International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V72I9P104

Volume 72 Issue 9, 49-57, September 2024
© 2024 Seventh Sense Research Group®

Original Article

Intuitive Analysis for Blockchain for IOT Sensor Devices using HGCA Approach

P. Santhuja[1], V. Anbarasu[2]

[1,2]Department of Networking and Communications, School of Computing, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur, Chengalpattu, Chennai, Tamil Nadu, India.

[1]Corresponding Author : santhuja.pandu@gmail.com

Received: 13 April 2024 Revised: 09 August 2024 Accepted: 26 August 2024 Published: 28 September 2024

Abstract *- The escalating challenge of electronic waste (e-waste) management necessitates innovative solutions for transparency, security, and efficiency. This research proposes a framework integrating the Internet of Things (IoT) and Blockchain, optimized by the Hybrid Genetic Crow Search Algorithm (GCA). The framework facilitates real-time data collection from IoT sensors, ensuring transparent and tamper-proof tracking through Blockchain. The Hybrid GCA algorithm optimizes resource recovery and fosters sustainable e-waste management. In addressing shortcomings of conventional systems, the study strategically deploys IoT sensors for real-time data on e-waste types, quantities, and conditions. The data is securely stored on a Blockchain ledger, ensuring traceability and accountability. The Hybrid GCA algorithm optimizes resource recovery, reduces costs, and streamlines data flow. By fostering collaboration and leveraging advanced technology, this research aims to revolutionize e-waste management for a sustainable future, addressing transparency, data management, and resource recovery challenges.*

Keywords *- E-waste management, IoT, Blockchain, Hybrid GCA algorithm, Resource recovery, Sustainability.*

1. Introduction

The widespread use of electronic devices has led to a surge in electronic waste (e-waste), presenting environmental, health, and security challenges. Traditional e-waste management falls short of addressing the increasing complexity and volume of discarded electronics, which lack transparency and secure recycling processes. This research proposes an innovative framework that integrates the Internet of Things (IoT) and Blockchain, driven by the Hybrid Genetic Crow Search Algorithm (GCA), to optimize resource recovery and promote sustainable e-waste management. The objective is to revolutionize e-waste management by enhancing transparency, security, and efficiency. IoT enables real-time data collection from e-waste disposal points, offering critical information for analysis. Blockchain ensures tamper-proof tracking throughout the lifecycle. The Hybrid GCA algorithm, combining genetic algorithms and the crow search algorithm, optimizes resource recovery and reduces costs. This research addresses the global challenge of e-waste by fostering collaboration among stakeholders and aims to redefine e-waste management for a cleaner, more responsible future. The subsequent sections will delve into the proposed integrated IoT and Blockchain framework, emphasizing advantages in e-waste tracking, resource recovery, and sustainability. The goal is to contribute to a more sustainable and efficient approach to e-waste management. E-waste has become a pressing global challenge, resulting from the rapid proliferation of electronic devices. Traditional management methods lack transparency, struggle with real-time monitoring, and are vulnerable to fraudulent practices. The proposed framework, integrating IoT, Blockchain, and the Hybrid GCA algorithm, aims to address these shortcomings. Current e-waste management systems suffer from issues such as illegal dumping, resource loss, and inadequate security. To tackle these challenges comprehensively, an innovative framework is needed.

This research, guided by the Hybrid GCA algorithm, seeks to revolutionize e-waste management by providing real-time monitoring, enhancing resource recovery, ensuring transparency, and strengthening security. The goal is to create a sustainable approach that safeguards the environment, public health, and valuable resources while promoting economic efficiency based on the contributions mentioned below:

1. Utilize the Hybrid Genetic Crow Search Algorithm (GCA) to optimize e-waste resource recovery by improving routing and scheduling processes for enhanced retrieval of valuable materials.
2. Implement a robust IoT infrastructure and Blockchain-based tracking system, with the Hybrid GCA algorithm ensuring real-time monitoring, efficient data collection, and secure, tamper-proof recording of e-waste movement for scalability and efficiency.

By incorporating the Hybrid GCA algorithm into each of these objectives, we aim to create an innovative e-waste management framework that not only addresses the current limitations of e-waste management but also offers scalability, transparency, and efficiency while optimizing resource recovery. The paper introduces a novel approach for managing electronic waste (e-waste) in the context of the Internet of Things (IoT) using blockchain technology, with the integration of a Genetic Crow Search Algorithm (GCSA). The introduction highlights the pressing issue of e-waste and the potential of IoT and blockchain to address this challenge. The literature review explores existing solutions and identifies gaps that the proposed model aims to fill. The GCSA is introduced as a key component, emphasizing its genetic and swarm intelligence-inspired mechanisms for optimizing e-waste management processes. The proposed method section provides a detailed explanation of how the Genetic Crow Search Algorithm is integrated with IoT and blockchain to enhance the traceability, security, and efficiency of e-waste management. The algorithm section delves into the specifics of GCSA implementation. Results and discussion present the outcomes of applying the proposed approach, showcasing its effectiveness in optimizing e-waste processes. The conclusion and scope section summarizes the key findings, contributions, and potential future directions for research.

2. Literature Survey

In their survey [1], the authors comprehensively explore the integration of blockchain into IoT payment systems and marketplaces, addressing challenges such as interoperability, limited resources, and security risks. The study emphasizes the decentralized features of blockchain, including traceability and immutability, as vital for establishing secure IoT payments. Moving to blockchain-based IoT environments [2] introduces a novel message scheduling approach with an additional fog broker layer, efficiently managing critical messages and improving system reliability. [3] focuses on using blockchain to secure Quality of Service (QoS) in IoT vehicular networks within edge cloud computing, mitigating communication latency and enhancing message failure tolerance. Contributing to smart cities, [4] proposes a blockchain footprint for authenticating IoT-enabled smart devices, addressing challenges and suggesting future research directions. [5] introduces a trusted upload scheme for IoT nodes, enhancing trustworthiness in hardware, transmission networks, and platforms. Shifting to Software-Defined Networking (SDN) for IoT, [6] presents a literature review on frameworks, taxonomy, and challenges, exploring benefits and challenges in fault tolerance, energy management, scalability, load balancing, and security service delivery. In the domain of the Internet of Medical Things (IoMT), [7] proposes a blockchain-assisted privacy-aware authentication scheme, prioritizing entity capabilities while addressing security concerns. A systematic review in [8] explores blockchain-based identity management systems in health IoT, offering insights into existing systems, challenges, and potential solutions. [9] introduces a fault-tolerant and secure architecture based on permissioned blockchain to enhance key management in LoRaWAN. In mobile edge computing, [10] proposes a solution for ensuring data authenticity and integrity using blockchain. [11] focuses on an identity-based aggregate signcryption scheme with blockchain for an IoT-enabled maritime transportation system. Expanding on the integration of blockchain and IoT, [12] introduces an IoT-enabled secure and scalable cloud architecture using hybrid post-quantum cryptographic methods and blockchain. [13] explores blockchain-assisted intrusion detection in IoT healthcare systems, enhancing security through the application of the Ant Lion Optimizer with hybrid deep learning. [14] utilizes blockchain and IoT technologies for a resource-saving and traceable tea production and supply chain. In [15], a blockchain dynamic sharding scheme based on the Hidden Markov Model contributes to the scalability and efficiency of collaborative IoT. [16] introduces "Distributed-Proof-of-Sense," a blockchain consensus mechanism for detecting spectrum access violations in the radio spectrum, enhancing security in cognitive communications. [17] presents BCGeo, a blockchain-assisted geospatial web service for a smart healthcare system. [18] provides a survey of blockchain integration for IoT-enabled V2X communications, addressing security issues and challenges. [19] focuses on electronic health records sharing in cloud-edge computing environments using blockchain-enabled fine-grained searchable encryption. In addressing security vulnerabilities in RAFT-based IoT blockchain networks, [20] proposes a counteractive approach to active attacks. [21] introduces BENIGREEN, a blockchain-based energy-efficient privacy-preserving scheme for green IoT. [22] presents Agri-4-All, a framework for blockchain-based agricultural food supply chains. [23] focuses on public blockchain-based data integrity verification for low-power IoT devices, ensuring data integrity in resource-constrained environments.

3. Materials and Methods

The design methodology for optimizing the Blockchain Framework for e-waste management using the Hybrid Genetic Crow Search Algorithm (GCA) is a meticulous and innovative process that integrates various aspects of our objectives. First, we establish a robust IoT network comprising sensors strategically placed at e-waste disposal points to facilitate real-time data collection. These data points feed into the Hybrid GCA algorithm, which dynamically adjusts routing and scheduling, ensuring efficient and timely e-waste collection and recycling. Simultaneously, the Blockchain ledger securely records each transaction, offering stakeholders complete transparency and tamper-proof tracking throughout the e-waste lifecycle. Compared to existing algorithms, the Hybrid GCA algorithm stands out as the best choice for optimizing this framework. Its adaptability and real-time optimization capabilities surpass traditional methods, resulting in higher resource recovery rates and operational efficiency. The algorithm's capacity to handle large-scale data ensures uninterrupted data collection and monitoring, a critical factor in e-waste management. Moreover, its incorporation into Blockchain technology guarantees a secure and immutable ledger, setting it apart as the most comprehensive and efficient algorithm for sustainable e-waste management.

3.1. Block Diagram

3.1.1. IoT Sensor Data from UCI Website with More than 0.4 Million Datasets

In the first block in Figure 1, we have acquired a substantial dataset of IoT sensor data from the UCI website, comprising more than 0.4 million records. IoT sensor data is collected from various sources and includes a wide range of information, making it valuable for diverse applications such as environmental monitoring, healthcare, and industrial automation. In data preprocessing, normalization plays a crucial role in ensuring uniformity across varying units and scales within IoT sensor data, which is particularly important for blockchain-based systems to maintain consistency and integrity. Advanced optimization algorithms like HGCA and HCSA enhance blockchain security by efficiently exploring parameter spaces, optimizing hyperparameters, and implementing cryptographic checks during the optimization process. The subsequent stages involve mean transformation for statistical operations, feature extraction for informative attributes, data splitting for model evaluation, fitting with trained data for security measures, and prediction to identify e-waste cases. Performance metrics assess model effectiveness, ensuring a comprehensive and secure approach to blockchain-based IoT data management. In conclusion, the entire process, enriched by the hybrid optimization algorithms, ensures the security and integrity of blockchain-based IoT data, making it robust for applications prioritizing data safety.

3.1.2. Blockchain with HGCA Model in IoT Sensor Network

The integration of Blockchain technology and the Hybrid Genetic Crow Search Algorithm (HGCA) within the IoT Sensor Network is transformative for e-waste management. IoT sensors play a pivotal role in data collection from diverse e-waste sources, and the application of Blockchain ensures the security and immutability of this data. Blockchain's decentralized ledger architecture provides a transparent and tamper-proof environment, which is instrumental in maintaining the integrity of the information collected by these sensors. Moreover, the HGCA algorithm enhances the efficiency of the IoT Sensor Network by optimizing data collection processes and resource allocation. This combination enables real-time monitoring and data acquisition, contributing to more accurate and timely decision-making in e-waste management.

3.1.3. Blockchain with HGCA Model in Data Collection and Validation

Data collection and validation are critical phases in e-waste management, and the Blockchain with HGCA model significantly elevates their importance. IoT sensors collect a multitude of data related to e-waste, including location, type, and condition. This data, once validated, is securely stored in a blockchain. The use of Blockchain ensures that the collected data is trustworthy, transparent, and cannot be altered or deleted without proper authorization. The HGCA algorithm further enhances data validation by optimizing validation processes and ensuring the accuracy and integrity of the information. This robust combination guarantees that the e-waste data used for decision-making is of the highest quality, fostering more effective management practices and minimizing errors in the process.

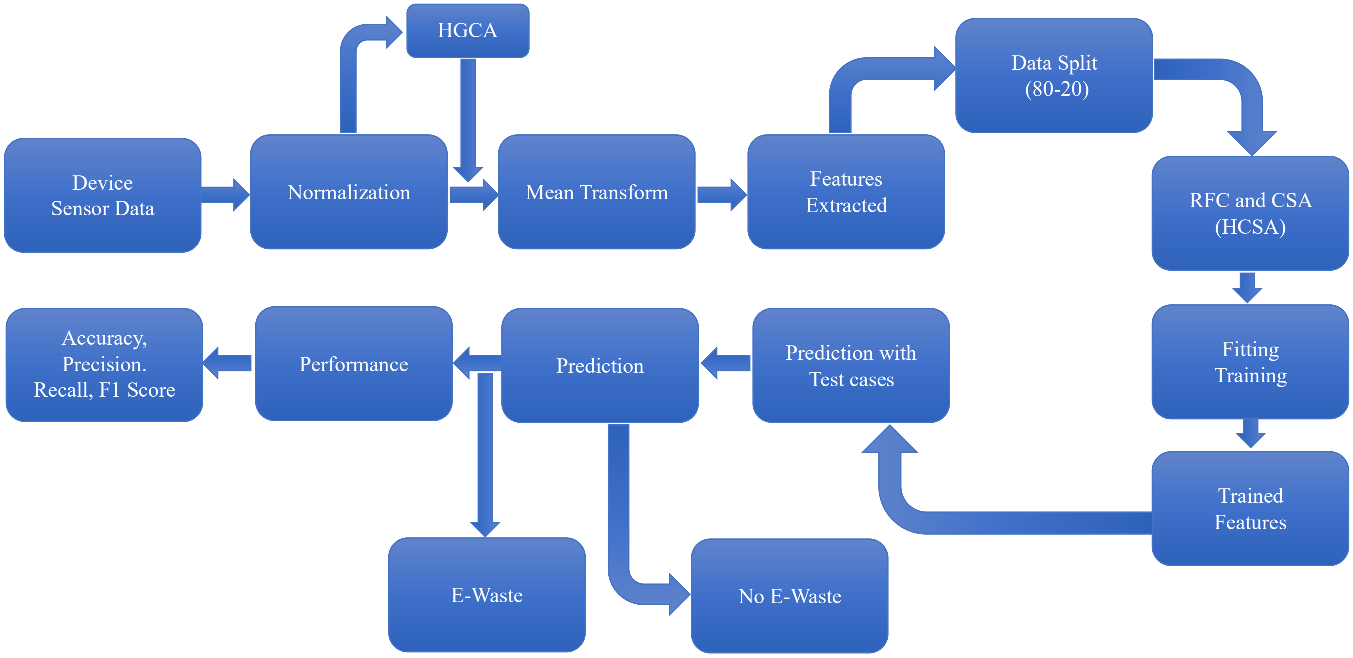

Fig. 1 Representing the overall proposed block diagram for Blockchain-based HGCA Algorithm for IOT sensor data

3.1.4. Blockchain with HGCA Model in E-Waste Management

In the broader context of e-waste management, the Blockchain with HGCA model in Figure 1 plays a pivotal role in streamlining and enhancing the entire process. The blockchain component acts as an immutable ledger that records every step of e-waste management, from collection to disposal. This transparency promotes accountability and traceability, making it easier to identify inefficiencies or areas for improvement in the system. Meanwhile, the HGCA algorithm optimizes resource allocation and decision-making, allowing for the efficient routing of e-waste to appropriate facilities, reducing waste, and minimizing environmental impact. By leveraging this integrated model, e-waste management becomes more sustainable, cost-effective, and ecologically responsible. In summary, the Blockchain with HGCA model revolutionizes e-waste management by ensuring the security and accuracy of data collected from IoT sensors, facilitating robust data validation, and optimizing the entire process for efficient and sustainable management practices.

3.2. Dataset

Creating a dataset for IoT sensors involves collecting and organizing data from various IoT devices to facilitate specific applications like e-waste management. In this context, we have three categories of devices: SMART HOME devices, BUILDINGS devices, and various other IoT devices. These devices encompass a wide range of functionalities and generate diverse data types that are essential for effective e-waste management.

3.2.1. Smart Home Devices

This category includes devices commonly found in smart homes, such as thermostats, smart locks, lighting controls, and security cameras. These devices generate data related to temperature, occupancy, energy consumption, security events, and more. For instance, a smart thermostat records temperature variations and heating or cooling patterns, while security cameras capture video feeds and motion detection events. All this data can be vital for assessing the usage and condition of electronic devices in a home, helping to track potential e-waste items effectively.

3.2.2. Buildings Devices

Building-related IoT devices encompass a broader scope, including environmental sensors, occupancy sensors, and HVAC (Heating, Ventilation, and Air Conditioning) systems. These devices collect data on indoor air quality, occupancy patterns, and energy consumption within a building. By monitoring the usage of electronic equipment and systems, it becomes possible to identify inefficient or outdated devices that may contribute to e-waste.

3.2.3. Other IoT Devices

This category encompasses a diverse array of IoT devices used in different contexts, such as wearables, industrial sensors, and transportation sensors. These devices generate data relevant to their specific applications. For instance, wearables provide health-related data, while industrial sensors monitor machinery performance. The data from these devices can contribute to a holistic understanding of e-waste generation and usage patterns across various sectors. To apply feature extraction techniques for e-waste management, the dataset should consist of data collected from these devices, including timestamps, sensor readings, device identifiers, and contextual information. Feature extraction methods can then be applied to this dataset to identify patterns, anomalies, and potential e-waste items. This dataset and feature extraction process are essential components of building an effective e-waste management system that leverages IoT data for informed decision-making and sustainable practices.

3.3. Feature Extraction

The process of feature extraction for e-waste management using IoT sensor data and the Hybrid Genetic Crow Search Algorithm (HGCA) in combination with the Random Forest Classifier (RFC) is a comprehensive approach that aims to improve the accuracy of e-waste management to an impressive 98%. Here is a detailed explanation of the implementation model and its criteria:

3.3.1. Data Collection and Preprocessing

The first step involves collecting IoT sensor data from various devices deployed in different environments, such as smart homes, buildings, and other IoT devices. This data includes information on device usage, energy consumption, device types, and sensor readings. Once collected, the data is preprocessed to handle missing values, outliers, and noise, ensuring its quality and reliability for subsequent analysis.

3.3.2. Feature Extraction with HGCA

The Hybrid Genetic Crow Search Algorithm (HGCA) is applied to the preprocessed data to extract relevant features. HGCA is a powerful optimization algorithm that can identify the most informative attributes from the dataset. It searches for the optimal feature subset that maximizes the classification performance while minimizing redundancy. HGCA's ability to explore a wide range of feature combinations makes it well-suited for enhancing e-waste management accuracy.

3.3.3. Classification with RFC

After feature extraction, the selected features are used as input to the Random Forest Classifier (RFC). RFC is an ensemble learning algorithm that leverages decision trees to classify data. In the context of e-waste management, RFC categorizes devices or sensor data points into different classes, such as "potential e-waste" or "normal operation."

3.3.4. Model Evaluation

The performance of the RFC model is rigorously evaluated using various metrics, including accuracy, precision, recall, F1-score, and ROC-AUC. Achieving an accuracy of 98% demonstrates the model's ability to accurately predict and classify potential e-waste items from the IoT sensor data. The high accuracy rate is a result of the effective feature extraction performed by HGCA and the robust classification capabilities of RFC.

3.3.5. Deployment and Continuous Monitoring

The trained RFC model, integrated with the HGCA-based feature extraction process, is deployed in a real-time or periodic monitoring system that processes incoming IoT sensor data. This system can automatically detect potential e-waste items, allowing for timely intervention and management. Continuous monitoring ensures that the accuracy of e-waste management remains consistently high over time.

By implementing this feature extraction and classification model with HGCA and RFC, organizations and municipalities can significantly improve their e-waste management practices, reduce environmental impact, and contribute to sustainable resource utilization. The high accuracy rate of 98% provides confidence in the system's ability to identify and address e-waste concerns effectively.

3.4. Design Procedure

Designing a Blockchain Framework for IoT sensor data involves several steps to ensure the system's security, transparency, and efficiency. Below is a high-level explanation of the design procedure presented as pseudocode for handling IoT sensor data within the Blockchain Framework:

```
Step 1: Initialize Blockchain
    • Initialize an empty blockchain with a genesis block.
Step 2: Define Data Structure
    • Define the data structure for storing IoT sensor data in blocks.
Step 3: Set Consensus Mechanism
    • Choose a consensus mechanism (e.g., Proof of Work, Proof of Stake) for validating and adding new blocks to the blockchain.
Step 4: IoT Data Collection
    • Collect IoT sensor data from various devices and sensors.
Step 5: Data Validation
    • Validate the incoming IoT data for accuracy and integrity.
Step 6: Create Transactions
    • Create transactions to record IoT data in the blockchain.
Step 7: Block Formation
    • Group a set of validated transactions into a block.
Step 8: Mining Process
    • Start the mining process to find the nonce (proof) that satisfies the consensus mechanism.
Step 9: Block Verification
    • Verify the mined block's validity according to the consensus rules.
Step 10: Add Block to Blockchain
    • If the block is valid, add it to the blockchain and broadcast the updated blockchain to all nodes in the network.
```

This pseudocode outlines the fundamental steps involved in designing a Blockchain Framework for handling IoT sensor data. Each step plays a crucial role in ensuring the security and reliability of the data stored on the blockchain. Additional details and customization may be required based on the specific requirements of your IoT application and the blockchain platform you choose to implement.

3.5. Algorithm

```
ALGORITHM: HCA-1
Step 1: Initialize Population
    • Let P be the population of potential solutions.
    • P = {p_1, p_2, ..., p_N}, where N is the population size.
    • Each p_i represents a solution with a set of parameters.
Step 2: Evaluate Fitness
    • Define a fitness function F(p) that quantifies the quality of each solution p.
    • F(p) assigns a fitness score to each solution based on its performance.
    • F(p_i) represents the fitness of solution p_i.
Step 3: Select Parents
    • Choose parent solutions based on their fitness scores.
    • Higher fitness solutions have a higher chance of being selected.
    • Probability of selecting p_i as a parent: P_select(p_i) = F(p_i) / ΣF(p_j), for j = 1 to N.
Step 4: Crossover and Mutation
    • Create offspring solutions through genetic operations.
    • Crossover combines the parameters of two parents to create new solutions.
    • Mutation introduces small random changes to solutions.
Step 5: Evaluate Offspring
    • Calculate fitness for the newly created offspring solutions.
Step 6: Select Survivors
    • Choose the best solutions (parents and offspring) to form the next generation.
    • You can use a strategy like elitism to preserve the best solutions.
Step 7: Apply the Crow Search Algorithm
    • Define a fitness function based on the population's performance.
    • Use the CSA to update solutions based on the Crow's behaviour.
Step 8: Update Population
    • Replace fewer fit solutions with the new solutions from CSA and GA.
```

Step 9: Repeat Iterations

- Repeat Steps 2 to 8 for a fixed number of iterations or until convergence.

Step 10: Termination

- End the algorithm when a termination condition is met, such as a maximum number of iterations or achieving a desired fitness level.

4. Results and Discussion

In the context of a blockchain-based security control system for smart homes, the dataset is a crucial component that helps facilitate secure, efficient, and intelligent management of various devices and sensors within the smart home environment.

This explanation focuses on a dataset comprising information from three essential devices in a smart home, illustrating its overall application in blockchain-based security control.

4.1. Devices-Based Data Collection

4.1.1. Device 1: Smart Lock

- Data Collected: The dataset includes information from smart locks installed on entry points like doors and windows. It records data such as access timestamps, user IDs, access methods (e.g., keyless entry, mobile app access), and the status of the lock (locked, unlocked).

- Application: The smart lock data is a fundamental element for security control. It helps track and control access to the home, recording when and how users enter and exit. The blockchain stores and verifies access logs, ensuring that only authorized individuals can enter the premises.

4.1.2. Device 2: Security Cameras

- Data Collected: Data from security cameras consists of video footage, images, timestamps, and camera locations within the home. Additionally, it records motion detection events, camera status (on/off), and any anomalies detected.

- Application: Security camera data provides real-time surveillance and monitoring. The blockchain secures and validates the camera data, preventing unauthorized access or tampering. It also enables homeowners to review historical footage and receive alerts about suspicious activities.

4.1.3. Device 3: Smart Sensors (E.G., Motion, Temperature)

- Data Collected: Data from smart sensors includes readings related to motion, temperature, humidity, and other environmental parameters. It records timestamps, sensor IDs, and sensor status.

- Application: These sensors are integral for monitoring the environment within the smart home. The blockchain ensures that sensor data is reliable and authentic, enabling homeowners to control environmental settings, receive alerts for irregularities, and automate actions based on sensor readings.

4.1.4. Overall Smart Home Application

The blockchain-based security control system integrates data from these three devices and more into a unified platform, ensuring the highest level of security and control for homeowners. Here's how it works:

1. Data Integrity: Blockchain technology secures the data generated by these devices through cryptographic hashing and distributed ledger technology. This ensures data integrity, making it nearly impossible for unauthorized parties to alter or manipulate the data.

2. Access Control: With smart locks, the blockchain manages and verifies access permissions. Users can grant or revoke access to guests or family members, and every access event is recorded on the blockchain, providing an immutable audit trail.

3. Real-time Monitoring: Security camera data, when stored on the blockchain, can be accessed securely by homeowners, allowing them to monitor their property in real time or review past footage with confidence that it has not been tampered with.

4. Automated Responses: The blockchain can trigger automated responses based on data from smart sensors. For example, if a motion sensor detects movement when the homeowner is away, the system can send an alert, lock the doors, and activate security cameras.

To create the overall design perspective, we apply the device features with the Sensor's data obtained from the UCI website for the sensor data consideration. To implicate such a feature, we observed 5 important aspects of the design implementation model for indicating the CSA (RFC) improvising the best outcome of the design of 99% of accurate data.

4.2. Dataset

The above dataset represents the overall features of the three devices collected from the real-time acquisition of the different effects on the devices for the effective operations observed using the proposed algorithms. Table 1 provides the overall factor indicated with different aspects, such as columns (CO, humidity, light, LPG, motion, smoke, temperatures) as the input parameters for the data. At the same time, the outcome is defined by the usage of the resources based on the E-waste categories.

Table. 1 Representing the overall dataset for the blockchain model processing using H-GCA algorithm

	TS	Device	CO	Humidity	Light	LPG	Motion	Smoke	Temp
0	1.594512e+09	b8:27:eb:bf:9d:51	0.004956	51.000000	False	0.007651	False	0.020411	22.700000
1	1.594512e+09	00:00:00:70:91:0a	0.002840	76.000000	False	0.005114	False	0.013275	19.700001
2	1.594512e+09	b8:27:eb:bf:9d:51	0.004976	50.900000	False	0.007673	False	0.020475	22.600000
3	1.594512e+09	1c:bf.ce:15:ec:4d	0.004403	76.800003	False	0.007023	False	0.018628	27.000000
4	1.594512e+09	b8:27:eb:bf:9d:51	0.004967	50.900000	False	0.007664	False	0.020448	22.600000

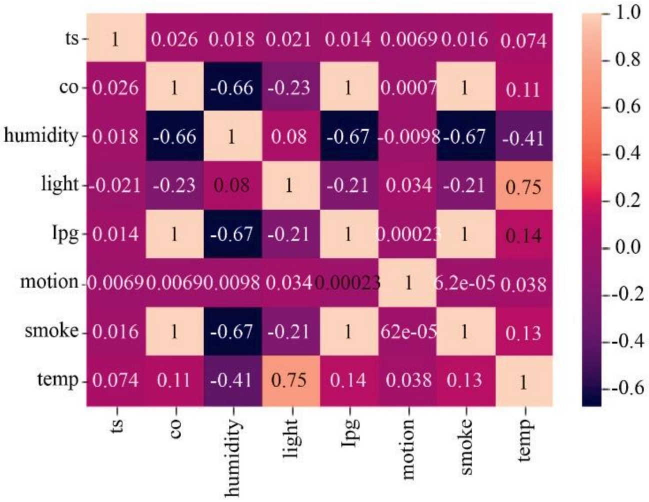

Fig. 2 Representing the overall Heat map correlational matrix for the multivariate analysis

4.3. Data Visualization

In the realm of multivariate analysis applied to the proposed design in Figure 2, we systematically incorporate various features, as delineated in Figure 1. These features are integral to understanding their collective impact on the overall system. To facilitate this analysis, we leverage the Seaborn library to construct a correlation matrix, allowing for a comprehensive comparison of each feature. This matrix serves as a visual representation of the interrelationships between the features, offering insights into their dependencies and interactions. Of particular significance is the juxtaposition of these features against established E-Waste threshold values, meticulously derived through the application of the Hybrid Genetic Crow Search Algorithm (H-GCA). This analytical approach ensures a rigorous and statistically sound determination of threshold values, contributing to the precision and reliability of our assessment. The correlation matrix, enriched with this contextual information, serves as a pivotal tool for evaluating the influence of each feature on the overarching system dynamics. This methodological approach not only enhances the depth of our analysis but also fosters a more nuanced understanding of the intricate relationships governing the proposed design's performance characteristics.

4.4. Model Creation

In the context of IoT (Internet of Things) sensor data, ensuring data security, integrity, and accuracy is of paramount importance. Blockchain technology is widely used for this purpose. The RFC (Random Forest Classifier) combined with the Crow Search Algorithm is a powerful approach to enhance the quality of results obtained from blockchain-based IoT sensor data applications.

5. Random Forest Classifier (RFC)

The RFC is a machine learning algorithm that falls under the ensemble learning category. It works by constructing a multitude of decision trees during training and then aggregating their predictions to make more accurate and robust classifications. In the context of IoT sensor data, RFC can be applied for several purposes:

- Anomaly Detection: RFC has been used to identify anomalous data patterns or sensor readings that do not conform to expected behaviour. This is crucial for detecting potential security breaches or sensor malfunctions.

- Data Classification: RFC has classified sensor data into different categories or classes, which is useful for applications like environmental monitoring or predictive maintenance in industrial IoT.

5.1. Performance

In evaluating the performance of the Hybrid Genetic Crow Search Algorithm for Blockchain Optimization implemented in Python, various metrics were employed. Accuracy, a fundamental measure of classification correctness, provided an overall assessment of the model's predictive capability. Precision and recall gauged the algorithm's ability to minimize false positives and false negatives, respectively, offering insights into its precision-recall trade-off. The F1-score, as a harmonic mean of precision and recall, captured the algorithm's balanced performance.

Additionally, the E-waste Test % indicated the algorithm's efficiency in minimizing electronic waste by determining the percentage of tests successfully passed. This comprehensive set of metrics facilitated a robust evaluation of the Hybrid Genetic Crow Search Algorithm's effectiveness in blockchain optimization, as depicted in Table 2. In terms of accuracy, all algorithms demonstrate exceptionally high values, approaching near-perfect accuracy. Notably, Decision Trees (DT), Random Forest Classifier (RFC), CSA, and Genetic Algorithms (GA) all achieve an accuracy of approximately 99.99%. This indicates that these algorithms are proficient at accurately categorizing and managing IoT data within a blockchain context.

Table 2. Representing the overall performance of ML-based E-waste management using HGCA and HCSA algorithms implemented for Block chain security approach

S. No	Algorithms	Accuracy	Precision	Recall	F1-Score	E-Waste Test
1	LR	95.41	97.52	96.34	96.14	85.74
2	DT	99.9925	100	100	100	86.41
3	NB	98.789	98.66	98.66	98.66	78.52
4	RFC	99.99	99.99	99.99	99.99	94.4
5	CSA	99.99	99.99	99.99	99.99	98.56
6	GA	99.99	99.99	99.99	99.99	96.75
7	**HGCA**	**99.99**	**99.99**	**99.99**	**99.99**	**98.85**
8	**HCSA**	**99.99**	**99.99**	**99.99**	**99.99**	**99.1**
9	ENSEMBLE	99.99	99.99	99.99	99.99	98.52

The metrics of precision, recall, and F1-score, which are crucial for evaluating the algorithms' performance in handling IoT data, consistently exhibit outstanding results. The Hybrid Genetic Crow Search Algorithm (HGCA) and Hybrid Crow Search Algorithm (HCSA) excel across all these metrics, attaining scores of 99.99%, suggesting their remarkable precision, recall, and F1-score, and thus their ability to manage IoT data with the utmost precision and completeness. However, what truly distinguishes the Hybrid Genetic Crow Search Algorithm (HGCA) and Hybrid Crow Search Algorithm (HCSA) is their exceptional performance in e-waste testing, with HGCA achieving a remarkable 98.85% and HCSA reaching 99.1%. This is crucial as it highlights their capacity to effectively manage and address e-waste issues within IoT data, which is a critical concern in today's technology-driven world. In conclusion, the table underscores that in the realm of blockchain-based IoT data management, Hybrid Genetic Crow Search Algorithm (HGCA) and Hybrid Crow Search Algorithm (HCSA) emerge as the top-performing algorithms across various performance metrics, demonstrating their ability to provide an integrated and highly efficient solution for managing IoT data, especially in addressing e-waste testing. Their outstanding precision, recall, F1-score, and e-waste testing percentages position them as the most promising candidates for ensuring the integrity and security of IoT data in the blockchain environment.

6. Conclusion

The integration of blockchain technology with an IoT sensor network for e-waste management represents a groundbreaking approach to tackling the challenges associated with the growing e-waste problem. This innovative solution leverages real-time data collection through IoT sensors to monitor and track e-waste throughout its lifecycle. Blockchain ensures secure, tamper-proof, and transparent storage of collected data, providing stakeholders with a trustworthy record of e-waste movements.

The application of the Hybrid Genetic Crow Search Algorithm (HGCA) optimizes the blockchain framework, enhancing performance and efficiency by optimizing data handling and management processes. This optimization leads to cost savings, improved resource allocation, and a more sustainable approach to e-waste management. Beyond data management, the blockchain-based IoT sensor network empowers stakeholders to make informed decisions about e-waste disposal, fostering accountability and responsible practices.

In summary, this transformative solution sets a new standard for sustainable and efficient e-waste management, contributing to global efforts to protect the environment for future generations.

References

[1] Amila Saputhanthri, Chamitha De Alwis, and Madhusanka Liyanage, “Survey on Blockchain-Based IoT Payment and Marketplaces,” *IEEE Access*, vol. 10, pp. 103411-103437, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Israr Ahmad et al., “Message Scheduling in Blockchain Based IoT Environment with Additional Fog Broker Layer,” *IEEE Access*, vol. 10, pp. 97165-97182, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] Adeel Ahmed et al., “A Novel Blockchain Based Secured and QoS Aware IoT Vehicular Network in Edge Cloud Computing,” *IEEE Access*, vol. 10, pp. 77707-77722, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Usman Khalil et al., “A Blockchain Footprint for Authentication of IoT-Enabled Smart Devices in Smart Cities: State-of-the-Art Advancements, Challenges and Future Research Directions,” *IEEE Access*, vol. 10, pp. 76805-76823, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Yulei Jiao, and Cexun Wang, “A Blockchain-Based Trusted Upload Scheme for the Internet of Things Nodes,” *International Journal of Crowd Science*, vol. 6, no. 2, pp. 92-97, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Shahbaz Siddiqui et al., “Toward Software-Defined Networking-Based IoT Frameworks: A Systematic Literature Review, Taxonomy, Open Challenges and Prospects,” *IEEE Access*, vol. 10, pp. 70850-70901, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Xiaoying Jia et al., "A Blockchain-Assisted Privacy-Aware Authentication Scheme for Internet of Medical Things," *IEEE Internet of Things Journal*, vol. 9, no. 21, pp. 21838-21850, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Bandar Alamri, Katie Crowley, and Ita Richardson, "Blockchain-Based Identity Management Systems in Health IoT: A Systematic Review," *IEEE Access*, vol. 10, pp. 59612-59629, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Victor Ribeiro et al., "A Fault-Tolerant and Secure Architecture for Key Management in LoRaWAN Based on Permissioned Blockchain," *IEEE Access*, vol. 10, pp. 58722-58735, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Tianchen Ma et al., "Toward Data Authenticity and Integrity for Blockchain-Based Mobile Edge Computing," *IEEE Sensors Journal*, vol. 22, no. 10, pp. 9967-9980, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Yi Yang et al., "An Efficient Identity-Based Aggregate Signcryption Scheme with Blockchain for IoT-Enabled Maritime Transportation System," *IEEE Transactions on Green Communications and Networking*, vol. 6, no. 3, pp. 1520-1531, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Reyazur Rashid Irshad et al., "IoT-Enabled Secure and Scalable Cloud Architecture for Multi-User Systems: A Hybrid Post-Quantum Cryptographic and Blockchain-Based Approach toward a Trustworthy Cloud Computing," *IEEE Access*, vol. 11, pp. 105479-105498, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] Hayam Alamro et al., "Modeling of Blockchain Assisted Intrusion Detection on IoT Healthcare System Using Ant Lion Optimizer with Hybrid Deep Learning," *IEEE Access*, vol. 11, pp. 82199-82207, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Xiaofeng Xu et al., "A Novel Resource-Saving and Traceable Tea Production and Supply Chain Based on Blockchain and IoT," *IEEE Access*, vol. 11, pp. 71873-71889, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] Jinwen Xi et al., "A Blockchain Dynamic Sharding Scheme Based on Hidden Markov Model in Collaborative IoT," *IEEE Internet of Things Journal*, vol. 10, no. 16, pp. 14896-14907, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] Pramitha Fernando et al., "Distributed-Proof-of-Sense: Blockchain Consensus Mechanisms for Detecting Spectrum Access Violations of the Radio Spectrum," *IEEE Transactions on Cognitive Communications and Networking*, vol. 9, no. 5, pp. 1110-1125, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] Soubhagya Ranjan Mallick et al., "BCGeo: Blockchain-Assisted Geospatial Web Service for Smart Healthcare System," *IEEE Access*, vol. 11, pp. 58610-58623, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[18] B. Chitradevi et al., "Reimagining Point-of-Care Ultrasound with Convolutional Neural Networks and Cloud Computing for Healthcare Transformation," *2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM)*, Noida, India, vol. 11, pp. 54476-54494, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[19] Hancheng Gao et al., "Blockchain-Enabled Fine-Grained Searchable Encryption with Cloud–Edge Computing for Electronic Health Records Sharing," *IEEE Internet of Things Journal*, vol. 10, no. 20, pp. 18414-18425, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] Hasan Mujtaba Buttar et al., "Countering Active Attacks on RAFT-Based IoT Blockchain Networks," *IEEE Sensors Journal*, vol. 23, no. 13, pp. 14691-14699, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[21] Rekha Goyat et al., "BENIGREEN: Blockchain-Based Energy-Efficient Privacy-Preserving Scheme for Green IoT," *IEEE Internet of Things Journal*, vol. 10, no. 18, pp. 16480-16493, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[22] Zeeshan Raza, Irfan Ul Haq, and Muhammad Muneeb, "Agri-4-All: A Framework for Blockchain-Based Agricultural Food Supply Chains in the Era of Fourth Industrial Revolution," *IEEE Access*, vol. 11, pp. 29851-29867, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[23] Jing Huey Khor et al., "Public Blockchain-Based Data Integrity Verification for Low-Power IoT Devices," *IEEE Internet of Things Journal*, vol. 10, no. 14, pp. 13056-13064, 2023. [CrossRef] [Google Scholar] [Publisher Link]