ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13 Issue 04 April 2026

# IoT -Blockchain Enabled Cybersecure Tracking Framework with Anomaly Detection to Prevent Information Leakage in E-Waste Logistics

[1] Sivadarshini S, [2] Shakana P R, [3] Valarmathi P

[1][2][3] Department of Computer Science and Engineering, B.S. Abdul Rahman Crescent Institute of Science and Technology, Chennai, India

Email: [1] darshini0093@gmail.com, [2] prshakana2@gmail.com, [3] valarmathi@crescent.education

***Abstract***— *The volume of electronic waste (e-waste) is increasing exponentially, posing two crises, environmental degradation and cybersecurity vulnerability, especially due to the leakage of information stored in discarded storage media. Conventional e-waste management solutions usually use central databases and manual records that are prone to manipulation of data and records cannot be traced securely. In this study, the authors suggest ECOCYPHER, a combined system based on Internet of Things (IoT) sensors and permissioned Hyperledger Fabric blockchain to offer an immutable, fully end-to- end traceable logistical network. The system processes apply RFID and GPS-based IoT tracks to track the movement of e-waste, and a multi-tier security protocol that incorporates authentication with the help of a hash of SHA-256 and One-Time Password (OTP) application blocks unauthorized access and theft of information. In addition, the framework will have an anomaly detection engine based on Local outlier factor (LOF), haversine route deviation analysis, and Z-score statistical monitoring to detect anomalies like illegal dumping or unapproved diversions. There is a performance assessment that states that the proposed system has a high transaction and low latency, thus providing scalable digital governance. Through its solutions to the shortcomings of recent models, including the absence of advanced security analytics and reputation management, it offers a capable infrastructure of secure e-waste management in the times of Industry 4.0.*

***Index Terms***— *Endpoint Detection and Response, Artificial Intelligence, SIEM, Anomaly Detection, Attack Simulation, Cybersecurity*

## I. INTRODUCTION

The electronic waste (e-waste) has been the most rapidly growing waste stream in the world due to the proliferation of electronic devices globally. When the electronic equipment hit its end-of-life phase, inadequate management and inappropriate disposal produces critical environmental and health risks, as a result of the existence of dangerous chemicals such as lead, mercury, and cadmium. The fourth Global E-waste Monitor (2024) notes that the e-waste production is becoming five times quicker than recorded recycling choices, and the likely value of recoverable natural resources is standing at approximately US 62 billion that is not counted nor contributing to the growth of pollution risks worldwide.

In addition to environmental ecology, e-waste poses a very deep and nearly unknown cybersecurity problem. Hardware that is discarded, e.g. hard drives, circuits boards, communication modules, etc., usually contains sensitive data, e.g. encryption keys, social security numbers, or classified government data. In case the logistics chain is compromised, the adversaries are able to intercept these devices scanning the storage media in bulk to steal personal information. The existing e-waste management systems are mostly disjointed and based on manual records, which does not enable real-time monitoring as well as the authenticity of data in order to determine whether waste is reaching the authorized recycling centers or it is diverted to the black market.

To close these systemic loopholes, a combination of Internet of Things (IoT) technology and blockchain can offer a decentralized, non-modifiable system that can be utilized to track assets in real-time. This work is a model intended to provide the appropriate level of cybersecurity by embracing the concepts of permissioned blockchain networks so that each e-waste movement can be stored in an immutable registry. By closing the divide between the digital documentation maintained about e-waste and the actual reality, the proposed system will transform e-waste logistics into a process of active documentation rather than a passive one, with an ensuing result of a digital system of governance, strong and secure, and effectively scalable to the needs of modern smart city systems.

## II. BACKGROUND AND MOTIVATION

The logistics of e-waste is a multi-level system of stakeholders, such as collection points, transport organizations, and authorized recyclers. Trust between these entities is complicated by the disjointed data processing, as well as coopetition nature by which entities have to cooperate and simultaneously secure the secret of their own operations. Centralized storage models create single points- of-failure and are extremely prone to unauthorized alterations without making it hard to regulate the actual chain-of-custody of hazardous material to the regulatory bodies.

ISSN (Online) 2394-2320
International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Volume 13 Issue 04 April 2026

The first reason why this work should be developed is connected with the growing threat of information leakage. Lost storage devices are usually purchased in large numbers by their opponents who search through them to find valuable information, including crypto-wallets, blueprints of important infrastructure, or sensitive government files. The existing logistics chains do not provide evidence-based destruction certificates, which leaves an empty space upon the possibility of devices being redirected to the black market even before their data is confirmed to be erased. Also, aberration on transit- like route variation or some unwelcome delays- are generally signals of illegal dumping or unauthorized changing of components, which cannot be identified in the real-time in the traditional systems.

This implementation combines the digital records and the real-life world by implementing IoT technologies and a permissioned blockchain. IoT sensors allow viewing the physical assets movement in real time, and the blockchain makes sure that such records are unchangeable and visible to anyone with the necessary access. This integration enhances digital governance as it is a guarantee that the data that is registered is in fact physical action, which is a good way of reducing both environmental risk and cybersecurity threat.

## III. RELATED WORK

The basic combination of IoT and blockchain technologies has been researched widely across all the fields of logistics. Kharche et al. conducted a study to investigate the application of blockchain technology to integrated IoT networks to come up with scalable Intelligent Transportation Systems (ITS) in India. Their effort described the capability of this architecture to manage data insecurely and in real- time and presented a guide in building scalable tracking infrastructures. Nevertheless, such implementations are mostly constrained within the ITS spectrum and have not been modified comprehensively in order to accommodate the specific environmental and data-security challenges faced in the management of hazardous e-waste.

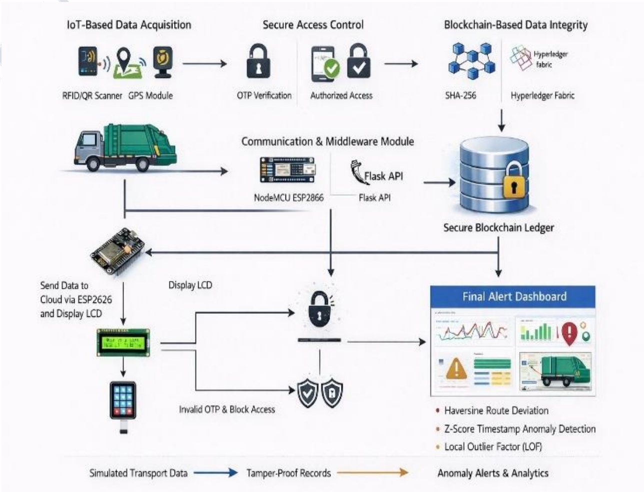
Recent research has reverted to the specialized e-waste tracking structures in order to solve the absence of lifecycle traceability. Santhuja and Anbarasu suggested a IoT-based system with blockchain that used LoRa sensors to monitor e-waste bins, which could serve as a solid foundation to monitor the collection points. Expanding on this, Khan and Ahmad came up with an Ethereum-based system of smart cities that captures lifecycle events to make e-waste traceable throughout manufacturing to disposal. Not withstanding these developments, both models have severe drawbacks as the former is more interested in bin-level activity compared to transit logistics, whereas the latter does not provide a high-level security, analytics and reputation sensitive stakeholder selection required to curb information leakage amid high risks transfers.

These tracking systems are further streamlined in the optimization and resource allocation strategies, but they also create a new problem. To enhance the data integrity of sensor networks, Santthuja and Anbarasu proposed an intuitive analysis, a Hybrid Genetic Crow Algorithm (HGCA) which enhances efficiency and yet is computationally intensive to standard IoT nodes. In the same manner, Arafatur Rahman suggested a smart garbage collection system that is concerned with equity and efficient routing of the collection trucks. Although this method is much more effective in distributing the workload and giving it structure, there is no immutable ledger based on blockchain, so the obtained records can be modified and altered. ECOCYPHER fills such gaps in systems through synthesis of real time monitoring and automated security enforcement, as well as decentralized trust.

## IV. PROPOSED SYSTEM

This anomaly detection and information leakage prevention framework, which has been developed to solve the issue of cybersecurity through the integration of physical e-waste resources and centralised digital registry. The system works at various levels.The system, which is centred on an Arduino-based edge controller, is used in the automation of capturing various important data related to logistics, including the unique identification of items and continuous tracking of the geospatial location. A layered style is used in the proposed architecture and it isolates hardware sensing, cryptographic security and decentralised storage meaning that the records of a transaction are authentic and immutable. With a dedicated machine learning engine that delivers real-time behavioural control, ecocypher will transform e-waste management to show less of a manual documentation to a proactive model of digital governance, which will significantly reduce the risks of data theft and cyber non-compliance with the environment throughout the logistics lifecycle.

*Proposed System and Technical Modules*




This system is a multidimensional, cyber oriented design, which intersects physical e-waste resources and a decentralized digital registry.

### A. Layered System Architecture.

The system follows 7-layer architecture style based on the idea of the base paper IoT network structure, which guarantees the modularity and security of all transition points:

IoT Layer: Edge-level sensors which are physical nodes that include microcontrollers and sensors.

Security Layer: Provides cryptographic principles, namely, the hash-SHA-256.

Gateway Layer: Middleware This is a Flask-based API, which provides secure data routing.

Blockchain Layer: Blockchain Layer: Hyperledger Fabric network of peers, orderers and channels are built on the Blockchain Layer.

Smart Contract Layer: It performs automated integrity checks for Train codes.

ML Layer: Special anomaly detector engine that is dedicated to behavioural analysis.

Dashboard Layer: Real time monitoring and alerting, as well as visualisation.

### B. Module Description

*IoT Based Data Acquisition Module*

This module is the main interface of physical identification. It also uses Arduino Uno that is connected to an EM-18 RFID reader (125 kHz) to record unique IDs of passive RFID tags placed on e-waste parts. An option of the Neo-6M GPS module has capability to offer real-time 3D positioning at the cost of at least four satellites hence high-precision geospatial monitoring. TSOP1738 IR sensors are also used to check the lock status of the container and in this case, any disruption in the 38 kHz signal is detected to signal illegal physical access.

*Secure Access Control Module*

The physical security is implemented via an automated system where multi-factor validation will be done at the recycling point. The entry of a One-Time Password (OTP) is integrated into the module and this is solved against the cloud server before the electronic lock is released. In case a seal has been violated during transit, the IR sensor will signal an immediate notification of an Intrusion Alert that will be signaled to the blockchain as a high-priority event before the swap of high-value parts can occur.

*Communication & Middleware Module*

This module allows bridging the hardware edge to the cloud backend. One of the modules, an ESP8266 of the type NodeMCU (ESP8266) is used to connect to Wi-Fi (802.11 b/g/n) and send sensor payloads with the help of HTTP requests to a Flask-based API middleware. The middleware authenticates the NodeMCU node and prepares the data to hash and serves as a buffer that does not expose directly the blockchain network to the external IoT devices.

*Blockchain-Based Module of Data Integrity*

To provide immutability, any transaction is documented within a permissioned Hyperledger Fabric blockchain. The logs of all the records of the logistic are digested through the algorithm of the hash-256 where a 256-bit distinctive fingerprint is generated. Chaincode (Smart Contracts) automatically checks the authenticity of the hash, the identity of the transport node, and the appropriateness of the timestamp and makes the commitment of the block based on a RAFT consensus mechanism. This is so that information about destruction of storage media can be proved as genuinely true, and cannot be retroactive.

*Detection of Anomalies and Monitoring Modules*

The last module uses machine learning to manage logistics behaviour. The Local Outlier Factor (LOF) computes the local reachability density to determine "density-based" outliers, i.e. a recycler with an unattainable amount of waste relative to its counterparts. The Haversine formula is a calculation of the shortest distance on a spherical surface that is used to identify route atrocities beyond a 100m metric whereas Z-score analysis is used to track any temporal aberrations in the delivery times.

## V. RESULT AND STUDY

With this framework, a tamper-proof logistics chain is obtained with 0 reported data manipulation when tested.

### A. Technical Performance Metrics.

It suggests that Hyperledger Fabric can handle a high level of transaction throughput, topping at 1,148.3 TPS on the top-tier models, and with an average latency of 0.21 - 2.1 seconds, which is not very far out of the operating range of urban sanitation networks. The anomaly detector models (especially LOF) have been shown to be at a level of accuracy of up to 95.6 to identify outliers in heterogeneous datasets.

### B. Real- time Dashboard and Alerting System

One of the benefits of the proposed system is the introduction of a social dashboard that will allow real-time monitoring of the e-waste cycle. The monitoring engine has been able to raise categorical alerts depending on the severity of the incident:

Red Flag (Critical): This is the topmost priority alert that is triggered when the Haversine formula is used to identify the route deviation of more than 100 meters; it means possible illegal dumping or illegal diversion.

Orange Flag (Warning): Warnings are sent when suspicious temporal delays during transit points have been detected in the Z-score analysis, indicating that someone might have tampered with it or even conducted an unauthorized inspection.

Yellow Flag (Advisory): When the Scan Sequence Integrity check represents any missing or duplicated RFID scans, advisory alerts are generated to indicate that there may have been an attempt to manipulate the records.

All alerts are connected to the Android application based on the IoT, according to which authorised regulators and logistics managers can be informed about the security breach

ISSN (Online) 2394-2320
International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Volume 13 Issue 04 April 2026

or environment-related violation in real-time and react in advance to such a threat.

## VI. FUTURE ENHANCEMENT

Future research and development will be aimed at the improvement of intelligence and resource resilience of the tracking infrastructure. One of them is the integration of TinyML directly onNodeMCU edge devices to allow local and real-time anomaly detection, detecting physical tampering or theft indicators without necessarily being connected to the cloud, therefore minimising communication latency.

An additional dynamic expansion of the system is to include the system as a direct business partner with Original Equipment Manufacturers (OEMs) and manufacturers. Using the immutable ledger of the blockchain, producers will be able to get real-time information about the state of their products at the end-of-life, which will make it easier to repurpose the recovered materials directly. This integration enables the introduction of Digital Product Passports (DPP) that can trace the composition of a device on its journey back to manufacturing and eventually recycling to ensure that valuable materials such as gold, lithium and copper can be provenance to a supply chain of the producer, in order to make the entire economy closed-loop circular. A system like this would help the producers to automate their Extended Producer Responsibility (EPR) compliance and also limit their use of virgin raw materials.

A blockchain-based reward system (gamification) is also a part of the strategic improvements. The system can be used to encourage an increased number of consumers and informal recyclers to use formal channels of recycling by offering them digital tokens to motivate them. Regulation ally, any subsequent generation will focus on a smooth coordination with government portals, a cross-border logistics system, to track the transit of hazardous waste across the borders. Also, the use of weight sensors to check the payload and solar-powered modules will increase the autonomy of the system to work in infrastructure-restricted areas.

## VII. CONCLUSION

This research enables to illustrate this framework as a powerful, IoT-Blockchain based system of logistics of e-waste security. The system successfully fills the identified environmental and cybersecurity gaps in the conventional centralised management models by incorporating real-time sensing operation and cryptographic hashing as well as decentralised storage. The modular 7-layer architecture will be integrated in such a way that all the e-waste movements will be permanently registered, so that authorities will have a verifiable chain-of-custody which will prevent illegal dumping and information leakage of discarded storage media.

The performance measurements affirm the Hyperledger Fabric network optimization based on the use of permissioned needed to operate large-scale urban sanitation and the LOF-based anomaly detection module to provide a highly sophisticated level of monitoring that cannot be achieved with traditional systems. The fact that zero reported data manipulation was attained in the process of testing is the emphasis of the reliability of this decentralized approach. Moreover, a severity-coded alerting dashboard will enable stakeholders to receive real-time notifications and act proactively when the security is breached or the environment is violated.

To sum up, this anomaly detection (ecocypher) which prevents information leakage from e wastes is the solution that facilitates open and responsible e-waste recycling, as well as protects confidential state and personal data, potentially leading to the creation of safe and environmentally friendly smart cities of the digital era. This model will be further improved in the future, with the implementation of producer-integrated material reuse, and edge-based TinyML detection, to become a highly autonomous, socially integrated governance framework of global e-waste management.

## REFERENCES

[1] A. Kharche, S. Badholia, and R. K. Upadhyay, “Implementation of Blockchain Technology in Integrated IoT Networks for Constructing Scalable ITS Systems in India,” Blockchain: Research and Applications (Elsevier), vol. 5, no. 1, p. 100188, Jan. 2024.
[2] P. Santhuja and V. Anbarasu, “Blockchain-Enabled IoT Solution for E-Waste Management and Environmental Sustainability through Tracking and Tracing,” International Journal of Engineering Trends and Technology (Seventh Sense Research Group), vol. 71, no. 12, pp. 157–167, Dec. 2023.
[3] M. A. Rahman et al., “IoT-Enabled Intelligent Garbage Management System for Smart City: A Fairness Perspective,” IEEE Access (IEEE), vol. 12, pp. 82693–82705, Jun. 2024.
[4] V. S. Malagitti et al., “A Survey of IoT and Blockchain Solutions for Advancements in E-Waste Management,” International Journal of Environmental Sciences (The ASPD), vol. 11, no. 5s, pp. 1105– 1126, May 2025.
[5] R. Shevchuk et al., “Anomaly Detection in Blockchain: A Systematic Review of Trends, Challenges, and Future Directions,” Applied Sciences (MDPI), vol. 15, no. 15, p. 8330, Aug. 2025.
[6] X. Ma, K. Zhang, and T. Li, “Research on Government–Enterprise Collaborative Recycling Strategies: An Examination of Consumer Value Perception in the Context of Carbon Generalized System of Preferences,” Sustainability (MDPI), vol. 17, no. 16, pp. 1–28, Aug. 2025.
[7] S. Jena, “Smart Healthcare Ecosystem Using Hyperledger Fabric for Digital Identity Management,” Blockchain Healthcare Today (Tory Cenaj), vol. 8, p. 411, Sep. 2025.
[8] B. Manasa and P. V. Krishna, “A Secure, Scalable System for Precision Agriculture Using IoT, Blockchain, and Predictive Analytics,” International Journal of Computer Engineering Research Trends (IJCERT), vol. 12, no. 6, pp. 1–13, Jun. 2025.
[9] S. Noliya, A. Gupta, and V. Kumar, “E-waste management through Blockchain Technology: Supply chain led environmental sustainability,” EDPACS (Taylor & Francis), vol. 37, no. 4, pp. 1– 18, Jul. 2025.
[10] N. Karankar and A. Seth, “An IoT system for access control using blockchain and message queuing system,” EURASIP

Journal on Information Security (Springer), vol. 2025, no. 1, p. 31, Oct. 2025.

[11] Z. Xie et al., "An anomaly detection scheme for data stream in cold chain logistics," PLoS ONE (Public Library of Science), vol. 20, no. 3, p. e0315322, Mar. 2025.

[12] H. Rhachi, "Enhanced Anomaly Detection in IoT Networks Using Deep Autoencoders," Sensors (MDPI), vol. 25, no. 10, p. 3150, May 2025.

[13] T. Bishtawi et al., "Integrating blockchain technology for secure access control in smart home environments: A comprehensive review," International Journal of Data and Network Science (Growing Science), vol. 9, no. 3, pp. 373–384, Jan. 2025.

[14] N. Zacharia et al., "Hyperledger Fabric Blockchain-Based Approach towards Secured Port Weighbridge Systems," Journal of Computer and Communications (SCIRP), vol. 13, no. 5, pp. 46–65, May 2025.

[15] M. L. T. Alaoui, M. Belhiah, and S. Ziti, "IoT-Enabled Waste Management in Smart Cities: A Systematic Literature Review," International Journal of Advanced Computer Science and Applications (The SAI Organization), vol. 16, no. 4, pp. 131–142, Apr. 2025.

[16] P. Santhuja and V. Anbarasu, "E-waste prediction and optimal route selection using adaptive deep Markov random field and block chain," Kybernetes (Emerald), vol. 54, no. 9, pp. 4902–4930, Sep. 2025.

[17] O. Ayeni, "Smart Waste Management in the Age of Industry 4.0: IoT, AI and Blockchain Applications in Circular Economy Systems," World Journal of Advanced Research and Reviews (WJARR), vol. 28, no. 1, pp. 379–391, Jan. 2025.

[18] K. Kumar and A. F. A. Al-Sharif, "E-waste Management Using Blockchain Technology," Data and Metadata (SEU), vol. 3, p. 355, Sep. 2024.

[19] P. Krishnan et al., "eSIM and blockchain integrated secure zero- touch provisioning for autonomous cellular-IoTs in 5G networks," Computer Communications (Elsevier), vol. 216, pp. 324–345, Jan. 2024.

[20] S. Shahanas et al., "Anomaly Detection in Time Series Data in IoT Environment," International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), vol. 13, no. 3, pp. 106–112, Mar. 2024.

[21] A. Petkovski and V. Shehu, "Anomaly Detection on Univariate Sensing Time Series Data for Smart Aquaculture Using K-Means, Isolation Forest, and Local Outlier Factor," IEEE Access (IEEE), vol. 12, pp. 4500–4515, Jan. 2024.

[22] M. Hossen et al., "A Reliable and Robust Deep Learning Model for Effective Recyclable Waste Classification," IEEE Access (IEEE), vol. 12, pp. 9501–9515, Jan. 2024.

[23] N. Bawankar et al., "IoT-Enabled Water Monitoring in Smart Cities With Retrofit and Solar-Based Energy Harvesting," IEEE Access (IEEE), vol. 12, pp. 58222–58238, Jun. 2024.

[24] A. M. Alabdali, "Blockchain based solid waste classification with AI powered tracking and IoT integration," Sustainability (MDPI), vol. 16, no. 4, p. 1105, Feb. 2024.

[25] M. Ghouse et al., "Survey on Effective Disposal of E-Waste to Prevent Data Leakage," Computer Assisted Methods in Engineering and Science (IPPT PAN), vol. 31, no. 2, pp. 187–212, May 2024.

[26] E. Altulaihan et al., "Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks," Sensors (MDPI), vol. 24, no. 2, p. 713, Jan. 2024.

[27] M. Hasan et al., "Artificial Intelligent Model to Enhance Thermal Conductivity of Hybrid Nanofluid for Automotive Radiator," IEEE Access (IEEE), vol. 12, pp. 179164–179175, Nov. 2024.

[28] G. Pradeep et al., "Hybrid Energy-Efficient Task Offloading Algorithm (HEETA): A framework for optimizing edge computing offloading decisions," Journal of Electrical Systems (ESR Groups), vol. 20, no. 5s, pp. 237–246, Aug. 2024.

[29] R. Selvaa and S. K. Priya, "Blockchain Based Logistics Protocol Using Hyperledger Fabric," International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering (IJIREEICE), vol. 13, no. 4, pp. 211–215, Apr. 2025.

[30] X. Qi and T. Zhang, "Information sharing between competing recyclers in a reverse supply chain," International Journal of Industrial Engineering Computations (Growing Science), vol. 16, no. 2, pp. 443–462, Apr. 2025.