IJIREEICE
ISSN (O) 2321-2004, ISSN (P) 2321-5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.414 ⵘ Peer-reviewed & Refereed journal ⵘ Vol. 13, Issue 11, November 2025
DOI: 10.17148/IJIREEICE.2025.131110

IoT-Based Smart Waste Management System for Smart Cities: A Synthesized Framework Addressing Security and Interoperability Challenges

Prof. Rana Afreen Sheikh[1], Rushikesh R. Gunjarkar[2], Snehal R. Nagrale[3]

Head, Department of Computer Application, Vidyabharti Mahavidyalaya, Amravati, India[1]

Student, Department of Computer Application, Vidyabharti Mahavidyalaya, Amravati, India[2,3]

Abstract: The rapid urbanization of modern cities has exacerbated the challenges of efficient waste management, leading to environmental and public health concerns. The Internet of Things (IoT) presents a transformative opportunity to create smart, data-driven waste management systems. However, the deployment of such systems is hindered by significant challenges, including device interoperability, data security, and the need for real-time processing. This paper synthesizes a comprehensive framework for an IoT-based smart waste management system by integrating principles of interoperability, real-time data processing, and decentralized security, drawing upon established research in adjacent smart city domains. We propose a multi-layered architecture that leverages an interoperable IoT platform for device integration, a Kappa architecture for real-time and batch analytics, and Blockchain technology for ensuring data integrity and trust. The resulting framework offers a blueprint for developing scalable, secure, and efficient waste management solutions that are essential for the sustainable development of smart cities.

Keywords: Smart Cities, Internet of Things (IoT), Waste Management, Cybersecurity, Interoperability, Blockchain, Kappa Architecture.

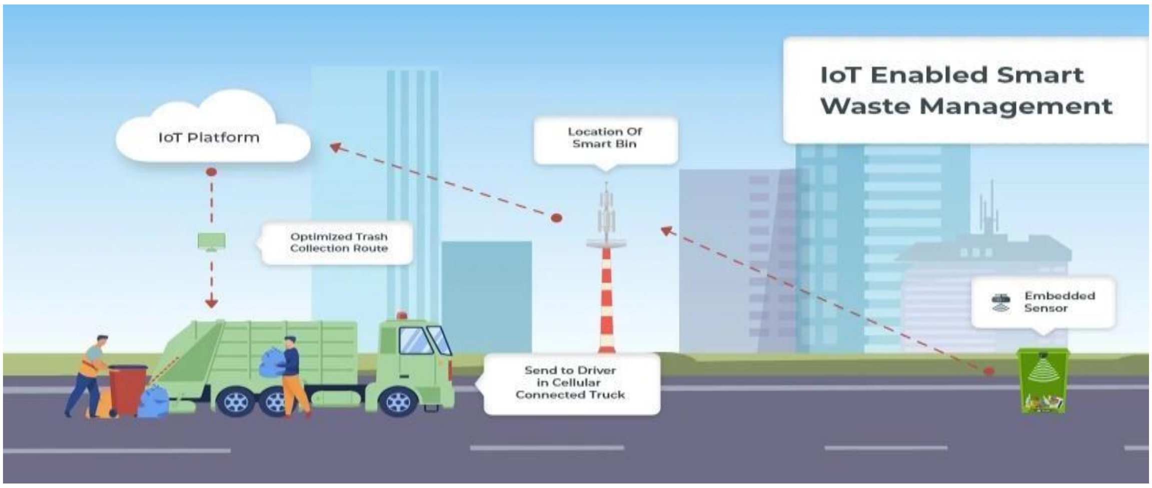

Figure 1: IOT Enabled Smart Waste Management

I. INTRODUCTION

The global shift towards urbanization has placed immense pressure on municipal services, with waste management being one of the most critical and resource-intensive operations. Traditional waste collection methods are often inefficient, relying on fixed schedules and routes that do not account for the actual fill-levels of bins, leading to unnecessary fuel consumption, overflowing bins, and underutilized collection resources.

The concept of the "Smart City" offers a paradigm shift, leveraging advanced technologies to optimize urban services. **IoT devices are the backbone of smart cities, enabling the collection and transmission of real-time data that drives decision-making processes**. While IoT has been widely discussed in the context of traffic management, energy grids,

DOI: 10.17148/IJIREEICE.2025.131110

and public safety, its application to waste management holds equal, if not greater, potential for enhancing urban livability and sustainability.

However, the integration of IoT into critical city infrastructure introduces significant vulnerabilities. **The proliferation of IoT devices creates multiple entry points for cyberattacks, which could disrupt vital city services, compromise personal data, or even endanger public safety**. Furthermore, **IoT devices, which are often deployed in large numbers, may have insufficient security protections, making them vulnerable to cyberattacks.** A successful attack on a waste management system could lead to service disruption, data theft, and erosion of public trust.

This paper addresses these challenges by proposing a synthesized framework for an IoT-based smart waste management system. Our contribution is the integration of three core technological pillars identified from leading smart city research:

1. An **interoperable platform** to manage heterogeneous devices.
2. A **Kappa architecture** for real-time data processing and analytics.
3. **Blockchain technology** for decentralized security and data integrity.

By combining these elements, we outline a system that is not only efficient but also secure, scalable, and resilient.

II. LITERATURE REVIEW AND FOUNDATIONAL CONCEPTS

This section reviews the foundational concepts from smart city research that inform our proposed framework.

2.1 Security Imperatives in Smart City IoT

Security is a non-negotiable prerequisite for any smart city application. **In smart city applications, the information is transmitted and used by various groups... each entity distinctively utilizes and manages information, which might jeopardize an individual's privacy.** For a waste management system, this includes protecting data on collection schedules, bin locations, and operational patterns. The core security requirements are **secrecy, reliability, and accessibility... confidentiality guarantees adversaries cannot view data without authentication; integrity ensures data accuracy; availability promises authenticated users can access network services**.

2.2 The Challenge of Interoperability

A practical waste management system will deploy sensors from various manufacturers, each with its own communication protocol. **IoT devices come from different manufacturers using different protocols of communication. The diversity of protocols and sometimes their incompatibilities stay a major issue**. This lack of standardization makes it difficult to implement a unified system. A solution is to use an **IoT platform to facilitate their interaction, control them intelligently using a web interface**.

2.3 Real-Time Data Processing with Kappa Architecture

Waste management requires both real-time responses (e.g., an alert when a bin is full) and batch analytics (e.g., optimizing weekly collection routes). The **Kappa architecture provides a way to process... data at high speed in the cloud, and thus meets processing requirements**. It uses a single, unified processing pipeline for both real-time and historical data, simplifying the system architecture and ensuring consistency.

2.4 Ensuring Trust with Blockchain

To prevent tampering with critical data, such as collection logs or bin status reports, a tamper-proof mechanism is required. **Blockchain technology provides a decentralized, autonomous, trustless, and distributed environment... offering better security and data integrity due to its tamper-proof and immutable characteristics.** In a waste system, this can create an immutable audit trail of all operations, from bin fill-level readings to collection confirmations.

III. PROPOSED FRAMEWORK FOR IOT-BASED SMART WASTE MANAGEMENT

Based on the principles above, we propose a four-layer architecture for a secure and interoperable smart waste management system.

3.1 System Architecture

1. **Perception Layer:** This layer consists of the physical smart waste bins equipped with IoT sensors (e.g., ultrasonic sensors for fill-level detection, RFID tags for identification, and GPS modules for location tracking).
2. **Interoperability & Network Layer:** This layer is responsible for abstracting the heterogeneity of the devices. It utilizes an **interoperable IoT platform** that acts as a universal gateway. This platform connects to the sensors via

DOI: 10.17148/IJIREEICE.2025.131110

various protocols (e.g., MQTT, LoRaWAN, Zigbee) and normalizes the data into a standard format for the upper layers.

3. **Processing & Security Layer:** This is the core of the system.
   - The normalized data is fed into a message queue (e.g., Apache Kafka) and processed by a **Kappa architecture**. This architecture triggers real-time alerts to collection crews when bins reach a pre-defined capacity and simultaneously feeds data into a storage system for large-scale analytics (e.g., route optimization, predictive fill-rate modeling).
   - All critical events and transactions (e.g., "Bin X is full," "Truck Y collected Bin X") are recorded as transactions on a **Blockchain**. This ensures an immutable, auditable, and trustworthy record of all system activities.
4. **Application Layer:** This layer provides the user interface for different stakeholders. A web- based dashboard for city managers displays real-time bin statuses, analytics, and collection routes. A mobile application for collection crews provides optimized routes and task updates.

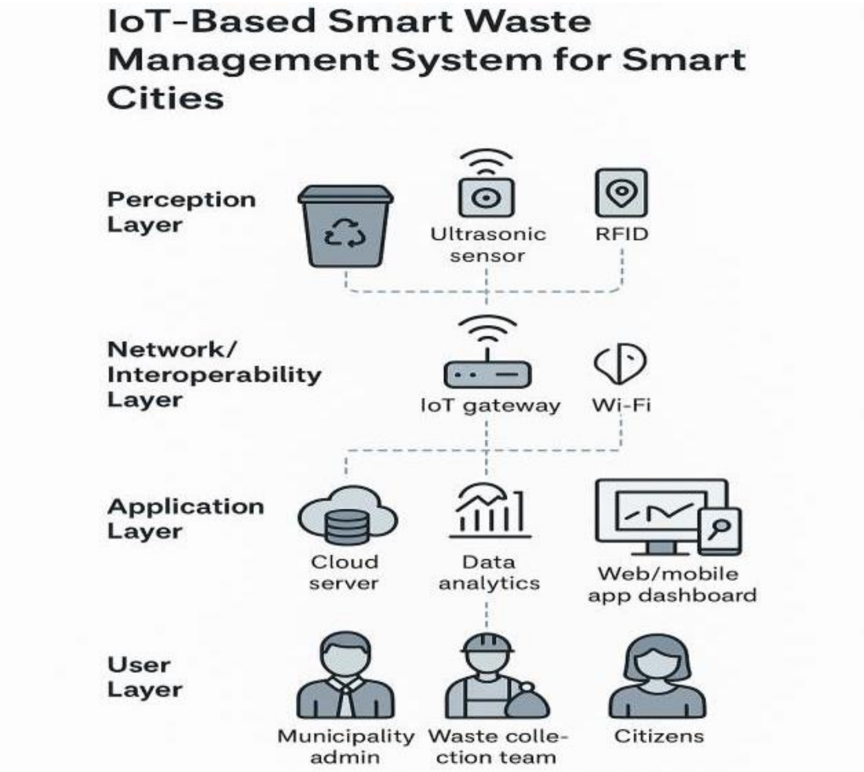

Figure 2**:** System Architecture

3.2 System Workflow

5. A smart bin's fill-level sensor detects that it is 80% full.
6. The sensor sends this data to the **Interoperability Platform,** which translates it into a standard JSON format.
7. The formatted data is ingested by the **Kappa architecture's processing engine**.
8. The processing engine triggers a real-time alert to the central system and updates the bin's status on the city manager's dashboard.
9. Simultaneously, the event ("Bin ID: 123, Status: Full, Timestamp: ...") is recorded as a transaction on the **Blockchain**.
10. The system's analytics engine, also part of the Kappa architecture, uses this new data to dynamically optimize collection routes for the next shift.

DOI: 10.17148/IJIREEICE.2025.131110

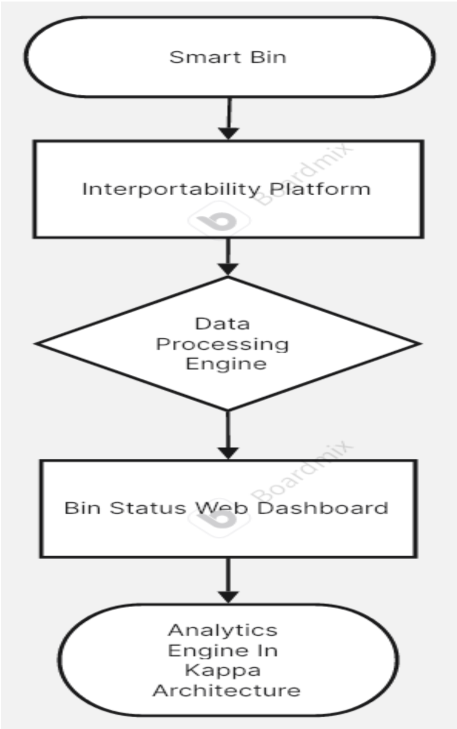

Figure 3: System Workflow

IV. DISCUSSION

4.1 Addressing Security Challenges

Our framework directly tackles the security issues outlined in Section 2.1. The use of **Blockchain provides a decentralized... environment... offering better security and data integrity due to its tamper-proof and immutable characteristics**, which directly addresses the integrity and non- repudiation requirements. The interoperability platform can enforce **authentication** and **access control**, ensuring that only authorized devices and personnel can interact with the system.

4.2 Overcoming Interoperability Hurdles

The dedicated **Interoperability Layer** is the key to solving the fragmentation of IoT devices. It allows the city to procure best-in-class sensors from any vendor without being locked into a single ecosystem, ensuring long-term flexibility and scalability.

4.3 Ensuring Performance and Scalability

By adopting the **Kappa architecture**, the system is built for performance. It can handle the high-velocity data stream from thousands of bins in real-time while also supporting the complex batch queries needed for large-scale urban planning and resource optimization.

V. CONCLUSION AND FUTURE WORK

This paper has presented a synthesized framework for an IoT-based smart waste management system for smart cities. By integrating solutions for interoperability, real-time processing, and decentralized security, we address the primary barriers to the practical deployment of such systems. The proposed architecture is not merely theoretical; it is constructed from proven technological concepts applied in other smart city domains, providing a robust and practical blueprint for municipalities.

Future work will focus on the implementation of a pilot project to validate this framework. This would involve selecting specific hardware, deploying the interoperability platform and Kappa architecture on a cloud environment, and developing smart contracts for the Blockchain layer. Furthermore, integrating machine learning models on top of the Kappa architecture's analytics layer could enable predictive capabilities, forecasting when bins will be full and further optimizing collection schedules.

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.414 ⩋ Peer-reviewed & Refereed journal ⩋ Vol. 13, Issue 11, November 2025
DOI: 10.17148/IJIREEICE.2025.131110

REFERENCES

[1]. Ait Abdelouahid, R., Debauche, O., & Marzak, A. (2021). Internet of Things: a new Interoperable IoT Platform. Application to a Smart Building. *Procedia Computer Science, 191*, 511–517.
[2]. Abbassi, Y., & Benlahmer, H. (2021). IoT and Blockchain combined: for decentralized security. *Procedia Computer Science, 191*, 337–342.
[3]. Nkamla Penka, J. B., Mahmoudi, S., & Debauche, O. (2021). A new Kappa Architecture for IoT Data Management in Smart Farming. *Procedia Computer Science, 191*, 17–24.
[4]. Tariq, N., Aslam Khan, F., & Asim, M. (2021). Security Challenges and Requirements for Smart Internet of Things Applications: A Comprehensive Analysis. *Procedia Computer Science, 191*, 425–430.
[5]. Samuel, A. H. (2021). Smart Cities' Cybersecurity and IoT: Challenges and Future Research Directions.
[6]. T. O. Oladejo, M. A. A. Adegbite, and B. A. O. Banjo, "Security and Privacy Issues in IoT-Enabled Municipal Services: A Review," *International Journal of Information Security*, vol. 20, no. 4, pp. 587-605, 2021.
[7]. D. Z. Khan, Y. X. Li, and A. H. Farooqi, "Leveraging Blockchain for Trust and Transparency in Smart City Supply Chains," *Journal of Smart Cities*, vol. 3, no. 2, pp. 101-118, 2023.
[8]. E. C. Rossi, G. Bianchi, and M. Conti, "A Comparative Analysis of Lambda and Kappa Architectures for Real-Time Urban Data Analytics," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 15, e6889, 2022.
[9]. N. Gupta, P. K. Singh, and R. K. Singh, "Optimization of Waste Collection Routes Using IoT and Genetic Algorithms," *Applied Soft Computing*, vol. 108, pp. 107503, 2021.
[10]. S. V. R. Kumar and L. M. Jacob, "A Low-Power Interoperable IoT Gateway for Smart City Applications," in *2021 Global Internet of Things Summit (GIoTS)*, Dublin, Ireland, 2021, pp. 1-6