INFOMANIA: THE RESEARCH JOURNAL
Volume 2, Issue 1, January - February 2026
https://infomaniajournal.com **ISSN:3108-0006**

Securing Smart Traffic Control Systems: Cloud Data Security Trends and Emerging Solutions in Smart Cities

Sachin M. Vaidya[1]
sachin.m.vaidya@gmail.com[1]
Research Student of Computer Engineering, Pillai College of engineering, Panvel
Navi Mumbai – 410206, Maharashtra

Shankar M. Patil [2]
smpatil2k@gmail.com [2]
Professor of Computer Engineering, Smt Indira Gandhi College of engineering,
Navi Mumbai – 400701, Maharashtra

Abstract

Cloud computing has increasingly been used to support data-driven services for healthcare, transportation, energy and governance in smart cities. The scale-out, efficiency of cloud computing can provide the user with a power to do real-time analytics, and make smart decision; in-order to achieve this purpose that presents serious challenge when it comes to confidentially, privacy, integrity and data resiliency. In this paper, we survey the recent developments on secure cloud data in smart cities. I also mention a few of those researchers and the papers, such as: smart city security framework, IoT & cloud integration, mobile cloud threats, SCADA next-gen migration and 6G-enabled audit. POST-CATEGORIES: pentest-mgmt.

Comparative analysis also finds some remaining research blocks in policy-aware cryptography, verifiability auditing and resilient city-scale infrastructures. The chapter concludes with a summary of future research directions to enhance the security and transparency from the cloud-based smart cities.

Keywords: Smart Cities, Cloud Security, Data Privacy, Zero-Trust, Edge Computing, Homomorphic Encryption, SCADA, 6G.

I Introduction

What is a “Smart” city? A smart city means an urban area that links internet of thing devices as well as sensors and ICT systems together in order to make the services more effective such as energy-distribution, traffic-management, health-care and citizen-services. In such a setting, cloud computing acts as an underlying backbone offering elastic storage scale and scaling analytics with real-time decision support [1].

But the increasing reliance on the cloud offers crucial attack surface. While citizen data, ICS and mobility logs often traverse multi-tenant cloud ecosystems and are prone to insider threats, unauthorized access, intrusion as well as regulatory non-compliant threats [2][3]. As cities continue to advance toward hyper-connected environments, securing data privacy integrity and availability is increasingly critical for urban authorities.

Cloud technology has been introduced to the smart city, which can realize real-time data processing, service integration everywhere and resource optimization. From traffic management to public health and safety, cloud infrastructures serve as the backbone for practically all urban intelligence initiatives [4]. However, continued issues such as cyber security and privacy threats, interoperability problems, and trust management compel our awareness [5]. Recent work highlights hybrid security strategies, privacy-by-design model options, and resilient encryption techniques [6][8]

II. Literature Review

Smart cities combine cloud-computing with IoT and new technologies to improve governance, mobility, healthcare and energy use. Although such systems facilitate data-driven services, they also give rise to various risks in terms of confidentiality, integrity, and availability. Rosadi et al. [2] identified governance vacuums, insider threats and interoperability problems by means of a Smart City Interaction Framework and Energy Reports [4] emphasized the fact that ICT infrastructure can be subject to failure due cyber-security issues and lack of performance with respect to data leakage.

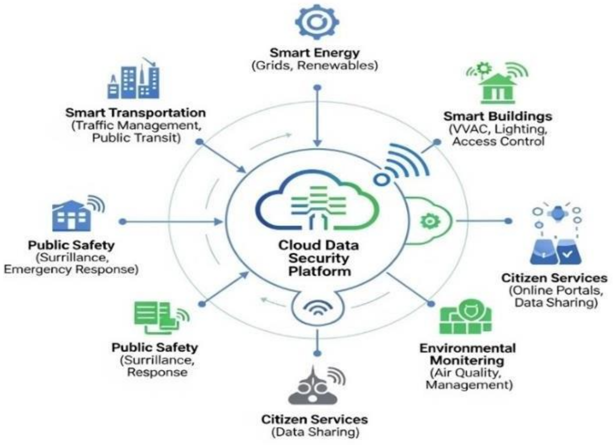


Figure 1.1. Cloud Data Security Platform in Smart Cities

Blockchain has become a cornerstone of transparency and trust. Majeed et al. [1] reviewed the integration of blockchain and IoT, cited its merits in decentralization, while expressing concerns about scalability. Rejeb et al. [8] supported the increase in blockchain adoption from smart city applications, whereas Sharma and Park [20] studied smart contracts with a focus on automation but hindered by contract immutability risks. Khanna and Sharma [6] suggested blockchain–cloud integration patterns for scalability and audit. Together, these studies demonstrate the role of blockchain in creating a responsible and tamper-resistant environment

Privacy and governance models are just as important. Zhang et al. [6] also proposed trust–privacy models, but did not offer real-time encryption procedures. Rizi et al. [7] reviewed privacy enhancing technologies (PETs), and advocated stack-based in several modules between fog, edge and cloud. The Law and Mobility Journal [8] follows these with a discussion of GDPR compliance and data sovereignty, highlighting the separations between technical solution design and policy enforcement. These findings emphasise that sustainable urban services depend on PET adoption and governance-led monitoring.

Artificial intelligence is transforming the face of smart city cybersecurity. Gupta et al. combined blockchain assisted AD to improve IoT security, meanwhile, the integration complexity still exists. Demertzi et al. [21] plotted security threats against mobility, healthcare and energy sectors suggesting intrusion detection for the sector. These analyses present AI as a critical driver of agile, sector-oriented defence.

The convergence of clouds and IoT: A survey Recently, as the enabling technologies The potential to converge among cloud computing and IoT have been became available for developing solutions for future 1. Tahirkheli et al. [3] have pointed out security weaknesses in virtualization and trust management, Bhardwaj et al. [5] found an unequal worldwide acceptance through a bibliometric study. Trigka and Dritsas [12] introduced cloud–edge coordination to minimize the latency, while Songhorabadi et al. [17] focused on fog computing to achieve distributed resilience. By combining these techniques, that would improve scalability but would deserve orchestrating challenges.

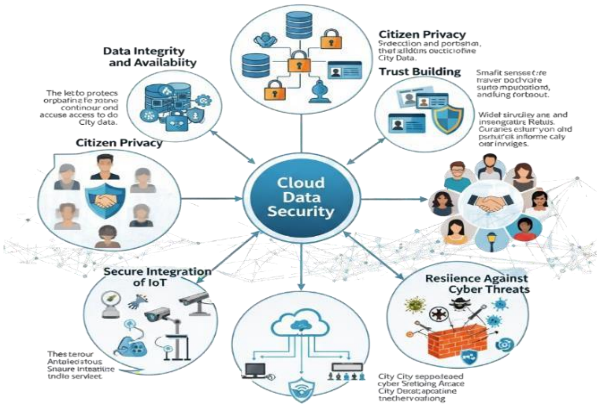
Critical infrastructures remain exposed. SCADA security vulnerabilities were brought to attention in moving to the ESMDI Energies cameos [5]. Guan et al. [19] presented CP-ABE with secret sharing for compatible health data telemetry, and Rasori et al. [18] proposed ABE-Cities for fine-grained access control. Sookhak et al. [14] presented a classification of composite defences.

Finally, hardware-level risks persist. Kocher et al. [16] revealed speculative executon attacks on confidentiality and Rani et al. [13] highlighted real-world deployment barriers. The preprint Security and the Smart City [15] consolidated a number of emergent paradigms, but reported minimal usage. In sum, literature [1][21] demonstrates that smart city security requires a convergence of blockchain, PETs, AI, cloud–edge orchestration, and governance. Persistent challenges scalability, hardware vulnerabilities, and fragmented deployment—demand continued innovation and cross-domain collaboration.

Author(s), Year	Focus Area	Key Contribution	Security/Privacy Limitation	Recent Trends	Roles in Smart Cities	Challenges	Emerging Solutions
Majeed et al., 2021 [1]	Blockchain for IoT-based Smart Cities	Reviewed blockchain integration with IoT in smart cities.	Scalability and interoperability challenges.	Blockchain-IoT fusion, consensus protocols	Trust models for urban IoT	Blockchain overhead, device constraints	Lightweight consensus, sharding, hybrid blockchain
Zhang et al., 2023 [6]	Trust and Privacy	Proposed trust-privacy for sustainable smart cities.	Did not address real-time encryption methods.	Trust-aware computing, privacy scoring	Citizen trust in services	Dynamic privacy enforcement	ECC-based encryption, trust-privacy fusion models
Gupta et al., 2022 [11]	AI + Blockchain for IoT Security	Systematic review of PETs like anonymization	Integration complexity, resource constraints.	AI-blockchain hybrids, federated learning	Enhanced IoT anomaly detection	Model poisoning, energy overhead	Lightweight federated AI with on-chain verification
Rizi & Seno, 2022 [7]	Privacy-Enhancing Technologies (PETs)	resilient ecosystems using fog SDN.	Weak integration with IoT-cloud ecosystems.	PETs for edge and federated analytics	Data protection in distributed systems	Fragmentation of PET deployments	Modular PET stacks for fog/edge/cloud
Kumar et al., 2023 [10]	Fog, SDN, NFV, MEC	ABE for fine-grained smart city access control.	Scalability challenges.	Edge-native orchestration	Real-time edge resilience	Resource constraints	Microservices and adaptive load balancing
Rasori et al., 2018 [18]	Attribute-Based Encryption (ABE-Cities)	Combined CP-ABE with secret sharing for secure telemetry.	Overhead in key management.	Policy-based ABE	Role-based access for urban sensing	Key revocation, distribution	Proxy re-encryption, hierarchical ABE
Guan et al., 2018 [19]	Secure IoT/Smart Grid Data Acquisition	hardware vulnerabilities impacting confidentiality.	Prototype; city-scale not tested.	CP-ABE + secret sharing	Critical infrastructure telemetry	Communication overhead	Aggregation-friendly encryption
Kocher et al., 2020 [16]	Speculative Execution (Spectre)	secure automation of services via contracts	Difficult to mitigate quickly.	Hardware/runtime mitigations	Security for cloud processors	Legacy hardware exposure	Microcode, compiler mitigations
Sharma & Park, 2021 [20]	Blockchain Smart Contracts	Mapped threats across mobility, healthcare, energy domains.	Scalability and contract vulnerabilities.	Hybrid blockchain models	Automated governance	Gas costs, immutability	Permissioned contracts, formal verification
Demertzi et al., 2022 [21]	Domain-wise Threat Mapping		Some claims unverified (preprint).	Domain-aware IDS, cross-domain analysis	Sector-specific security	Cross-domain dependencies	Integrated domain-specific defences

Table 2.1 Comparative Review of Cloud Data Security in Smart Cities

III. Roles of Cloud Data Security in Smart Cities


Data Integrity and Availabiity
The let to protecs orpbafinz feratne continour ond accuse access to do City data.
Citizen Privacy
Srdecction and porbshon, thet alldins oecticiofwe City Data.
Trust Building
Smafit sensset:re traver poclvote surte mpuoatiord, andlung fortsout.
Widet sirvciley ane and insengcatire Retuis. Curanes esturr yon olrd psrhut'ek informe caly oar invdges.
Citizen Privacy
Cloud Data Security
Secure Integration of IoT
Thes terour Antaledstous Snaure intbatiire tndle servleet
Resiience Against Cyber Threats
City City seppoteaed cyber Sretioing Arcace City Decat; apoatine tnethervoationg

. **Figure 3.1:** Roles of Cloud Data Security in Smart Cities

Ensuring cloud data security underpins the trust, privacy and resilience within smart city infrastructures. It maintains the integrity and availability of information for vital services like healthcare, transportation, energy [1], [2] to citizen privacy via privacy-enhancing technologies and compliance frameworks [6], [8]. Trustworhy infrastructures make also use of Trust among citizens, governments and service providers (encouraging take up of digital services) [6]. Furthermore, cloud security facilitates a secure interoperation of the IoT ecosystems by encryption, blockchain and secured communication protocols[9]

Finally, it strengthens resilience against cyber threats like ransomware, DoS, and advanced persistent threats by leveraging AI-driven detection, intrusion prevention, and zero-trust models [5], [10].

IV. Challenges in Cloud Data Security for Smart Cities

Despite advances in technology, smart city environments still face serious security and privacy vulnerabilities. Low-level anonymization techniques and unsecure storage models can cause unauthorized access and data abuse[3], [7], [13]. Scalability challenges also make intrusion detection systems infeasible; many of IDS models have a high latency and and/or low accuracy which are not applicable to widespread IoT deployments [5], [17].

Inter-operability represents another significant problem since heterogeneous IoT devices and cloud platforms use conflicting protocols and standards [2], [8]. The resulting inconsistency undermines trust establishment and policy enforcement. Legacy OT systems, i.e., SCADA cannot represent or have been designed for cloud integration and consequently their migration into the cloud may suffer from denial-of-service, replay and insider threats [5], [14].

Moreover, solutions based on privacy-preserving deep learning also seem appealing but present prohibitive costs and scalability challenges when being deployed in distributed IoT systems [11]. At the technology level, threat such as spec- tative execution attacks (e.g., Spectre) can be leveraged on cloud processors at hardware level, leading to con- fidentiality breach [16]. Recent post- quantum challenges also increase the pressure of the existence of quantum-safe security models [19]. Last but not the least, governance and legal nuances such as lax GDPR enforcement and stringent data sovereignty make it difficult to ensure compliance [8]

.VI. Emerging Solutions

In order to address the challenges described above, scholars and policy makers have come up with various creative solutions:

In order to solve the problems that troubled cloud-based smart cities, some emerging technologies have been introduced in recent study.

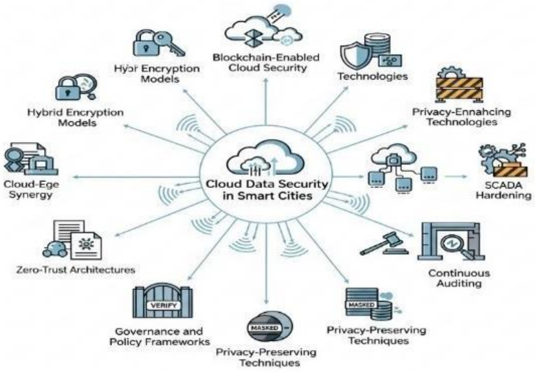

Hybr Encryption Models
Blockchain-Enabled Cloud Security
Technologies
Hybrid Encryption Models
Privacy-Ennahcing Technologies
Cloud-Ege Synergy
Cloud Data Security in Smart Cities
SCADA Hardening
Zero-Trust Architectures
Continuous Auditing
VERIFY
Governance and Policy Frameworks
MASKED
Privacy-Preserving Techniques
MASKED
Privacy-Preserving Techniques

Figure 6.1: Emerging Solutions for cloud data security in Smart cities

Blockchain technology has been extensively utilized in setting up trust, transparency and auditability in decentralized systems [1], [6], [8], [20]. Pooling decentralized consensus with immutable ledgers, blockchain promotes accountability, not to deny the scalability concerns. Related to this, AI-based approaches such as anomaly detection enhance the resiliency of a system by providing support for real time discovery of malicious traffic [11]. When combined with blockchain, AI delivers predictive analytics and irrefutable verification.

In doing so, privacy-enhancing technologies (PETs) can contribute to fostering good faith in citizens. Fine-grained access control and secure telemetry are supported by techniques including attribute-based encryption (ABE) [7], secret sharing [18, 19]. At the infrastructure level, fog and edge computing address latency by offloading processing from clouds to devices, which brings with it a degree of resilience [10], [12], [17]. These architectures push routing closer to user's mission, reducing single points of failure.

Federated learning has been emerging as a remedy for centralization threats, making it possible to train models together without disclosing raw data [11]. Concurrently, domain-aware detection mechanisms customize defense systems for specific sectors like healthcare, energy or mobility [21]. Lastly, intermediate steps to guarantee alignment with citizen rights are achieved in a multi-part chain including hybrid encryption, differential privacy, zero-trust architectures [3], [4], and governance automation [8].

SMART Traffic Control System (SMART Traffic Signal in Smart Cities)

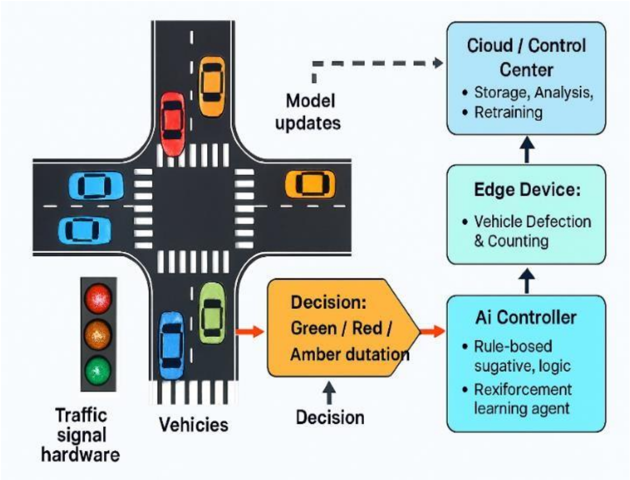


Figure 6.1: Emerging Solutions for cloud data security in Smart cities

Speed Limiting: CCIS apply radar sensor to acquire over speed vehicle. Notifications come on the phone when limits are violated, and e-challans/fines mark the rule breaking.

Motion-Activated Pedestrian Safety: Crosswalks with motion sensitive crossing signs and timers. Signals give priority to safe crossing when pedestrians are detected and CCTV cameras. ensure penalties for vehicles who do not respect the rule of pedestrian precedence in force.

Acts Responsive and Dynamic Management of Signalized intersections: Green time and red time are controlled automatically in real-time according to the traffic flow volume& queue length. Vehicles that jump signals or block junctions are recorded by the system and fines are sent out via Automatic Number Plate Recognition (ANPR).

Response Priority Emergency Vehicle Fast-: When ambulances, fire trucks or police vehicles are detected the system forms a rapid green-light corridor. At the same time, cars occupying emergency lanes are monitored and their drivers fined to preserve clear access for emergency personnel.

Time-bound optimization: Each decision (change in signal, activation of pedestrian button, emergency pre-emption) is a time-bound process functioning at second level response windows. Vehicles that cause delays, or violate any rules are documented, with fines implemented to ensure the flow of traffic remains smooth and fluid.

VII Conclusion

Cloud Data Security is the key method in developing and sustaining reliable smart cities, as the federation of data will trust them while preserving their confidentiality and allowing them to provide efficient services. The literature 1 mentions encryption, blockchain, (AI) (PETs), and governance frameworks as building blocks for the development of future solutions. Blockchain establishes transparency and auditability 1[20] and AI-based anomaly detection is a tool for defending against ever changing threats [11]. Fine-grained access control is enforced by PETs such as attribute based encryption and secret sharing [7] 18 while the governance provides guarantees with respect to regulation and ethics issues [8].

Nevertheless, persistent challenges remain. Adoption is severely restricted by scalability and interoperability issues 3, while trust is compromised by hardware vulnerabilities in for example, speculative execution [16]. Additionally, the fragmented legal Cloud Data Security is considered as a prime process in building and supporting feasible smart cities because data federations could rely on them such that their privacy may not be invaded for effective services to be provided. [19] real-world AI–blockchain implementations [11] domain-specific defense mechanisms models [21], and common pilot frameworks [13].By integrating innovation with governance, smart cities can evolve into transparent, adaptive, and citizen-centric ecosystems.

References

[1] U. Majeed, M. A. Khan, and A. Rehman, “Blockchain for IoT-based smart cities: Recent advances, challenges, and a roadmap,” *Computer Communications*, vol. 170, pp. 116–133, 2021.
[2] E. Ismagilova, L. Hughes, Y. K. Dwivedi, and K. R. Raman, “Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework,” *Information Systems Frontiers*, vol. 22, no. 2, pp. 1–23, 2020.
[3] A. I. Tahirkheli, S. Iqbal, and M. N. Khan, “A survey on modern cloud computing security over smart environments,” *Electronics*, vol. 10, no. 15, p. 1811, 2021.
[4] C. Ma and Y. Zhang, “Smart city and cyber-security: Technologies used, leading challenges and future recommendations,” *Energy Reports*, vol. 7, pp. 7994–8003, 2021.
[5] V. Bhardwaj, N. P. Rana, and R. Islam, “Smart cities and the IoT: An in-depth analysis of global research trends and future directions,” *Discover Internet of Things*, vol. 4, no. 1, p. 12, 2024.
[6] A. Khanna and M. Sharma, “Blockchain–cloud integration: A survey,” *Future Generation Computer Systems*, vol. 130, pp. 95–110, 2022.
[7] T. Poleto, C. Costa, and A. Silveira, “Information security applications in smart cities: A survey,” *Future Internet*, vol. 15, no. 12, p. 393, 2023.
[8] A. Rejeb, K. Rejeb, and J. G. Keogh, “Blockchain technology in the smart city: A bibliometric review,” *Sustainability*, vol. 13, no. 21, p. 11840, 2021.
[9] A. Gharaibeh et al., “Smart cities: A survey on data management, security, and enabling technologies,” *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2456–2501, 2017.
[10] A. V. Dastjerdi and R. Buyya, “Mobile cloud computing: Security and privacy issues,” in *Mobile Cloud Computing*, Elsevier, 2016, pp. 153–180.
[11] R. Gupta, S. Tanwar, and R. Sharma, “Integrating blockchain with artificial intelligence to secure IoT

networks: Future trends," *Journal of Reliable Intelligent Environments*, vol. 8, no. 2, pp. 93–108, 2022.

[12] M. Trigka and E. Dritsas, "Edge and cloud computing in smart cities," *Future Internet*, vol. 17, no. 3, p. 118, 2025.

[13] S. Rani, S. Rana, and S. Jindal, "Security and privacy challenges in the deployment of smart cities," *Journal of Parallel and Distributed Computing*, vol. 170, pp. 1–14, 2022.

[14] M. Sookhak, A. Gumaei, and F. Haider, "Security and privacy of smart cities: A survey, research challenges and solutions," *Journal of Network and Computer Applications*, vol. 102, pp. 1–14, 2019.

[15] "Security and the smart city: A systematic review," *ResearchGate preprint*, 2025.

[16] P. Kocher et al., "Spectre attacks: Exploiting speculative execution," *Communications of the ACM*, vol. 63, no. 7, pp. 93–101, 2020.

[17] A. Songhorabadi, H. R. Rabiee, and M. T. Manzuri, "Fog computing approaches in smart cities: A state-of-the-art review," *arXiv preprint arXiv:2011.14732*, 2020.

[18] A. Rasori, L. Ferretti, and M. Marchetti, "ABE-Cities: An attribute-based encryption system for smart cities," *arXiv preprint arXiv:1807.11793*, 2018.

[19] Y. Guan, X. Wu, and X. Cheng, "Achieving efficient and secure data acquisition for cloud-supported IoT in smart grid," *arXiv preprint arXiv:1810.10746*, 2018.

[20] S. Sharma and J. Park, "Blockchain-based smart contracts for secure smart city applications," *IEEE Access*, vol. 9, pp. 116–133, 2021.

[21] E. Demertzi, K. Giannoutakis, and K. Kolomvatsos, "An overview of cyber threats, attacks, and countermeasures on the primary domains of smart cities," *arXiv preprint arXiv:2207.04424*, 2022.