raise in the public services have accelerated the development of smart cities in India. Smart cities integrate Information and Communication Technologies (ICT), Internet of Things (IoT), data analytics, and intelligent infrastructure to improve urban services, resource management, sustainability, and citizens' quality of life (Chatterjee & Kar, 2017; Chatterjee, Kar, & Gupta, 2018). These technologies enable cities to provide interconnected and data-driven services across transportation, utilities, public safety, waste management, and digital governance. However, increasing dependence on connected technologies also creates concerns regarding security, privacy, and citizens' trust. These concerns are raised in karnataka because several cities in the state have adopted smart-city initiatives involving digitally enabled infrastructure and technology-based public services. Bengaluru and other Smart Cities Mission cities in Karnataka increasingly rely on IoT, digital platforms, intelligent transportation, urban monitoring, and data-driven decision-making. With implication of technology improved the service sector efficiency, their extensive collection and processing of citizen-related information can create concerns about unauthorized access, cyberattacks, data misuse, and privacy violations. Indian research has highlighted security and privacy as important considerations in citizens' adoption of technology-enabled smart-city services (Chatterjee et al., 2018; Kumar et al., 2022).

Security in a smart-city environment extends beyond technical protection against cyber threats. It also includes citizens' perception that their personal information, digital identities, location data, and interactions with urban services are adequately protected. Privacy concerns may emerge when citizens are uncertain about what data are collected, how they are used, and who can access them. Consequently, perceived security and privacy can influence citizens' confidence in both smart-city technologies and the institutions responsible for their implementation. Chatterjee and Kar (2017) found

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

that privacy, security, and trust are relevant to citizens' adoption of IT-enabled services in the context of Indian smart cities. Trust is therefore an important behavioural factor in smart-city technology usage. Citizens may be more willing to use technology-enabled urban services when they believe that the systems are secure, their information is protected, and the responsible organizations operate reliably. Evidence from Karnataka also demonstrates the importance of trust and transparency in technology-enabled public services. Hebbar and Kiran (2024), in their study of smart cities in Karnataka, examined factors including trust, transparency, information quality, and facilitating conditions in relation to citizens' intention to use mobile-government services. However, greater attention is required to understand the relationship between perceived security, privacy, trust, and the broader propensity to use smart-city technologies.

This ethical dimensions of intelligent has increasingly became important. Venumuddala, Prakash, and Chaudhuri (2024) highlighted issues such as trust, fairness, justice, and dignity in the governance of IoT interventions in Karnataka's smart cities. This indicates that successful smart-city development requires not only technological efficiency but also citizen confidence and responsible management of data and technology.For examining citizens' perceptions of security and trust in smart-city technologies and their influence on the propensity to use such technologies in Karnataka, India.

2. THEORETICAL BACKGROUND

2.1 Smart Cities, Components and Characteristics

Smart cities are a way to build and run cities. In cities ideas from Information and Communication Technologies, the Internet of Things, artificial intelligence, data analytics, cloud computing and connected infrastructure are used to make city services run better to keep the city clean and green and to give people a higher quality of life. In India smart-city projects are about using technology for transport, online government, waste cleanup, safety, utilities and overall city management. Smart-city projects only work well if people in the city join in if institutions can manage and if the public trusts the technology. Indian research has been looking more at the people side of smart-city projects. For example Chatterjee and Kar in 2017 studied how Indians use IT services in cities and found that people-focused factors are key, to making technology work. Similarly, Chatterjee, Kar and Gupta (2018) demonstrated that technological, organizational and citizen-related factors influence the adoption of IT-enabled services in proposed Indian smart cities. These studies indicate that smart-city development should not be viewed solely as an infrastructure or technology project; rather, citizens are important stakeholders whose perceptions and behaviour influence the success of smart-city initiatives.

Karnataka provides a relevant setting for examining these relationships because several cities in the state have been included in India's Smart Cities Mission. Smart-city initiatives in Karnataka incorporate IoT-enabled infrastructure, intelligent transportation, urban monitoring, digital public services and integrated systems for managing urban resources. Venumuddala, Prakash and Chaudhuri (2024) specifically examined smart-city IoT interventions in Karnataka and highlighted the importance of governance and ethical considerations in the implementation of connected urban infrastructure. Their work demonstrates that technology-enabled urban systems involve not only technical and operational issues but also questions of trust, accountability and responsible governance. Smart cities can therefore be understood through three interconnected dimensions: technological, human and institutional. The technological dimension includes ICT, IoT, artificial intelligence, sensors and data platforms; the human dimension includes citizens, users and other stakeholders; and the institutional dimension includes governments, policies, regulations and governance mechanisms. The interaction among these dimensions determines whether smart-city technologies are perceived as useful, secure, trustworthy and acceptable by citizens.

2.2 Citizen Trust in Smart-City Technologies

Trust refers to an individual's confidence that a technology, organization or institution will act reliably, securely and in accordance with expected responsibilities. In smart cities, trust may involve confidence in both the technological system and the government or organizations responsible for managing it. Trust has when citizens cannot directly evaluate the technical characteristics of a smart-city system. For example, citizens using a digital public service information is

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

encrypted or how it is stored. They must therefore rely partly on their perception that the responsible institution will protect their information and use it appropriately. Recent research also demonstrates the relationship between trust and data privacy in smart-city environments. A 2026 study of smart-city data sharing found that trust in government and firms' data management influences citizens' willingness to disclose information, while trust can also reduce the negative influence of privacy concerns. In Karnataka, trust is also relevant to citizen interaction with digital government services. Research on smart cities in Karnataka has examined trust and transparency alongside other factors influencing citizens' use of mobile-government services. This provides a basis for extending the discussion beyond m-government toward broader smart-city technologies.

2.3 Propensity to Use Smart-City Technologies

Propensity to use technology refers to an individual's willingness or intention to engage with technology-enabled services. In the present study, it represents citizens' willingness to use and continue using smart-city technologies when such services are available. Technology acceptance research generally suggests that behavioural intention users' perceptions of trust, risk and security. Indian smart-city research has similarly examined citizen behavioural intention toward smart mobility and other technology-enabled services. A 2024 study involving 509 residents of Indian smart cities found that significantly influenced attitudes and behavioural intentions toward smart-mobility services. However, smart-city technologies are not limited to services that citizens directly operate. Many intelligent infrastructure systems, such as traffic monitoring, environmental sensors and automated urban-management systems, operate in the background and affect citizens without requiring direct interaction. This distinction makes citizen perceptions of security, privacy and trust particularly important.

2.4 Conceptual Relationships and Hypothesis Development

The preceding literature,proposes that citizens' perceptions of security, privacy and risk influence trust for smart-city technologies, while these security subsequently influence their propensity to use such technologies.

The proposed framework is therefore structured around the following relationships:

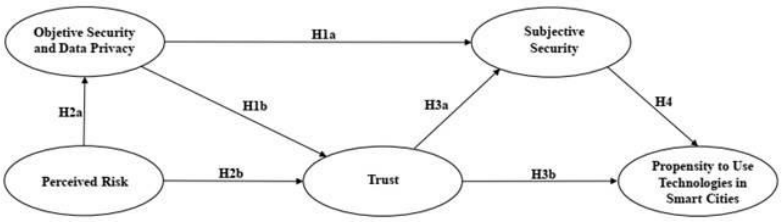
Perceived Security → Trust

Data Privacy → Trust

Perceived Risk → Trust

Trust → Propensity to Use Smart-City Technologies

Perceived Security → Propensity to Use Smart-City Technologies



The model adopts a citizen-centred perspective and positions trust as a key behavioural mechanism linking responsible technology characteristics with citizens' willingness to engage with smart-city technologies.

Accordingly, the study proposes the following hypotheses:

H1: Perceived security positively influences citizens' trust in smart-city technologies.

H2: Perceived data privacy positively influences citizens' trust in smart-city technologies.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

H3: Perceived risk negatively influences citizens' trust in smart-city technologies.

H4: Citizen trust positively influences the propensity to use smart-city technologies.

H5: Perceived security positively influences the propensity to use smart-city technologies.

H6: Citizen trust mediates the relationship between perceived security and the propensity to use smart-city technologies.

H7: Citizen trust mediates the relationship between perceived data privacy and the propensity to use smart-city technologies.

3. METHOD

3.1. Research Design and Sample Selection

The present study adopts an empirical, exploratory-descriptive research design using a quantitative, cross-sectional approach. The relationships among perceived security, data privacy, perceived risk, citizen trust, and propensity to use smart-city technologies.

A non-probability convenience sampling technique was used to collect responses from individuals who use smartphones, mobile applications, digital platforms, online payment systems or technology-enabled public services. Those respondents were chosen because familiarity with technologies enables them to give clear thoughts about security, privacy, risks and trust associated with smart-city technologies. The study looks at citizens in Karnataka people who live in urban and metropolitan areas where smart-city initiatives and technology-enabled public services are growing. Karnataka is a place because cities such as Bengaluru, Belagavi, Davanagere, Hubballi-Dharwad, Mangaluru, Shivamogga and Tumakuru are linked to smart-city projects and digitally enabled urban development. Including respondents from cities gives more variety in age digital experience and use of technology-enabled services. The target group was adult residents of Karnataka who know technologies and have used or seen technology-enabled urban services. Respondents were told that the study is academic and that participation is voluntary. The questionnaire was sent through a survey letting people, from different places answer.

3.2. Sample Size Determination

The required sample size was determined using G*Power 3.1.9 software, following the recommendations of Faul et al. (2009). For PLS-SEM, sample-size assessment considers the endogenous construct with the largest number of predictors in the proposed structural model. The analysis was based on commonly recommended parameters, including a statistical power of 0.80, a significance level of 0.05, and a medium effect size of 0.15, consistent with the recommendations of Cohen (1998). The model contains multiple predictors of the endogenous constructs, particularly citizen trust and propensity to use smart-city technologies. Although the minimum required sample can be estimated using GPower, the study sought to obtain a substantially larger number of responses to improve the stability and reliability of the parameter estimates and to provide adequate statistical power for testing the proposed relationships. The final sample size was therefore determined after considering the GPower estimation, the complexity of the proposed model, and the anticipated quality of the collected responses.

3.3. Research Instrument

The collected data using a questionnaire that we built from measurement scales that had already been validated in the literature. We changed the measurement items so that they fit smart-city technologies and the urban setting in India. The questionnaire had two parts. The first part asked for the respondents' demographic and technology-use details, such as age, gender, education level, job, where they live and how experience they have with digital technologies or smart-city services. The second part measured the concepts that were part of our model. The major constructs examined in the study were:

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

- Perceived Security (PS)
- Data Privacy (DP)
- Perceived Risk (PR)
- Citizen Trust (TR)
- Propensity to Use Smart-City Technologies (PUTSC)

A five-point Likert scale for the measurement items with 1 meaning Disagree and 5 meaning Strongly Agree. We changed the wording of the items where needed so that they would match how citizens see smart-city technologies and digital urban services in Karnataka. Before the survey we ran a pilot test to check that the instrument was reliable and easy to understand. The comments we received in the pilot helped us improve the wording and order of the questions.

3.4. Data Collection

The questionnaire was distributed electronically among eligible respondents residing in Karnataka. The online survey approach was adopted because the study specifically focuses on citizens who interact with digital technologies and technology-enabled services. Respondents were provided with a brief explanation of the purpose of the research and were informed that their participation was voluntary. No personally identifying information was required for the statistical analysis. The collected responses were subsequently screened and prepared for statistical analysis. The cleaned dataset was coded and imported into SPSS for preliminary data screening and descriptive analysis. Further analysis was conducted using SmartPLS to examine the measurement and structural models through Partial Least Squares Structural Equation Modeling (PLS-SEM).

3.5. Data Analysis Technique

The study uses Partial Least Squares Structural Equation Modeling (PLS-SEM) to look at the relationships between the variables in the research. PLS-SEM was chosen because the main goal is to explain how variance there is in the endogenous constructs and to check how security, privacy, risk, trust and citizens willingness to use smart-city technologies are connected. PLS-SEM works well when dealing with latent constructs that are measured using indicators and when the model has many linked relationships. It is also a fit for exploratory and predictive studies. Unlike covariance-based SEM PLS-SEM does not require the strict assumptions about multivariate normality. The analysis was done in two steps. First the measurement model was tested to make sure the constructs were reliable and valid. This step checked indicator loadings Cronbach's alpha, composite reliability and Average Variance Extracted (AVE). It also looked at convergent and discriminant validity. Second the structural model was tested to see if the predicted relationships between the constructs were supported.

3.6. Ethical Considerations

The study followed standard research-ethics principles during questionnaire administration and data analysis. Participation was voluntary, and respondents were informed about the academic purpose of the study. Respondents were given the option to discontinue participation, and the information collected was used exclusively for research purposes. The data were analyzed in aggregate form to maintain respondent confidentiality.

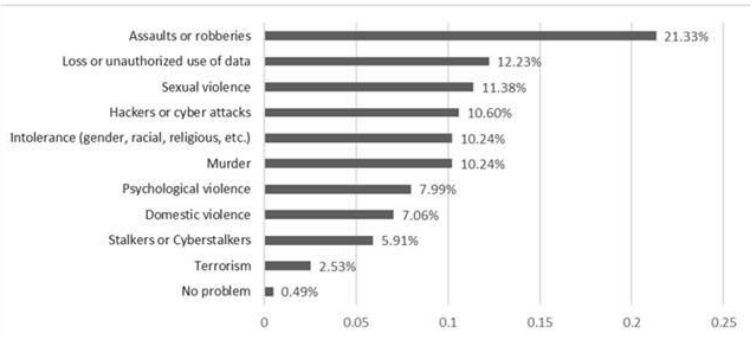
4. DATA PRESENTATION AND ANALYSIS

4.1. Characterization of Respondents

The people who took part in the study show that there are women than men. Women made up 57.9% (n = 348) of the people surveyed. Men made up 42.1% (n = 253). When it comes to age many of the people were between 18 and 27 years old. That group was 61.04% (n = 367) of the people surveyed. The fact that there are younger people is important, for this study because this group usually uses smartphones, mobile apps, digital platforms, online services and technology-based city services.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026



Source: Elaborated by the authors.

In the Karnataka context, citizens' perceptions of security are increasing interaction with digitally enabled urban infrastructure. The smart-city initiatives across Karnataka has resulted in greater integration of information and communication technologies, Internet of Things (IoT) applications, intelligent transportation systems, digital public services, surveillance technologies, and data-driven urban management. Consequently, security is no longer restricted to conventional concerns relating to physical safety but increasingly includes the protection of digital information and personal data.

Particular attention is therefore required toward concerns relating to the loss, unauthorized access, disclosure, or misuse of personal and transactional data. Citizens increasingly interact with digital platforms through smartphones and applications to access transportation, payments, public information, municipal services, and other technology-enabled facilities. As the volume of digitally generated citizen information increases, concerns regarding data security and privacy become important dimensions of responsible smart-city development. The findings therefore indicate that security within the Karnataka smart-city context should be understood from both physical and digital perspectives. While conventional urban safety remains important, the protection of citizens' information, privacy, and digital identity has become an increasingly relevant component of citizens' perceptions of smart-city technologies. This is particularly important because a lack of confidence in the protection of personal information may influence citizens' willingness to interact with technology-enabled urban services.

4.2. Normality, Common Method Bias, Non-Response Bias, and Collinearity

I checked the normality of the data using Mardias multivariate normality test. The results for the indicators were statistically significant at $p < 0.001$ showing that the assumption of multivariate normality was not met. The non-normal distribution of the data supports the use of Partial Least Squares Structural Equation Modeling (PLS-SEM) because PLS-SEM does not require multivariate normality. Because the study relies on data collected through a structured questionnaire I assessed potential common method bias (CMB). I conducted Harmans single-factor test as suggested by Podsakoff and Organ (1986) using the measurement items. The variance explained by the extracted component was 39.75%, which is below the commonly applied threshold of 50%. This result indicates that a single factor did not account for the majority of the variance suggesting that common method bias was not a concern in the dataset. The conducted a non-response bias analysis by comparing the responses of two respondent groups using an independent-samples t-test. The comparison did not identify significant differences between the groups. This finding indicates that systematic differences between late/non-respondents were not evident supporting the use of the complete valid sample for subsequent analysis, examined multicollinearity among the predictor constructs using the Variance Inflation Factor (VIF). The VIF values associated with the constructs predicting propensity to use smart-city technologies were, below the recommended threshold of 3.3. The observed values are:

Construct	VIF

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

Objective Security and Data Privacy (OSDP)	1.820
Perceived Risk (PR)	1.950
Propensity to Use Smart-City Technologies (PUTSC)	1.993
Subjective Security (SS)	2.276
Trust (TR)	1.690

As all the VIF values were below 3.3, serious multicollinearity among the predictor constructs was not identified.

4.3. Structural Equation Model

Following the estimate of the PLS-SEM model the measurement model was checked to make sure the constructs were reliable and valid. The check looked at how strong each indicator was the Cronbachs alpha, the reliability the average variance extracted and how different the constructs were from each other. In the time the measurement model was tested indicators that had factor loadings lower than the suggested level of 0.70 were considered for removal. So SS1, TR4 and PUTSC4 were taken out of the model to make the measurement model better and get indicator reliability. The measurement model was checked before looking at the relationships between the hidden constructs. Cronbachs alpha was used to check how consistent the items were. Composite reliability was also checked as another way to see how reliable the constructs were. The average variance extracted values were checked to see if the constructs were all measuring the thing. The results showed that the constructs that stayed had levels of consistency and that they all measured the same thing. To check how different the constructs were the Heterotrait–Monotrait Ratio was used. This was suggested by Henseler, Ringle and Sarstedt in 2015. The HTMT values for each pair of constructs were below the suggested level of 0.90. This shows that each construct was an idea in the smart-city model, for Karnataka. Table 1 shows the results of the measurement model. It includes Cronbachs alpha, reliability and average variance extracted.

Table 1. Convergent and Discriminant Validity

Constructs	CA	CR	AVE	R^2	(1)	(2)	(3)	(4)	(5)
(1) Objective Security and Data Privacy	0.837	0.902	0.754	0.032	0.868				
(2) Perceived Risk	0.782	0.873	0.696	—	-0.178	0.834			
(3) Propensity to Use Technologies in Smart Cities	0.820	0.893	0.736	0.232	0.322	-0.190	0.858		
(4) Subjective Security	0.812	0.889	0.727	0.576	0.618	-0.262	0.474	0.853	
(5) Trust	0.856	0.912	0.777	0.314	0.540	-0.242	0.530	0.705	0.881

The reliability coefficients show that the measurement items kept in the study are consistent with each other. The composite reliability numbers also back up how reliable the constructs are. The AVE results give evidence that the constructs converge together. Table 2 shows the numbers that help prove that the constructs are distinct, from each other.

Table 2. HTMT Criterion

Constructs	OSDP	PR	PUTSC	SS	TR
OSDP	—	—	—	—	—
PR	0.218	—	—	—	—
PUTSC	0.387	0.235	—	—	—
SS	0.748	0.325	0.583	—	—
TR	0.639	0.290	0.468	0.841	—

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

All HTMT values were below 0.90, supporting discriminant validity among the reflective constructs.

4.4. Structural Model and Hypothesis Testing

After we checked that the measurement model was reliable and valid we looked at the model to see how Objective Security and Data Privacy (OSDP) Perceived Risk (PR) Trust (TR) Subjective Security (SS) and Propensity to Use Smart-City Technologies (PUTSC) are related. We used the bootstrapping procedure in PLS-SEM to estimate the model. Bootstrapping makes small samples from the original data set and helps us see if the path coefficients are statistically significant. The analysis examined the relationships, among OSDP, PR, TR, SS and PUTSC and the corresponding hypotheses. The results of the model are presented in Table 3.

Table 3. Structural Path Results and Hypothesis Testing

Hypotheses	**β**	**Bootstrapping β (n = 5,000)**	**Standard Deviation**	***t*-Value**	***p*-Value**	**CI 2.5%**	**CI 97.5%**
Direct Relationships							
H1a: OSDP → SS	0.335	0.335	0.038	8.887	0.000	0.262	0.409
H1b: OSDP → TR	0.513	0.513	0.037	13.906	0.000	0.437	0.582
H2a: PR → OSDP	-0.178	-0.181	0.044	-4.097	0.000	-0.266	-0.096
H2b: PR → TR	-0.150	-0.152	0.035	-4.337	0.000	-0.219	-0.085
H3a: TR → SS	0.524	0.524	0.036	14.540	0.000	0.452	0.591
H3b: TR → PUTSC	0.121	0.121	0.053	2.277	0.023	0.014	0.224
H4: SS → PUTSC	0.389	0.389	0.059	6.629	0.000	0.275	0.504
Indirect Relationships (Mediators)							
M1: PR → OSDP → TR	-0.091	-0.092	0.022	-4.080	0.000	-0.136	-0.049
M2: OSDP → TR → SS	0.268	0.268	0.026	10.265	0.000	-0.218	0.320
M3: TR → SS → PUTSC	0.204	0.203	0.035	5.802	0.000	0.137	0.276

The relationships among security, privacy, perceived risk, trust, subjective security, and propensity to use smart-city technologies are statistically significant. The findings suggest that citizens' perceptions of security and privacy are closely associated with their trust in smart-city technologies and that trust and perceived security subsequently influence citizens' willingness to use technology-enabled urban services. The mediation analysis further examined TR in the proposed relationships. The significant indirect effects, demonstrating that trust mechanism through which security- and privacy-related perceptions influence citizens' perceptions and technology-use intentions. Where both statistically significant, the mediation was interpreted as partial mediation. Overall, the structural model provides empirical evidence that responsible deployment of smart-city technologies in Karnataka requires attention not only to technological functionality but also to citizens' perceptions of security, privacy, risk, and institutional/technological trust.

5. DISCUSSION OF THE RESULTS

When analyzing the hypotheses formulated in Table 3, the proposed model provides empirical evidence regarding the relationships among Objective Security and Data Privacy (OSDP), Perceived Risk (PR), Trust (TR), Subjective Security (SS), and Propensity to Use Smart-City Technologies (PUTSC) in the Karnataka context. The findings demonstrate that citizens' propensity to use smart-city technologies is influenced not only by the availability and functionality of digital technologies but also by their perceptions of security, privacy, risk and trust. This is particularly relevant in Karnataka, where cities such as Bengaluru, Belagavi, Davanagere, Hubballi-Dharwad, Mangaluru, Shivamogga and Tumakuru have been associated with smart-city initiatives and digitally enabled urban services. The findings are consistent with emerging Indian research showing that citizen perceptions are important in the adoption of technology-enabled public services. Hebbar and Kiran, in their study of mobile-government adoption in Karnataka's smart cities, examined 1,444

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

citizen responses using PLS-SEM and found that trust, transparency, information quality and other technology-related factors significantly influence usage intentions. Their findings demonstrate the importance of citizens' perceptions and institutional factors in encouraging the adoption of digital public services in Karnataka. Similarly, Gupta et al.'s meta-analytic study of 68 empirical studies identified trust, perceived risk, privacy and security as important factors in understanding citizens' use of technology-enabled government services.

5.1. Objective Security and Data Privacy and Subjective Security

Hypothesis H1a, representing the relationship between Objective Security and Data Privacy (OSDP) and Subjective Security (SS), was supported ($\beta = 0.335$; $p < 0.001$). The positive relationship indicates that stronger perceptions of security and data protection are associated with stronger perceptions that smart-city technologies are safe and dependable to use. This finding is particularly relevant to Karnataka's smart-city environment because digitally enabled urban services increasingly depend on interconnected information systems, IoT-enabled infrastructure, digital applications, integrated command and control mechanisms and data-driven public services. Citizens may not possess the technical knowledge required to directly evaluate encryption, authentication mechanisms, access controls or cybersecurity architecture. Consequently, their subjective assessment of security may depend on whether visible safeguards and responsible data-management practices are associated with the technology. The finding is also consistent with the Indian smart-city literature. Mishra, Sharma and Choudhary's study of Jammu Smart City examined data privacy and security, user trust and satisfaction across 11 smart-city services and found that data privacy and security are important dimensions of users' experience with smart-city services. In Karnataka, Venumuddala, Prakash and Chaudhuri's work on smart-city IoT governance similarly emphasizes the importance of governance and ethical considerations in implementing IoT-based urban interventions.

5.2. Objective Security and Data Privacy and Trust

Similarly, hypothesis H1b, which examined OSDP and Trust (TR), was supported ($\beta = 0.513$; $p < 0.001$). This represents relationships that citizens' trust in smart-city technologies is strongly associated with their perception that personal information and digital interactions are adequately protected. In a smart-city environment, citizens may provide or generate information through digital public-service applications, mobile platforms, transportation systems, digital payment mechanisms, municipal services and other technology-enabled infrastructure. The increasing interconnection of these systems makes data protection an important component of citizens' confidence in smart-city services. The result is supported by Indian evidence. Mishra, Sharma and Choudhary reported a relationship between data privacy and security and users' trust in the context of Jammu Smart City. In addition, Gupta et al.'s MASEM study found that privacy, security, perceived risk and trust are interconnected factors in technology-enabled government-service use. The Karnataka-specific evidence reported by Hebbar and Kiran further supports the importance of trust in digital public-service adoption.

5.3. Perceived Risk and Objective Security and Data Privacy

The negative relationship proposed in hypothesis H2a, representing the path PR → OSDP, was supported ($\beta = -0.178$; $p < 0.001$). The negative coefficient indicates that higher perceived risk is associated with weaker perceptions of security and data privacy. This relationship reflects the opposing nature of the two constructs. When citizens perceive a high possibility of unauthorized access, data leakage, misuse of personal information, surveillance or cyber-related threats, they may be less likely to perceive smart-city technologies as adequately protected. Conversely, when citizens believe that appropriate safeguards are available to prevent or manage such risks, their perceptions of security and privacy may become more favourable. This issue is particularly important for Karnataka because smart-city services involve interconnected digital systems and multiple stakeholders. Information may move between citizens, government agencies, technology providers and service operators. Such interdependence can create uncertainty regarding how information is collected, processed, stored and shared. Gupta et al.'s synthesis of 68 empirical studies demonstrates the relevance of perceived risk, privacy and security to citizens' trust and technology-use behaviour. Similarly, Indian smart-

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

governance research has found that insecurity can negatively influence citizens' perceptions of smart-governance services, while favourable technology perceptions can subsequently influence usage intentions.

5.4. Perceived Risk and Trust

Likewise, hypothesis H2b concerning the relationship PR → TR was supported ($\beta = -0.150$; $p < 0.001$). The negative coefficient indicates that greater perceived risk is associated with lower levels of trust in smart-city technologies. Citizens may hesitate to trust digital urban services when they are uncertain about who can access their information, how long personal information will be retained, whether information may be shared with third parties, and what consequences could arise from unauthorized access or a security breach. Such uncertainty can become particularly important when citizens are required to provide personal information in order to access public or technology-enabled urban services. The finding corresponds with the broader evidence synthesized by Gupta et al., which identifies perceived risk, privacy and security as important factors associated with trust in technology-enabled government services. It is also relevant to the Karnataka context because smart-city systems involve interactions between citizens, government institutions and technology providers. The Karnataka study by Hebbar and Kiran provides additional contextual support for the importance of trust. Their research found that information quality and transparency contributed to trust and that trust was relevant to usage intention in Karnataka's smart cities.

5.5. Trust and Subjective Security

Hypothesis H3a, representing the relationship TR → SS, was supported ($\beta = 0.524$; $p < 0.001$). This was the strongest direct relationship among the hypotheses reported in the model. The result indicates that citizen perception that smart-city technologies are secure. Citizens cannot necessarily inspect the technical security architecture of a smart-city platform themselves. Instead, their perception of security in the organizations, institutions and technology providers responsible for managing the system. In this sense, trust acts as an important interpretive mechanism. When citizens believe that institutions are responsible, transparent and capable of protecting their information, they may be more likely to perceive the technology as safe. Conversely, uncertainty regarding institutional practices can weaken perceptions of security even when technical safeguards exist. This finding is consistent with Indian smart-city research. Mishra, Sharma and Choudhary examined data privacy and security together with user trust in Jammu Smart City and highlighted the importance of privacy and security in shaping users' experience with smart-city services. Gupta et al. similarly demonstrate through their meta-analytic evidence that privacy, security, risk and trust are closely connected in digital government-service use. For Karnataka, the result indicates that maintaining citizens' trust requires continuous attention to data protection, institutional accountability, security practices and responsiveness to citizen concerns.

5.6. Trust and Propensity to Use Smart-City Technologies

Hypothesis H3b, examining the relationship TR → PUTSC, was supported ($\beta = 0.121$; $p = 0.023$). The positive relationship indicates that greater trust is associated with greater propensity to use smart-city technologies. Although the coefficient is comparatively modest, its statistical significance demonstrates that trust constitutes an important component of citizens' technology-use decisions. The presence of a smart-city application or digitally enabled service does not automatically ensure citizen adoption. Citizens also need confidence that the technology will function appropriately and that their information and interactions will be managed responsibly. This finding is particularly relevant to Karnataka. Hebbar and Kiran's study of 1,444 citizens across Karnataka's smart cities found significant relationships involving trust, transparency, information quality and usage intention. Their findings demonstrate that citizen trust is relevant to digital public-service adoption in the Karnataka environment. Similarly, Indian research on smart governance has shown that citizens' perceptions of insecurity can affect their perceptions of smart-governance services and, subsequently, their intention to use them.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

5.7. Subjective Security and Propensity to Use Smart-City Technologies

Hypothesis H4, examining the relationship SS → PUTSC, was supported ($\beta = 0.389$; $p < 0.001$). The result demonstrates that citizens' perception of security has a significant positive relationship with their propensity to use smart-city technologies. When citizens perceive a digital urban service as safe and adequately protected, they may be more willing to consider using that service. This relationship is important because smart-city services can involve sensitive interactions, including digital payments, mobility services, municipal applications, online public services and other technology-enabled urban functions. The result also corresponds with Indian research on smart governance and digital public-service adoption, where insecurity has been found to influence citizens' perceptions of smart-governance services and their subsequent intention to use them. In Karnataka, this relationship becomes particularly relevant because smart-city development involves increasing integration of digital technologies into everyday urban services.

5.8. Mediating Relationships

The mediation results provide additional insight into the mechanisms connecting security, risk, privacy, trust and propensity to use smart-city technologies. The first mediation, M1 (PR → OSDP → TR), was significant ($\beta = -0.091$; $p < 0.001$). This indicates that perceived risk has an indirect negative relationship with trust through objective security and data privacy. Citizens' concerns about potential security and privacy threats may therefore influence their trust partly through their assessment of whether adequate security and privacy safeguards are available. The second mediation, M2 (OSDP → TR → SS), produced a significant indirect effect ($\beta = 0.268$; $p < 0.001$). This finding indicates that trust contributes to the relationship between objective security and data privacy and subjective security. In other words, security and privacy safeguards may strengthen citizens' subjective perception of security partly by increasing their trust in the institutions, systems and service providers responsible for smart-city technologies.

The third mediation, M3 (TR → SS → PUTSC), was significant ($\beta = 0.204$; $p < 0.001$). This result indicates that subjective security contributes to the relationship between trust and propensity to use smart-city technologies. Trust may therefore encourage technology use partly because it strengthens citizens' perception that smart-city technologies are safe and dependable. Taken together, the mediation findings demonstrate that security and privacy mechanisms do not operate independently from citizen perceptions. Instead, objective security and privacy, trust, subjective security and propensity to use are interconnected dimensions of smart-city technology adoption.

5.9. Theoretical and Practical Implications

Overall, proposed model in the Karnataka context. The results demonstrate that Objective Security and Data Privacy, Perceived Risk, Trust and Subjective Security are interconnected dimensions of citizens' propensity to use smart-city technologies by demonstrating that smart-city technology adoption should be understood not only in terms of technological functionality but also through citizens' perceptions of security, privacy, risk and institutional trust. The findings extend the understanding of technology adoption by highlighting the role of both tangible security-related mechanisms and intangible perceptions of safety and trust. The study is also consistent with Indian smart-city research emphasizing citizen-centred factors. For example, research in Karnataka has shown that information quality and transparency can strengthen trust and influence usage intention in smart-city mobile-government services. Similarly, research in Jammu Smart City has demonstrated the relevance of data privacy and security to users' trust and satisfaction. From a practical perspective, Karnataka's smart-city authorities and technology providers should focus on making security and privacy practices understandable to citizens. This may include clear privacy notices, transparent explanations of data collection and use, appropriate access controls, secure authentication mechanisms, mechanisms for addressing citizen concerns and clearly defined accountability for data management.

This is particularly important where smart-city systems involve multiple organizations, technology providers and interconnected platforms. Furthermore, the relationship between perceived risk and trust indicates the importance of reducing uncertainty. Authorities and service providers can address this through transparent communication regarding

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

what information is collected, why it is collected, how it is stored, who can access it, whether it is shared and what mechanisms are available when citizens have concerns. The findings from Indian smart-city research reinforce this perspective. Mishra, Sharma and Choudhary found that data privacy and security are relevant to users' trust in smart-city services, while Gupta et al.'s broader synthesis demonstrates the interconnected roles of trust, risk, privacy and security in technology-enabled government services. Therefore, smart-city development in Karnataka should not be evaluated only through technological infrastructure, service efficiency or digital connectivity. Citizen trust, perceived security, responsible data management and privacy protection should also be considered important dimensions of smart-city implementation. The findings also provide a basis for future research. Future studies could extend the proposed model by incorporating constructs such as transparency, perceived fairness, accountability, institutional trust, data-governance awareness, AI trust and citizen participation. Comparative research could examine whether perceptions differ across Bengaluru, Belagavi, Davanagere, Hubballi-Dharwad, Mangaluru, Shivamogga and Tumakuru. Finally, future studies could examine how citizens' experiences with individual smart-city services influence their perceptions of security and trust. Longitudinal studies may also determine whether trust and security perceptions change as citizens gain greater experience with digital urban services. Such research would contribute to a deeper understanding of responsible technology adoption and help policymakers develop smart-city systems that combine technological advancement with citizen confidence, privacy protection and accountable data governance.

REFERENCES

[1] Gupta, P., Hooda, A., Jeyaraj, A., Seddon, J. J. M., & Dwivedi, Y. K. (2025). Trust, risk, privacy and security in e-government use: Insights from a MASEM analysis. *Information Systems Frontiers, 27*(3), 1089–1105. https://doi.org/10.1007/s10796-024-10497-8

[2] Venumuddala, V. R., Prakash, A., & Chaudhuri, B. (2024). Governing smart city IoT interventions: A complex adaptive systems perspective. *Digital Government: Research and Practice, 5*(3), Article 23, 1–24. https://doi.org/10.1145/3660644

[3] Sharma, C., Choudhary, S., & Mishra, S. S. (2025). Unfolding the relationship between data privacy and security, users' trust and satisfaction in smart cities using the IS model. *Transforming Government: People, Process and Policy, 19*(4), 775–794. https://doi.org/10.1108/TG-06-2025-0190

[4] Dash, A. (2024). Understanding citizen adoption of smart governance: Integrating technology acceptance and readiness theories. *Global Knowledge, Memory and Communication*. https://doi.org/10.1108/GKMC-08-2024-0509

[5] Smart mobility reference used in the discussion: *Smart mobility in smart cities: Transforming the experiences of citizens into the future of smart cities.* (2024). *Transforming Government: People, Process and Policy, 18*(2), 287–302. https://doi.org/10.1108/TG-09-2023-0136

[6] arter, L., & Bélanger, F. (2005). The utilization of e-government services: Citizen trust, innovation and acceptance factors. Information Systems Journal, 15(1), 5–25. https://doi.org/10.1111/j.1365-2575.2005.00183.x

[7] Chatterjee, S., & Kar, A. K. (2018). Effects of successful adoption of information technology enabled services in proposed smart cities of India: From user experience perspective. Journal of Science and Technology Policy Management, 9(2), 189–209. https://doi.org/10.1108/JSTPM-03-2017-0008

[8] Choi, J. (2022). Enablers and inhibitors of smart city service adoption: A dual-factor approach based on the technology acceptance model. Telematics and Informatics, 75, 101911. https://doi.org/10.1016/j.tele.2022.101911

[9] Dash, A. (2024a). Smart mobility in smart cities: Transforming the experiences of citizens into the future of smart cities. Transforming Government: People, Process and Policy, 18(2), 287–302. https://doi.org/10.1108/TG-09-2023-0136

[10] Dash, A. (2024b). Understanding citizen adoption of smart governance: Integrating technology acceptance and readiness theories. Global Knowledge, Memory and Communication. https://doi.org/10.1108/GKMC-08-2024-0509

[11] Ebrahim, Z., & Irani, Z. (2005). E-government adoption: Architecture and barriers. Business Process Management Journal, 11(5), 589–611. https://doi.org/10.1108/14637150510619902

[12] Featherman, M. S., Miyazaki, A. D., & Sprott, D. E. (2010). Reducing online privacy risk to facilitate e-service adoption: The influence of perceived ease of use and corporate credibility. Journal of Services Marketing, 24(3), 219–229. https://doi.org/10.1108/08876041011040622

[13] Gupta, P., Hooda, A., Jeyaraj, A., Seddon, J. J. M., & Dwivedi, Y. K. (2025). Trust, risk, privacy and security in e-government use: Insights from a MASEM analysis. Information Systems Frontiers, 27(3), 1089–1105. https://doi.org/10.1007/s10796-024-10497-8

[14] Hakeem, M. J., & Sulphey, M. M. (2025). An evaluation of factors affecting the acceptance of smart city ICT services in India. Public Administration and Policy. https://doi.org/10.1108/PAP-07-2024-0114

[15] Hebbar, S., & Kiran, K. B. (2024). Social media integrated mobile government adoption model: Investigating adoption behaviour in Karnataka's smart cities. Electronic Government, an International Journal, 20(6), 705–733. https://doi.org/10.1504/EG.2024.141860

[16] Mishra, S., Sharma, C., & Choudhary, S. (2025). Unfolding the relationship between data privacy and security, users' trust and satisfaction in smart cities using the IS model. Transforming Government: People, Process and Policy, 19(4), 775–794. https://doi.org/10.1108/TG-06-2025-0190

[17] Shukla, R. (2017). Models of smart governance: Community involvement in local governance. In Proceedings of the Special Collection on eGovernment Innovations in India (pp. 82–87). Association for Computing Machinery. https://doi.org/10.1145/3055219.3055240

[18] Venumuddala, V. R., Prakash, A., & Chaudhuri, B. (2024). Governing smart city IoT interventions: A complex adaptive systems perspective. Digital Government: Research and Practice, 5(3), Article 23, 1–24. https://doi.org/10.1145/3660644

(This work is licensed under a Creative Commons Attribution 4.0 International License.)