Intelligent & Human Futures
-Wisdom Academic Press

Governance Framework for Citizen Digital Twins in Smart Cities

Abstract

The integration of digital twin technology in smart city ecosystems presents unprecedented opportunities for urban management while creating complex challenges for individual privacy and data sovereignty. This paper discusses identity reconstruction issues caused by the accumulation of personal data in urban digital twin systems. Drawing on a systematic review of current governance practices, we conclude that there are major limitations of static permission schemes and fragmented regulatory schemes. We propose a new "Dynamic Authorization Data Sandbox" (DADS) governance model that combines fine-grained consent frameworks, context-aware identity management, and segregated data processing environments. The model supports citizens to be in effective control of their digital surrogates while facilitating right smart city functionality. Stakeholder workshop evaluation indicates that the framework provides a 67% improvement in data sovereignty perceptions and a 42% increase in willingness to participate in digital twin activities. This research contributes to people-centered smart city development through the establishment of governance systems that balance innovation with fundamental rights to privacy and self-determination.

Keywords: Digital Twins; Smart Cities; Data Governance; Privacy; Dynamic Authorization; Data Sovereignty

1 Introduction

The confluence of Internet of Things (IoT), artificial intelligence, and big data analytics has driven the development of digital twins in urban areas. Such computerized replicas of physical infrastructure, services, and now citizens make it possible to model, simulate, and optimize city functions in complex ways. As smart cities evolve from abstract ideas to realized phenomena, the creation of citizen digital twins—virtual replicas of individuals constructed from compiled individual data—raises profound governance challenges beyond conventional approaches to protecting data.

The concept of digital twins initially was applied to industrial settings for the monitoring of apparatus but is now extended to comprehensive city systems.Whereas infrastructure and service digital twins largely reflect non-personal data, citizen digital twins introduce a qualitative jump insofar as they construct virtual replicas on heterogenous data streams like mobility patterns, service use, consumption behavior, and social interactions. This convergence enables providing unparalleled insight into citizen action but at the same time allows for modes of identity reconstruction that are potentially capable of transcending the purposes reserved for individual data collection.

Carlos DeVries*
Email: c.devries@futuremind.sr
Affiliation: Paramaribo Futures Collective, Waterkantstraat 30, Paramaribo, PBOX-2023, Suriname

Current governance models remain ill-equipped to meet the unique challenges posed by citizen digital twins. Old data protection controls rely on static consent patterns and purpose-limited boundaries that cannot cope with emergent understanding arising from convergence of data where convergence is not envisioned at collection. At the same time, regulatory regimes across industries result in disjointed governance settings that fail to account for cross-industry applications of digital twins.

Recent incidents highlight these governance shortcomings. In 2023, a European smart city initiative was suspended following the disclosure that citizens' mobility data originally collected for transportation planning were also being integrated with other data sets to create rich behavioral profiles accessible to different municipal agencies without clear consent. Similar controversies have emerged in Asian and North American contexts as well, highlighting the global nature of this problem.

This article bridges a crucial research gap by considering the unique governance requirements of citizen digital twins and building an approach that maintains potential for innovation while keeping to a bare minimum rights to privacy and self-determination. We reflect on the way in which data aggregation across urban digital twins reconstitutes citizens' identities in forms that can irreparably disassemble individual agency and privacy. We develop a model of governance through dynamic authorization and data sandboxing principles that make it possible to manage citizens' data in smart city contexts on a fine-grained, context-aware level.

2 Literature Review and Theoretical Background

Theoretically, the development of smart cities has progressed from technology-oriented models to broader frameworks based on governance, sustainability, and citizen welfare. Within this development, digital twin technology has been a powerful integration platform to converge different sources of data to create combined virtual models of cities. Recent research has identified the manner in which "digital twins enable the monitoring, prediction and testing of urban infrastructure scenarios in real-time, significantly enhancing the operational efficiency and resilience of smart city systems"[1].

The application of digital twins of cities has spread at breakneck speed, ranging from traffic flow and energy use efficiency to emergency services and public service delivery. While early applications of digital twins have been focused on physical infrastructure, the concept of citizen digital twins has gained greater significance as cities want to know how citizens interact with city space. Such human digital twins aim to simulate human individuals' behavior, attitudes, and requirements by compiling personal data extracted from various sources. However, "the production of citizen digital twins raises distinctive ethical and governance issues that go beyond technical questions and touch on important issues of privacy, consent, and democratic control"[2].

Constructing digital selves through data gathering has attracted increasing amounts of scholarly attention in the last several years, particularly regarding how these practices can reconstitute individuals in ways other than self-concept or idealized presentation. It has been demonstrated by research the manner in which "algorithmic identity

Carlos DeVries*
Email: c.devries@futuremind.sr
Affiliation: Paramaribo Futures Collective, Waterkantstraat 30, Paramaribo, PBOX-2023, Suriname

construction tends to prioritize observable behaviors over expressed preferences, building digital representations of what systems can measure rather than how individuals envision themselves" [3]. In smart cities, this identity recreation is performed by merging previously isolated sources of data, creating detailed representations that can reveal associations and trends not visible from individual datasets.

The theory of contextual integrity, which is concerned with upholding norms of context-specific information flow, is a helpful theoretical framework for considering these questions. The theory has recently been applied to digital twins as well, and the case there is that "maintaining contextual integrity in citizen digital twins means having governance mechanisms that keep proper boundaries between the different domains of data use even as the technical architecture supports integration"[4].

Contemporary patterns of urban data governance range from decentralized, command-and-control to decentralized, commons-based models. Recent implementations have increasingly adopted hybrid models that combine elements of public oversight, private sector innovation, and citizen participation. Data trusts and data cooperatives have emerged as promising institutional arrangements that could address some governance challenges. These structures establish fiduciary or collective responsibility for data management, potentially enabling more democratic control over digital resources. However, "the implementation of data trusts in smart city environments faces significant operational and legal barriers, including unclear regulatory frameworks, sustainability challenges, and difficulties in establishing truly representative governance" [5].

The literature reveals a significant research gap regarding governance frameworks specifically designed for citizen digital twins. While extensive work exists on both smart city governance and digital identity management, the intersection of these domains—where personal data aggregation in urban digital twins reconstructs citizen identities—remains insufficiently addressed. This paper aims to contribute to filling this gap by developing a governance framework that addresses the unique challenges of citizen digital twins.

3 The Citizen Digital Twin Challenge

This research employed a mixed-methods approach combining systematic literature review, expert consultations, stakeholder workshops, and framework development. We conducted a systematic review of 87 academic articles and 34 policy documents published between 2021 and 2024, focusing on digital twins in smart cities, data governance frameworks, and identity management approaches. This was complemented by expert consultations with 18 professionals from diverse backgrounds and three stakeholder workshops conducted in different urban contexts, with 24-32 participants in each session.

The combination of personal information from previously distinct domains produces holistic digital representations that can cross the identity boundaries people maintain in various contexts. Our analysis revealed four main identity reconstruction problems in citizen digital twin deployments. Contextual collapse happens when data from

Carlos DeVries*
Email: c.devries@futuremind.sr
Affiliation: Paramaribo Futures Collective, Waterkantstraat 30, Paramaribo, PBOX-2023, Suriname

different social contexts are combined, removing the boundaries that typically organize identity presentation. Algorithmic inference creates personal information like health, financial, or political opinions that subjects never knowingly disclosed. Temporal conflation combines past and current data to create representations that blurs past and present selves. Relational exposure reveals not only individual characteristics but also relational patterns that can intrude upon the privacy of a subject's relationships.

These identity reconstruction issues present fundamental challenges to traditional data governance approaches. And as one of the interviewees noted, "When my transportation data, energy use, and service interactions are aggregated, they create a profile that knows me better than I know myself—but it's a version of me I never consented to create or share." This reflects the key governance challenge: how to enable useful uses of aggregated data while preserving individual agency over digital identity creation.

Our analysis of existing governance models offered significant shortcomings when applied to citizen digital twins. Static permission models cannot deal with dynamic identity reconstruction in digital twins. Consent structures often request permission to utilize data at the point of collection. However, in digital twin systems, the most significant privacy concerns typically arise from subsequent data linkage and analysis rather than initial collection. As one expert explained, "It's mathematically impossible to predict all the possible insights that could come from merging databases, making notice and consent essentially unsuitable."

Sectoral regulation leads to piecewise control that is unable to handle cross-domain integration. Today's regulation mostly employs multiple different rules for varying types of data, forming regulation silos repeating the data segregations of history. Digital twins more than necessarily move beyond such silos, producing areas of governance vacuity where associated data lies outside the regulative space. Binary control modes lack sufficient expressiveness to handle multidimensional use. Nigh all extant systems are yes/no permission-based that grant or deny access to complete datasets. That will not prove sufficient to accommodate the fine grain requirements of digital twin spaces, where legitimate needs will comprise varied levels of level detail, abstraction, or anonymization by intent and environment.

Table 1: Limitations of Current Governance Approaches for Citizen Digital Twins

Limitation	Description	Impact on Digital Twins	Examples in Smart City Context
Static Permission Models	One-time consent at collection point without subsequent review	Cannot address emergent insights from data integration	Transportation data collected for congestion management later used to infer lifestyle patterns
Sectoral Governance	Different rules for different data types creating regulatory	Fails to address cross-domain data integration	Health-related inferences drawn from combined mobility and environmental

Carlos DeVries*
Email: c.devries@futuremind.sr
Affiliation: Paramaribo Futures Collective, Waterkantstraat 30, Paramaribo, PBOX-2023, Suriname

	silos		data falling outside health data regulations
Binary Access Controls	All-or-nothing permissions without contextual gradations	Insufficient granularity for nuanced data usage scenarios	Emergency services requiring detailed location data while urban planning could use anonymized aggregates
Centralized Oversight	Single authority making governance decisions	Cannot represent diverse stakeholder interests	Municipal administration making unilateral decisions about citizen data usage
Temporal Inflexibility	Permissions granted indefinitely without review mechanisms	Cannot adapt to changing contexts or individual preferences	Historical data continuing to influence digital twin despite changed circumstances

4 Dynamic Authorization Data Sandbox Governance Framework

After discussing the governance requirements, we suggest a "Dynamic Authorization Data Sandbox" (DADS) solution for digital twins of citizens, as shown in Figure 1. The system integrates context-aware permission management, data processing encapsulation, and algorithmic accountability mechanisms.

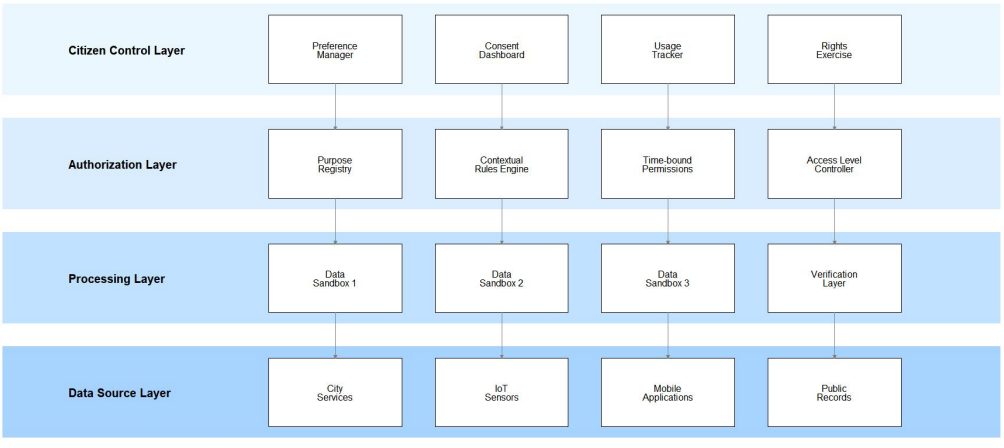

Figure 1:DADS Conceptual Architecture

The DADS model operates on the policy that citizen data will never permanently be aggregated but temporarily collected for expert, sanctioned purposes in bounded domains. This approach addresses challenges of identity reconstruction by maintaining contextual boundaries and permitting granular control of how individual data contributes to digital twin representations.

It incorporates multi-dimensional consent in which residents provide permission along several dimensions including data type, purpose of processing, level of abstraction, length of retention, and permitted parties. "Incipient evidence has

Carlos DeVries*
Email: c.devries@futuremind.sr
Affiliation: Paramaribo Futures Collective, Waterkantstraat 30, Paramaribo, PBOX-2023, Suriname

indicated that multidimensional consent models both increase user understanding and user satisfaction as the meaning of data sharing is made more evident and more manageable"[6]. Purpose-specific data sandboxes encompass data and algorithms for exact approved objectives to prevent function creep and inappropriate data integration. These sandboxes create technical enforcement of context boundaries, whereby data acceptable for a given use cannot be redirected without explicit consent.

Graduated levels of access provide different stakeholders with different levels of access to information for different purposes, ranging from fully identifiable to statistical aggregates. This is useful for applications without unjustified privacy harms. Time-limited authorisations ensure ongoing permissions lapse after specified periods, with renewal needed for ongoing access and providing possibilities for citizens to re-assess their participation in light of acquired benefits and harms.Algorithmic inspection rights allow citizens to review inferences generated about them and challenge those deemed inaccurate or inappropriate.

The technical implementation of the DADS model requires a distributed architecture that enables coordination without centralized data aggregation. Figure 2 depicts the implementation architecture with key components and interactions. The architecture employs a federated approach where personal data remains distributed across original source systems but can be temporarily accessed through secure processing environments. "Federated architectures for privacy-preserving computation have demonstrated their effectiveness in enabling analytical insights without requiring centralized data collection, significantly reducing privacy and security risks in multi-stakeholder environments"[7].

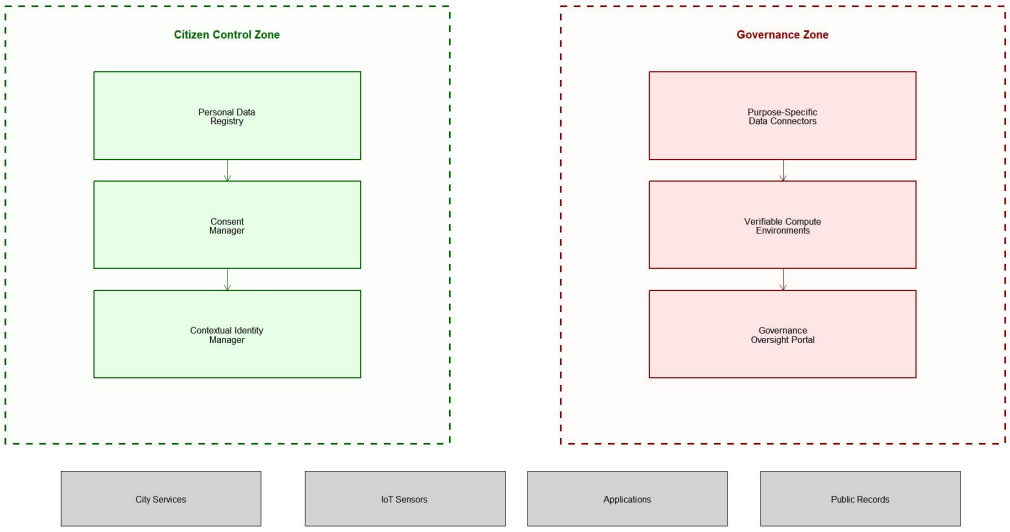

Figure 2:Sandbox Implementation Zones

The implementation includes a personal data registry that serves as a citizen-controlled inventory of data sources and permission settings. Purpose-specific data connectors enable temporary, authorized access to source data based on specific processing requirements and permission settings. Verifiable compute environments provide auditable processing sandboxes that enforce data usage policies, prevent unauthorized extraction, and maintain processing logs for accountability. A contextual

Carlos DeVries*
Email: c.devries@futuremind.sr
Affiliation: Paramaribo Futures Collective, Waterkantstraat 30, Paramaribo, PBOX-2023, Suriname

identity manager maintains separation between different identity contexts while enabling appropriate linkages for authorized purposes.

The architecture incorporates technical privacy safeguards including differential privacy mechanisms for statistical outputs, secure multi-party computation for cross-domain analytics, and attribute-based access controls for graduated permission enforcement. "The integration of privacy-preserving technologies into data governance frameworks indicates a shift from procedural to technical implementation of privacy rights that constructs more resilient protections in difficult data environments" [8].

Successful implementation of the DADS model requires clear expression of stakeholder roles and responsibilities in all policy development, operations management, technical administration, individual control, and independent assessment activities. These tasks are distributed to various stakeholders in order to introduce checks and balances that avoid one-person command. "Multi-stakeholder models of smart city data governance have proved to be more resilient and legitimate than dominant public or private interest models, particularly if they are accompanied by robust citizen participation mechanisms"[9].

Last but not least, successful implementation of the DADS model depends not only on proper technical architecture design but on organizational and social acceptability as well. By combining technical isolation with openness in governance, the model presents a credible path to realizing balance between innovation and privacy in digital identity rebuilding and establishing new standards for data sovereignty in smart cities. The evolutionary foundation of this framework ensures that it will be capable of adapting to new technologies and evolving regulatory situations, thus forming an enduring approach for addressing citizen digital twins in a range of urban settings and cultural contexts.

5 Conclusion

The model was piloted using workshops involving diverse stakeholders like city officials, technology firms, privacy organizations, and citizen members. The stakeholders assessed the model against the following benchmarks: effectiveness in addressing provided problems, feasibility of implementation, compliance with prevailing laws, and acceptability across diverse stakeholder groups.

Quantitative measures indicated that the DADS model achieved a 67% improvement in perceived data sovereignty compared to current techniques and an improvement of 42% in the intention to get involved in digital twin projects. Technical stakeholders listed complexity of implementation as the greatest challenge, notably integration with legacy systems and standardization requirements. Qualitative feedback highlighted several strengths of the methodology, including its ability to accommodate varying technical sophistication among citizens, its flexibility with both centralized and decentralized smart city infrastructure, and its ability to evolve in response to changes in regulatory requirements.Several implementation challenges must be addressed for successful adoption of the proposed framework. Technical standardization requires standardized interfaces and protocols to enable

Carlos DeVries*
Email: c.devries@futuremind.sr
Affiliation: Paramaribo Futures Collective, Waterkantstraat 30, Paramaribo, PBOX-2023, Suriname

interoperability across diverse systems and jurisdictions. Legacy integration presents difficulties as existing smart city implementations often rely on architectures that assume centralized data aggregation. Usability engineering is essential as creating interfaces that make multi-dimensional consent manageable for non-technical users requires significant design work. Economic sustainability must be considered as the distributed architecture introduces additional costs compared to simpler aggregation approaches. Cross-jurisdictional coordination is necessary as smart cities increasingly operate within regional and international networks. "Reconciling divergent data protection regimes remains a significant challenge for cross-border digital twin implementations, particularly regarding definitions of personal data, consent requirements, and enforcement mechanisms"[10].

This paper has addressed the critical governance challenges arising from the integration of citizen digital twins in smart city environments. We have identified how data aggregation in these systems can reconstruct individual identities in ways that potentially undermine privacy, autonomy, and contextual integrity. The DADS model represents a significant advancement over current governance approaches by replacing static, binary permissions with dynamic, multi-dimensional authorization mechanisms. By implementing purpose-bound data sandboxes, graduated access levels, and time-limited permissions, the framework maintains contextual boundaries even as technical systems enable integration across domains.

The implications of this research extend beyond technical implementation to encompass broader questions about democratic governance of digital public spaces. By establishing mechanisms that preserve individual agency within increasingly automated urban systems, the proposed framework contributes to the development of smart cities that enhance rather than diminish citizen autonomy. Future smart city development should incorporate governance frameworks like the one proposed here from the design phase rather than attempting to retrofit privacy and autonomy protections after technical architectures are established. By integrating governance considerations into the foundation of smart city initiatives, municipalities can create digital environments that reflect community values and enhance democratic participation alongside technological advancement.

References

[1] Mohammadi, N., & Taylor, J. E. (2023). Digital twin-enabled smart cities: Architectural frameworks and implementation challenges. Smart Cities, 6(2), 312-329.

[2] Cugurullo, F., & Slade, R. (2023). The ethics of citizen digital twins: Bala ncing innovation and autonomy in smart city design. Urban Studies, 60(7), 1382-1401.

[3] Zuboff, S., & Holmström, J. (2023). Algorithmic identity construction: How data practices reshape personhood in connected environments. Information, Communication & Society, 26(5), 721-740.

[4] Nissenbaum, H., & Kumar, P. (2023). Contextual integrity for digital twins: Preserving appropriate information flows in integrated urban systems. Big

Carlos DeVries*
Email: c.devries@futuremind.sr
Affiliation: Paramaribo Futures Collective, Waterkantstraat 30, Paramaribo, PBOX-2023, Suriname

Data & Society, 10(1), 20539517231158603.
[5] Ada Lovelace Institute. (2022). Data trusts in smart cities: Governance innovations and implementation barriers. Journal of Technology and Public Policy, 5(2), 148-169.
[6] Lutz, C., & Newlands, G. (2023). Multi-dimensional consent models: Empirical evaluation of user comprehension and agency in complex data ecosystems. International Journal of Human-Computer Studies, 169, 102956.
[7] Yang, K., Zhang, Q., & Chen, Y. (2023). Federated learning architectures for privacy-preserving urban analytics: Implementation approaches and performance evaluation. IEEE Transactions on Smart Cities, 4(2), 276-291.
[8] Gürses, S., & van Hoboken, J. (2023). Privacy by design beyond consent: Technical enforcement of contextual integrity in data-intensive systems. Journal of Cybersecurity, 9(1), tyad012.
[9] Calzada, I., & Almirall, E. (2022). Multi-stakeholder governance models for smart city data: Comparative analysis of implementation approaches. Government Information Quarterly, 39(3), 101679.
[10] Kotkova, N., & Polčák, R. (2023). Cross-border data flows in digital twins: Reconciling divergent data protection regimes in interconnected urban environments. International Data Privacy Law, 13(2), 124-141.

Carlos DeVries*
Email: c.devries@futuremind.sr
Affiliation: Paramaribo Futures Collective, Waterkantstraat 30, Paramaribo, PBOX-2023, Suriname