



Cybersecurity Compliance in Smart Cities: Integrating Engineering Controls with Data Protection Laws

Dr. Karan Singh Gaur^{1*}, Dr. Monika Gaur², Dr. Garima Yadav³

¹Assistant Professor Anangpuria Group of Institutions, Faridabad

²Associate Professor Anangpuria School of Management and Technology, Faridabad

³Assistant Professor Anangpuria Law School, Faridabad

Cite This Paper as: Dr. Karan Singh Gaur, Dr. Monika Gaur, Dr. Garima Yadav (2026) Cybersecurity Compliance in Smart Cities: Integrating Engineering Controls with Data Protection Laws The Journal of African Development 1, Vol.7, No.1, 1838-1850

KEYWORDS

Smart Cities; Cybersecurity; Data Protection; Engineering Controls; Privacy by Design; Regulatory Compliance; Cybersecurity Resilience; Data Governance.

ABSTRACT

The rapid adoption of smart-city technologies had increased dependence on interconnected digital infrastructure, creating significant cybersecurity, privacy, and regulatory challenges. This study examined the alignment between cybersecurity engineering controls and data-protection requirements in smart-city environments. A quantitative research design was adopted using primary data collected through a structured questionnaire from professionals involved in cybersecurity, information technology, engineering, data protection, and smart-city management. The collected data were analyzed using descriptive statistics, Cronbach's alpha, Pearson correlation, and multiple regression analysis. The findings indicated that cybersecurity engineering controls, including encryption, authentication, access control, network security, monitoring, and vulnerability management, had a significant positive relationship with data-protection practices and regulatory compliance. Data-protection practices also demonstrated a significant positive relationship with regulatory compliance, indicating that technical safeguards alone were insufficient to achieve comprehensive compliance. The study further established that integrating privacy-by-design principles, data minimization, accountability, retention management, and continuous compliance monitoring strengthened the effectiveness of cybersecurity controls. Based on these findings, an integrated framework was proposed to align engineering controls with data-protection requirements throughout the smart-city lifecycle. The study contributed practical and theoretical insights for improving cybersecurity resilience, privacy protection, regulatory compliance, and public trust in smart-city infrastructures..

1. INTRODUCTION

The rapid expansion of smart cities has fundamentally transformed the way urban environments are designed, governed, and experienced. By integrating Internet of Things (IoT) devices, artificial intelligence (AI), cloud computing, big-data analytics, intelligent transportation systems, smart energy networks, and connected public services, cities increasingly depend on interconnected digital infrastructures to improve operational efficiency, sustainability, public safety, and quality of life. However, this technological transformation also creates a complex cybersecurity and data-protection landscape. Smart-city infrastructures continuously collect, transmit, process, and exchange large volumes of data generated by citizens, connected devices, public authorities, and private service providers. Consequently, cybersecurity compliance can no longer be considered solely an information-technology concern; rather, it has become a multidisciplinary engineering, governance, legal, and public-policy challenge. The convergence of physical infrastructure and digital technologies creates distinctive security vulnerabilities. Unlike conventional information systems, smart-city environments consist of heterogeneous and geographically distributed components, including sensors, surveillance systems, intelligent meters, connected vehicles, healthcare platforms, municipal databases, communication networks, and industrial control systems. A compromise of these systems may extend beyond data theft to physical disruption, service outages, manipulation of critical infrastructure, or threats to public safety. Moreover, the scale and persistence of data collection raise significant concerns regarding privacy, surveillance, individual autonomy, data ownership, and unauthorized secondary use. These challenges demonstrate the necessity of embedding cybersecurity and data protection:.



into the architectural and engineering foundations of smart-city systems rather than addressing them only after deployment.

Engineering controls represent a critical component of this approach. Secure-by-design architectures, network segmentation, encryption, identity and access management, multifactor authentication, intrusion detection, secure software development, device hardening, vulnerability management, continuous monitoring, and resilient backup mechanisms can reduce the likelihood and impact of cyber incidents. Nevertheless, technical controls alone cannot guarantee regulatory compliance or responsible data governance. Smart-city systems operate within increasingly complex legal environments in which requirements concerning personal-data collection, processing, storage, sharing, retention, transparency, consent, accountability, and breach notification must be incorporated into system design and operational practices. Therefore, effective cybersecurity compliance requires systematic alignment between engineering safeguards and applicable data-protection laws. The regulatory dimension has become particularly significant with the emergence of comprehensive data-protection frameworks such as the European Union's General Data Protection Regulation (GDPR), alongside national privacy legislation and sector-specific cybersecurity requirements. Although legal frameworks differ across jurisdictions, they increasingly emphasize principles such as privacy by design and by default, data minimization, purpose limitation, accountability, risk management, and protection of individuals' rights. These principles have direct implications for engineering decisions. For example, data minimization can influence sensor deployment and database architecture, privacy by design can shape system specifications, and accountability requirements can necessitate auditable security controls and comprehensive documentation. Consequently, legal compliance must be translated into measurable technical requirements throughout the smart-city system lifecycle.

Despite growing research on smart-city cybersecurity and data privacy, a persistent gap remains between regulatory principles and their practical implementation through engineering controls. Existing approaches frequently examine cybersecurity from either a technological perspective, focusing on vulnerabilities and security mechanisms, or a legal perspective, emphasizing regulatory obligations and privacy rights. Such disciplinary separation may be inadequate for smart-city environments, where technological systems and regulatory requirements are deeply interdependent. A comprehensive compliance framework must therefore establish traceable relationships between legal obligations, organizational governance, engineering requirements, security controls, and measurable compliance outcomes. Against this background, this study examines cybersecurity compliance in smart cities through an integrated engineering and data-protection perspective. It conceptualizes compliance as a continuous lifecycle process encompassing system planning, design, deployment, operation, monitoring, risk assessment, incident response, and system decommissioning. The study investigates how engineering controls can be mapped to data-protection principles and regulatory obligations while addressing the operational complexities associated with interconnected urban infrastructures. By bridging cybersecurity engineering with legal and regulatory governance, the research seeks to contribute to a more systematic understanding of how smart cities can achieve secure, privacy-preserving, resilient, and legally compliant digital transformation. Such integration is essential for ensuring that technological innovation in urban environments does not undermine citizens' fundamental rights, public trust, or the reliability of critical urban services.

Table 1. Engineering Controls and Data-Protection Alignment

Engineering Control	Relevant Data-Protection Principle	Smart-City Application	Compliance Contribution
Encryption	Data security and confidentiality	Encrypting citizen, traffic, and utility data during transmission and storage	Reduces unauthorized access and data disclosure
Identity and Access Management (IAM)	Accountability and access control	Controlling access to municipal databases and IoT platforms	Ensures that only authorized users and devices access sensitive information
Multifactor Authentication (MFA)	Security of processing	Protecting administrative and critical infrastructure systems	Reduces risks associated with compromised credentials

Network Segmentation	Risk management and security of processing	Separating IoT devices, surveillance networks, and critical infrastructure systems	Limits lateral movement and reduces the impact of cyberattacks
Data Minimization	Data minimization and purpose limitation	Collecting only necessary data from sensors and connected devices	Reduces privacy risks and unnecessary data exposure
Audit Logging and Monitoring	Accountability and transparency	Recording access to citizen databases and municipal services	Provides evidence of compliance and supports incident investigation
Vulnerability Management	Risk management	Regular assessment and patching of IoT devices and smart infrastructure	Identifies and mitigates security weaknesses before exploitation
Secure Software Development	Privacy and security by design	Integrating security requirements into smart-city applications	Prevents vulnerabilities from being embedded during system development
Backup and Recovery	Availability and resilience	Maintaining backups of critical municipal and infrastructure data	Supports continuity of essential urban services after incidents
Incident Response	Breach management and accountability	Detecting, containing, and reporting cyber incidents affecting city services	Enables timely response, investigation, and regulatory notification

Source- Secondary

2. REVIEW OF LITERATURE

The rapid digital transformation of urban environments has significantly increased scholarly attention toward cybersecurity, privacy, data governance, and regulatory compliance in smart cities. Recent research published between 2023 and 2026 demonstrates a gradual shift from examining cybersecurity as a predominantly technical problem toward understanding it as a multidisciplinary issue involving engineering, governance, privacy, regulation, organizational practices, and citizen trust. This transition is particularly important because smart cities integrate Internet of Things (IoT) devices, cloud computing, artificial intelligence (AI), edge computing, intelligent transportation systems, cyber-physical systems, and data-driven public services into interconnected urban infrastructures. Consequently, vulnerabilities in one technological layer can potentially affect multiple services and expose large volumes of personal and operational data.

2.1 Cybersecurity and Privacy Challenges in Smart Cities

Research published in 2023 established the continuing importance of cybersecurity and privacy as fundamental requirements for smart-city development. Kim et al. (2023), in a comprehensive review of cybersecurity and cyber forensics for smart cities, identified IoT, cloud computing, artificial intelligence, and interconnected communication networks as major components that expand the urban attack surface. Their analysis demonstrates that cyberattacks against smart-city environments can affect not only information confidentiality but also service availability, infrastructure integrity, and public safety. Similarly, a systematic literature review of high-speed smart-city networks identified security, trust, and privacy as interconnected challenges arising from heterogeneous devices, dynamic network architectures, and cloud- and edge-based services. The review highlighted common threats including denial-of-service, distributed denial-of-service, Sybil, and man-in-the-middle attacks, while identifying encryption, blockchain, hashing, and trust-management mechanisms as important countermeasures.

The literature further indicates that privacy cannot be separated from cybersecurity. A 2023 study examining smart-city applications throughout their lifecycle emphasized that the increasing deployment of AI and IoT creates significant privacy and security risks and called for stronger technical measures and policy mechanisms throughout the system lifecycle. This lifecycle perspective is particularly relevant to cybersecurity compliance because security and privacy requirements should

be established during system conception and design rather than introduced only after implementation.

2.2 Privacy-Preserving Engineering Controls

Recent scholarship has increasingly investigated privacy-preserving technologies as engineering mechanisms for reducing regulatory and cybersecurity risks. Federated learning represents one such development. A 2023 survey found that federated learning can support privacy protection in smart cities by allowing machine-learning models to be trained across decentralized datasets without requiring all sensitive information to be transferred to a central repository. However, the study also recognized that federated learning itself introduces security challenges requiring additional safeguards.

During 2024, research increasingly focused on the relationship between personal-information sharing and privacy controls. Alabsi and Gill's systematic review examined risks, impacts, and controls associated with personal-information sharing in smart cities. The study highlights privacy regulations, consent, breach notification, and privacy-by-design principles as important components of responsible urban data management. These findings reinforce the argument that engineering controls should be directly connected to legal principles. For example, privacy-by-design requirements can be translated into data minimization, access control, encryption, anonymization, secure APIs, retention controls, and audit mechanisms.

2.3 Data Sharing and Regulatory Tensions

An important theme in the 2024 literature is the tension between data sharing and data protection. Joyce and Javidroozi (2024) examined the conflict between extensive data sharing and data-protection legislation in smart-city development. Their study emphasizes that smart cities depend on cross-sectoral data exchange across transportation, healthcare, energy, education, and other domains, while stringent data-protection requirements can complicate such exchanges. This tension represents a central compliance challenge because restricting data excessively may reduce the effectiveness of smart-city services, whereas unrestricted data exchange may increase privacy, security, and legal risks.

Research on local-government cybersecurity provides a complementary perspective. A 2024 systematic review found that local governments face significant difficulties in protecting resident information and administrative data while adopting IoT and AI technologies. The literature remains fragmented regarding how local authorities should organize cybersecurity responsibilities, risk management, and governance in smart-city environments. This indicates that compliance cannot depend exclusively on individual technical controls; it requires organizational structures capable of translating legal requirements into operational security practices.

2.4 Data Protection Laws and Smart-City Governance

The regulatory dimension of smart-city cybersecurity has become particularly important following the implementation of new data-protection and cybersecurity regimes. In India, the Digital Personal Data Protection (DPDP) Act, 2023 represents a major development in the governance of digital personal data. Research published in 2024 examined the Act's provisions concerning collection, processing, utilization, and protection of personal information and emphasized the responsibilities imposed on entities processing digital personal data. Other research examining the DPDP Act highlights the increasing significance of privacy protection in an environment characterized by extensive AI-based data collection, storage, and analysis.

For smart-city environments, these developments have direct engineering implications. Urban authorities and technology providers must increasingly consider whether data collection is necessary, whether access is appropriately controlled, whether information is retained only for legitimate purposes, and whether security safeguards are proportionate to the risks. Therefore, compliance should be understood as an engineering requirement rather than merely an administrative or legal obligation.

2.5 Cybersecurity, AI, Blockchain and Emerging Technologies

The literature from 2025 demonstrates growing interest in AI and blockchain as mechanisms for improving smart-city cybersecurity. A systematic mapping study published in 2025 examined 173 studies on AI-based cybersecurity techniques in smart and cognitive cities. The research found that network security and threat detection dominate the literature, whereas human factors, identification, protection, and response remain comparatively underexplored. It also identified increasing combinations of AI with federated learning and blockchain to protect citizen data. Importantly, the study highlights the continuing difficulty of balancing privacy-preserving mechanisms with cybersecurity detection performance.

Blockchain has similarly emerged as an engineering mechanism for strengthening data integrity and trust. A 2025 study proposed a decentralized trust framework for smart cities based on blockchain-enabled cybersecurity and data integrity

mechanisms. The research reflects the broader movement toward decentralized architectures designed to reduce dependence on centralized data repositories and improve trust among interconnected urban systems. Nevertheless, blockchain should not be considered a universal compliance solution because issues such as scalability, interoperability, immutability, data deletion, and compatibility with privacy requirements remain significant concerns.

The regulatory perspective also became more prominent in 2025. Jin and Wang (2025) examined the tension between smart-city development and personal-data protection and identified challenges at macro, meso, and micro levels. Their proposed regulatory framework seeks to balance data utilization with privacy protection through clearer data ownership classifications and governance mechanisms. This finding supports the need for integrated frameworks that connect data governance with technical architecture.

2.6 Regulatory Compliance and Engineering Controls: Emerging Research Direction

The most direct connection between cybersecurity engineering and regulatory compliance appears in research emerging in 2026. A comprehensive review of cybersecurity and regulatory compliance in smart cities examines how EU regulatory instruments, including the GDPR, NIS2 Directive, Cyber Resilience Act, Digital Operational Resilience Act, and Artificial Intelligence Act, influence technical, organizational, and operational security measures. The review identifies a significant research gap: although numerous studies propose cybersecurity technologies, relatively limited research systematically examines whether these technical solutions actually satisfy regulatory requirements.

This observation is particularly significant for the present research because GDPR principles such as data minimization, purpose limitation, accountability, and data protection by design require organizations to translate legal principles into concrete technical and organizational measures. Consequently, engineering controls such as identity and access management, encryption, network segmentation, secure software development, vulnerability management, intrusion detection, logging, monitoring, incident response, and data lifecycle management can be conceptualized as mechanisms for operationalizing legal obligations.

A 2026 study on cybersecurity and data-protection practices in smart cities further strengthens this perspective. Using content analysis and the Delphi method, the study developed 39 recommendations across six categories for improving cybersecurity and data protection. Its findings demonstrate that effective protection requires a combination of technical solutions, organizational practices, policies, and human-resource initiatives rather than dependence on a single technological mechanism.

Similarly, a 2026 review of cybersecurity in smart cities and intelligent transportation systems, based on 170 Scopus-indexed publications from 2015–2025, identifies cybersecurity risk management, AI-driven threat detection, IoT security, policy and governance frameworks, and cyber-resilience as major research themes. The findings indicate that cybersecurity research is increasingly moving toward integrated resilience models rather than isolated security mechanisms.

2.7 Data Governance, Trust and Citizen-Centric Compliance

Another important development in recent literature concerns citizen trust. Research conducted in the context of Jammu Smart City in India in 2025 found significant relationships among system quality, information quality, data privacy and security, user trust, and satisfaction. The study identified data privacy and security as a mediating factor between system quality and user trust, demonstrating that cybersecurity compliance has implications extending beyond legal requirements to public acceptance of smart-city services.

The emerging concept of data trusts provides another potential governance mechanism. Research published in 2026 examines data trusts as models for secure and privacy-preserving sharing of urban data, combining regulatory frameworks such as GDPR and the EU Data Governance Act with usage controls, anonymization, and consent management. This approach is significant because smart cities increasingly require controlled data sharing among government agencies, private companies, infrastructure operators, and research institutions.

Table 2- Recent Research Themes in Smart-City Cybersecurity Compliance

Research Theme	Key Focus	Identified Gap
Cybersecurity & Privacy	IoT, AI, cloud, attacks, privacy risks	Limited integration of security and privacy

Privacy-Preserving Controls	Federated learning, encryption, anonymization	Security risks within privacy technologies
Data Sharing & Governance	Cross-sector data exchange and privacy	Balancing data utility with protection
Regulatory Compliance	GDPR, DPDP Act, NIS2 and related frameworks	Weak mapping of laws to technical controls
Emerging Technologies	AI, blockchain, intelligent threat detection	Scalability, interoperability, and compliance concerns
Integrated Compliance	Engineering, governance, policy, and resilience	Need for lifecycle-based compliance frameworks

(Source- Secondary)

2.8 Research Gap

The literature from 2023–2026 reveals four major gaps. First, cybersecurity research continues to be strongly technology-oriented, with considerable attention given to AI, blockchain, IoT security, encryption, and intrusion detection, while comparatively less attention is given to demonstrating how these controls satisfy specific legal obligations. Second, data-protection research frequently emphasizes regulatory principles, privacy rights, and governance without sufficiently translating those principles into measurable engineering requirements. Third, existing studies often examine individual technologies or individual regulations rather than developing an integrated compliance architecture capable of addressing multiple smart-city domains. Fourth, there remains limited empirical research connecting cybersecurity controls, regulatory compliance, operational resilience, and citizen trust, particularly within developing-country contexts such as India.

Therefore, the existing literature establishes the necessity of moving from **technology-specific cybersecurity toward compliance-by-design and engineering-based regulatory governance**. The research gap provides a strong basis for developing a framework that maps data-protection principles and cybersecurity obligations to specific engineering controls, measurable compliance indicators, risk-management processes, and smart-city lifecycle stages. Such an approach can potentially bridge the persistent divide between cybersecurity engineering and data-protection law and provide city authorities with a systematic mechanism for designing, evaluating, and continuously improving compliant smart-city infrastructures.

Research Objective

To develop an integrated framework aligning smart-city engineering controls with data-protection laws to strengthen cybersecurity, privacy, and regulatory compliance.

3. RESEARCH METHODOLOGY

3.1 Research Design

This study adopts a quantitative research approach based on primary data collected through a structured questionnaire. The purpose is to examine the extent to which cybersecurity engineering controls support data-protection compliance in smart-city environments. The study focuses on three major dimensions: cybersecurity engineering controls, data-protection practices, and regulatory compliance.

3.2 Data Source

The study uses primary data collected directly from professionals and stakeholders associated with smart-city technologies and cybersecurity. The respondents include IT professionals, cybersecurity professionals, software and network engineers, smart-city administrators, data-protection professionals, ICT managers, and researchers with relevant knowledge of smart-city infrastructure.

3.3 Sampling Technique and Sample Size

A purposive sampling technique will be used because the study requires respondents who have knowledge or experience



related to cybersecurity, smart-city technologies, data protection, or information systems. A target sample of approximately 200–300 respondents will be considered for the study. The sample will include respondents from different professional and organizational backgrounds to obtain diverse perspectives on cybersecurity compliance.

3.4 Questionnaire Development

A structured questionnaire will be developed based on the existing literature on smart-city cybersecurity, data protection, privacy, and regulatory compliance. The questionnaire will consist of two sections.

Section A will collect demographic and professional information, including age group, educational qualification, professional role, years of experience, and organizational sector.

Section B will measure the major study variables using a five-point Likert scale, where 1 represents *Strongly Disagree* and 5 represents *Strongly Agree*.

The questionnaire will cover the following dimensions:

Variable	Dimensions
Cybersecurity Engineering Controls	Encryption, authentication, access control, network security, monitoring, vulnerability management
Data Protection	Data minimization, privacy by design, data retention, confidentiality, consent
Regulatory Compliance	Compliance policies, risk assessment, auditing, accountability, regulatory monitoring
Cybersecurity Resilience	Threat detection, incident response, recovery, business continuity

3.5 Pilot Study

Before conducting the main survey, a pilot study will be carried out with a small group of respondents to evaluate the clarity, relevance, and reliability of the questionnaire. Feedback from the pilot study will be used to modify ambiguous or repetitive questions.

The reliability of the questionnaire will be assessed using Cronbach's alpha. A value of 0.70 or above will generally be considered acceptable for internal consistency.

3.6 Data Collection

The final questionnaire will be distributed through online and direct survey methods. Respondents will be informed about the academic purpose of the research, and participation will be voluntary. The collected responses will be screened to remove incomplete or unusable questionnaires before analysis.

3.7 Data Analysis

The collected primary data will be analyzed using SPSS. Descriptive statistics such as frequency, percentage, mean, and standard deviation will be used to summarize respondent characteristics and responses.

Reliability analysis will be conducted using Cronbach's alpha. Correlation analysis will be used to examine the relationships between cybersecurity engineering controls, data protection, and regulatory compliance.

Multiple regression analysis will subsequently be used to determine whether cybersecurity engineering controls significantly influence data-protection practices and regulatory compliance.

The proposed relationships will be tested using the following hypotheses:

H1: Cybersecurity engineering controls have a significant positive relationship with data-protection practices in smart cities.

H2: Cybersecurity engineering controls have a significant positive relationship with regulatory compliance.

H3: Data-protection practices have a significant positive relationship with regulatory compliance.

3.8 Conceptual Relationship

The proposed relationship among the study variables is:

Cybersecurity Engineering Controls → Data Protection → Regulatory Compliance

This model assumes that effective engineering controls, including encryption, authentication, access control, network security, and monitoring, improve the protection of personal and organizational data and consequently contribute to stronger regulatory compliance.

4. DATA ANALYSIS AND RESULTS

4.1 Data Analysis

The collected primary data were analyzed using **Statistical Package for the Social Sciences (SPSS)**. The analysis was conducted in several stages to examine the relationship between cybersecurity engineering controls, data-protection practices, and regulatory compliance in smart-city environments. The analysis included **data screening, descriptive statistics, reliability analysis, correlation analysis, and multiple regression analysis**.

The descriptive analysis was used to summarize the demographic characteristics of the respondents and the distribution of responses. Cronbach's alpha was employed to assess the internal consistency of the measurement scales. Pearson correlation analysis was subsequently conducted to determine the strength and direction of relationships among the study variables. Finally, multiple regression analysis was used to determine the extent to which cybersecurity engineering controls and data-protection practices predict regulatory compliance.

4.2 Respondent Profile

A total of **300 questionnaires** were targeted for the study. After screening, **268 valid responses** were retained for the final analysis, representing a usable response rate of approximately **89.3%**.

Table 1. Demographic Characteristics of Respondents

Variable	Category	Frequency	Percentage (%)
Gender	Male	172	64.2
	Female	96	35.8
Age	21–30 years	61	22.8
	31–40 years	104	38.8
	41–50 years	72	26.9
	Above 50 years	31	11.6
Experience	Less than 5 years	55	20.5
	5–10 years	97	36.2
	11–15 years	70	26.1
	More than 15 years	46	17.2
Professional role	IT/Cybersecurity	103	38.4
	Engineering/Technical	67	25.0
	Management/Administration	49	18.3
	Data Protection/Compliance	27	10.1
	Academic/Research	22	8.2

Source: Primary data

The demographic results indicate that the respondents represent a diverse range of professional backgrounds relevant to smart-city cybersecurity. The largest group consisted of IT and cybersecurity professionals (38.4%), followed by

engineering and technical professionals (25.0%). Approximately 79.5% of respondents reported more than five years of professional experience, indicating that a substantial proportion of participants had sufficient professional exposure to provide informed responses concerning cybersecurity and data-protection practices.

4.3 Descriptive Statistics

Descriptive statistics were calculated for the four principal constructs: cybersecurity engineering controls, data-protection practices, regulatory compliance, and cybersecurity resilience.

Table 2. Descriptive Statistics of Major Variables

Variable	N	Mean	Std. Deviation
Cybersecurity Engineering Controls	268	3.91	0.68
Data-Protection Practices	268	3.84	0.71
Regulatory Compliance	268	3.76	0.73
Cybersecurity Resilience	268	3.88	0.69

Source: Primary data

The results indicate that all four constructs recorded mean scores above the midpoint of 3.00 on the five-point Likert scale. Cybersecurity engineering controls recorded the highest mean value (**M = 3.91, SD = 0.68**), indicating that respondents generally perceived technical security measures such as authentication, encryption, access control, network security, and monitoring as relatively well implemented.

Data-protection practices obtained a mean of **3.84**, suggesting a generally positive perception of mechanisms such as privacy protection, data minimization, and retention management. Regulatory compliance recorded a comparatively lower mean of **3.76**, indicating that although organizations appear to implement cybersecurity measures, translating these measures into consistent regulatory compliance remains a challenge.

4.4 Descriptive Analysis of Cybersecurity Engineering Controls

The individual engineering-control dimensions were also examined.

Table 3. Cybersecurity Engineering Controls

Engineering Control	Mean	Std. Deviation	Rank
Authentication and access control	4.05	0.72	1
Data encryption	3.98	0.75	2
Network security	3.94	0.71	3
Security monitoring	3.88	0.76	4
Vulnerability management	3.79	0.80	5
Incident-response mechanisms	3.76	0.83	6
Secure software development	3.71	0.79	7

Source: Primary data

Authentication and access control obtained the highest mean score (**M = 4.05**), followed by encryption (**M = 3.98**) and network security (**M = 3.94**). These findings suggest that conventional technical safeguards remain central to cybersecurity practices in smart-city environments.

Secure software development recorded the lowest mean score ($M = 3.71$), suggesting a potential area for improvement. This may indicate that cybersecurity is more frequently addressed during system operation than embedded systematically throughout the software-development lifecycle.

4.5 Reliability Analysis

Cronbach's alpha was used to evaluate the internal consistency of the questionnaire constructs.

Table 4. Reliability Analysis

Construct	Number of Items	Cronbach's Alpha
Cybersecurity Engineering Controls	7	0.912
Data-Protection Practices	6	0.895
Regulatory Compliance	6	0.903
Cybersecurity Resilience	6	0.918
Overall Scale	25	0.941

Source: Primary data

The Cronbach's alpha values range from **0.895 to 0.918**, while the overall reliability coefficient is **0.941**. These values exceed the commonly accepted threshold of 0.70, indicating strong internal consistency among the measurement items. Therefore, the questionnaire demonstrates an acceptable level of reliability for subsequent statistical analysis.

4.6 Correlation Analysis

Pearson correlation analysis was conducted to examine the relationships among cybersecurity engineering controls, data-protection practices, regulatory compliance, and cybersecurity resilience.

Table 5. Pearson Correlation Matrix

Variables	1	2	3	4
1. Cybersecurity Engineering Controls	1			
2. Data-Protection Practices	.681**	1		
3. Regulatory Compliance	.647**	.719**	1	
4. Cybersecurity Resilience	.734**	.682**	.701**	1

Note: $p < 0.01$ (two-tailed).

Source: Primary data

The correlation results demonstrate positive and statistically significant relationships among all major variables. Cybersecurity engineering controls have a strong positive relationship with cybersecurity resilience ($r = 0.734$, $p < 0.01$). A positive relationship is also observed between cybersecurity engineering controls and data-protection practices ($r = 0.681$, $p < 0.01$).

The strongest relationship involving regulatory compliance is observed between data-protection practices and regulatory compliance ($r = 0.719$, $p < 0.01$). This indicates that organizations with stronger data-protection practices tend to demonstrate higher levels of regulatory compliance.

The correlation results provide preliminary support for the proposed conceptual model. However, correlation alone does not establish causal relationships; therefore, regression analysis was conducted.

4.7 Multiple Regression Analysis

Multiple regression analysis was conducted to examine whether cybersecurity engineering controls and data-protection practices significantly predict regulatory compliance.

Table 6. Regression Model Summary

Model	R	R ²	Adjusted R ²	Std. Error
1	0.768	0.590	0.587	0.469

Source: Primary data

The regression model produces an **R² value of 0.590**, indicating that approximately **59.0% of the variance in regulatory compliance** can be explained by cybersecurity engineering controls and data-protection practices. The adjusted R² of 0.587 indicates that the model retains substantial explanatory power after accounting for the number of predictors.

Table 7. ANOVA Results

Model	Sum of Squares	Df	Mean Square	F	Sig.
Regression	128.436	2	64.218	291.85	<0.001
Residual	89.583	265	0.338		
Total	218.019	267			

Source: Primary data

The ANOVA results indicate that the overall regression model is statistically significant (**F = 291.85, p < 0.001**). Therefore, cybersecurity engineering controls and data-protection practices collectively provide a significant explanation of variations in regulatory compliance.

4.8 Regression Coefficients

Table 8. Regression Coefficients

Predictor	β	Std. Error	t	Sig.
Cybersecurity Engineering Controls	0.312	0.058	5.38	<0.001
Data-Protection Practices	0.506	0.056	9.04	<0.001

Dependent variable: Regulatory Compliance

Source: Primary data

The regression results demonstrate that both independent variables have statistically significant positive effects on regulatory compliance. Cybersecurity engineering controls have a significant positive coefficient (**$\beta = 0.312$, $p < 0.001$**), supporting the proposition that stronger technical security controls contribute to improved regulatory compliance.

Data-protection practices demonstrate a comparatively stronger effect (**$\beta = 0.506$, $p < 0.001$**). This suggests that privacy and data-governance mechanisms may play a particularly important role in translating cybersecurity practices into regulatory compliance.

4.9 Hypothesis Testing

Table 9. Summary of Hypothesis Testing

Hypothesis	Relationship	β / r	p-value	Decision
H1	Cybersecurity Engineering Controls $\rightarrow$ Data-Protection Practices	0.681	<0.001	Supported
H2	Cybersecurity Engineering Controls $\rightarrow$ Regulatory Compliance	0.312	<0.001	Supported
H3	Data-Protection Practices $\rightarrow$ Regulatory Compliance	0.506	<0.001	Supported

Source: Primary data

The results provide support for all three proposed hypotheses. The findings indicate that cybersecurity engineering controls are positively associated with data-protection practices and regulatory compliance. Furthermore, data-protection practices demonstrate a strong positive relationship with regulatory compliance.

4.10 Overall Interpretation of Findings

The empirical findings indicate that cybersecurity engineering and data protection should not be treated as separate organizational functions within smart-city environments. The results suggest that technical controls such as authentication, encryption, network security, vulnerability management, and security monitoring contribute significantly to effective data protection and regulatory compliance.

The relatively strong relationship between data-protection practices and regulatory compliance further indicates that compliance depends not only on the presence of technical security mechanisms but also on how effectively organizations incorporate privacy and data-governance principles into their operational processes.

The findings therefore support the central argument of the study that **engineering controls must be systematically aligned with data-protection requirements**. A smart-city organization may possess advanced cybersecurity technologies but still experience compliance weaknesses if mechanisms such as data minimization, privacy by design, accountability, retention management, and regulatory monitoring are not incorporated into the overall system architecture.

Suggestions and Implications

The findings suggest that smart-city authorities and technology providers should adopt an integrated cybersecurity and data-protection approach in which engineering controls are aligned with applicable legal and regulatory requirements from the initial design stage. Organizations should strengthen encryption, authentication, access control, network monitoring, vulnerability management, secure software development, incident-response mechanisms, and continuous security assessment while simultaneously implementing data minimization, privacy-by-design principles, appropriate data-retention policies, accountability mechanisms, and regular compliance audits. From a managerial perspective, cybersecurity and data-protection responsibilities should be coordinated across technical, administrative, and regulatory functions rather than being treated as separate activities. Policymakers should provide clearer sector-specific guidance for translating data-protection obligations into practical cybersecurity controls for smart-city infrastructure. The study also implies that regular employee training, risk assessments, third-party security evaluation, and continuous compliance monitoring are necessary to address evolving cyber threats. Academically, the findings contribute to the emerging literature by demonstrating the importance of integrating engineering controls with data-protection governance, while practically, the proposed approach can assist smart-city stakeholders in improving cybersecurity resilience, protecting citizens' personal information, strengthening regulatory compliance, and increasing public trust in digitally enabled urban services..

REFERENCE

- Kim, K., Alshenaifi, I. M., Ramachandran, S., Kim, J., Zia, T., & Almorjan, A. (2023). Cybersecurity and Cyber Forensics for Smart Cities: A Comprehensive Literature Review and Survey. *Sensors*, 23, 3681.
- Federated learning in smart cities: Privacy and security survey. (2023). *Information Sciences*, 632, 833–857.
- Security, trust and privacy risks, responses, and solutions for high-speed smart cities networks: A systematic literature review. (2023). *Journal of King Saud University – Computer and Information Sciences*, 35, 101788.
- Alabsi, M. I., & Gill, A. Q. (2024/2025). A Systematic Review of Personal Information Sharing in Smart Cities: Risks, Impacts, and Controls. *Journal of the Knowledge Economy*, 16, 5143–5182.

5. Joyce, A., & Javidroozi, V. (2024). Smart city development: Data sharing vs. data protection legislations. *Cities*, 148, 104859.
6. Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework. (2024). *Applied Sciences*, 14, 5501.
7. Jin, Y., & Wang, Y. (2025). Reassessing smart city development and personal data protection: A regulatory framework. *International Review of Economics & Finance*, 99, 104022.
8. Enhancing cybersecurity in smart and cognitive cities: A systematic mapping of AI-based techniques. (2025). *Array*, 28, 100606.
9. Islam, R., Bose, R., Roy, S., et al. (2025). Decentralized trust framework for smart cities: a blockchain-enabled cybersecurity and data integrity model. *Scientific Reports*, 15, 23454.
10. Cybersecurity and Regulatory Compliance in Smart Cities: A Comprehensive Review. (2026). *Smart Cities*, 9(5), 76.
11. Building security and resilience: a guide to implementing effective cybersecurity and data protection measures in smart cities. (2026). *Smart and Sustainable Built Environment*, 15(2), 908–937.
12. Joshi, S., Baviskar, A., & Rajmane, S. (2026). A review of cybersecurity in smart cities and intelligent transport systems. *Discover Internet of Things*, 6, 41.
13. Biyani, S., & Wimmer, M. A. (2026). Data Trusts in Smart Cities: Secure and Redacted Data Sharing. *Datenbank-Spektrum...*