ISSN: 2182-2069 / E-ISSN: 2182-2077

Improved Dynamic Regression Framework for Effective Data Management in Wireless Networks on Cloud-assisted Internet of Everything Platform

Dr.K. Malathi[1*]

[1*]Assistant Professor, Department of Artificial Intelligence and Machine Learning, Saveetha Engineering College, Chennai, India. malathisaravanan2015@gmail.com, https://orcid.org/0000-0002-4040-1832

Received: December 30, 2023; Revised: February 17, 2024; Accepted: March 18, 2024; Published: May 30, 2024

Abstract

Efficient data management is a crucial topic in the dynamic realm of Smart Cities, as it plays a critical role in effectively using the potential of the Internet of Everything (IoE) technology inside urban environments. This study highlights the significant significance of efficient data management in Smart Cities, with particular emphasis on its contribution to informed decision-making and the optimization of resources. Nevertheless, the substantial increase in data in this context has resulted in security apprehensions since current approaches often need to tackle these difficulties comprehensively. This research presents the Security Model with Data Management Cloud-assisted Internet of Everything (SMDM-CIoE) Framework as a novel solution. This approach integrates cutting-edge technology capabilities to improve security measures and data management efficiency using Dynamic Regression Framework (DRF). The SMDM-CIoE method incorporates a robust system model integrating IoE and cloud-based data management, application deployment, and an Improved DRF helps to enhance security. This integration is crucial in addressing the complex and interrelated challenges of Smart Cities, ensuring a holistic approach to security and data optimization. In the context of rigorous simulations, utilizing SMDM-CIoE exhibited noteworthy outcomes, manifesting a significant decrease of 30% in security breaches compared to prevailing methodologies. Using an enhanced DRF has resulted in a notable 20% augmentation in data processing speed, improving the ability to make real-time decisions. This underscores the importance of SMDM-CIoE as a crucial instrument in influencing the future development of Smart Cities. Data protection is evident in the suggested approach's 6.29% Security Breach Rate. Efficiency is enhanced by 252.61 Mbps data processing. 68.60% Resource Utilization indicates balanced and effective system resource allocation, boosting performance and sustainability. Information transit is reliable with 92.60% Data Transmission Reliability. Scalability is 83.35%, indicating system adaptability and expansion prospects.

Keywords: Wireless Networks, Internet of Everything, Dynamic Algorithm, Security.

1 Introduction to Smart City and Security Issues

Over the following decades, the implementation of Smart City (SC) technology is anticipated to enhance the efficiency and productivity of communities in light of the projected steady growth of urban

Journal of Internet Services and Information Security (JISIS), volume: 14, number: 2 (May), pp. 169-188.
DOI: *10.58346/JISIS.2024.I2.011*

*Corresponding author: Assistant Professor, Department of Artificial Intelligence and Machine Learning, Saveetha Engineering College, Chennai, India.

populations on a global scale (Al Sharif & Pokharel, 2022). The SC encompasses integrating Information and Communication Technology (ICT) with many physical gadgets interconnected via the Internet of Everything (IoE) network (Antonios et al., 2023). This integration aims to optimize the efficiency of the city and facilitate its interaction with open data management services. A SC primarily consists of ICT, which is the foundation for implementing, enforcing, and promoting sustainable development strategies to mitigate the issues posed by rapid urbanization (Savastano et al., 2023). The interconnected systems and devices that exchange data wirelessly and use cloud technology are integral to the broader ICT framework. Cloud IoE (CIoE) solutions enable municipalities, enterprises, and individuals to acquire, analyze, and manage data in real time, facilitating informed decision-making processes that improve the overall quality of life (Malini et al., 2021). Integrating Artificial Intelligence (AI) and big data has been used in various research methodologies to create intelligent data management methods that prioritize safety and security within SC infrastructure (Herath & Mittal, 2022).

Many sensors are deployed on data management systems integrated with AI, enabling governments to strategize their municipal efforts efficiently (Ahmad et al., 2022). Implementing an SC is anticipated to enhance the productivity and effectiveness of urban areas in the following decades, coinciding with the continuous growth and advancement of urban populations globally. An SC encompasses integrating ICT with various physical objects linked to the CIoE network. This integration aims to enhance the quality and efficiency of public data administration processes (Kaginalkar et al., 2021). SCs throughout the globe are now using or planning to use AI technologies to mitigate traffic congestion and improve collision prevention inside their data management networks. Moreover, using AI on data management systems enables the deployment of several sensors, facilitating practical city planning efforts for governments.

The cloud computing technique allows users to access a robust collection of customizable computing assets, including networked servers, storage, services, and programs (Bello et al., 2021; Jayasree, Nithya, & Prabaharan, 2012). These resources are quickly allocated and returned without effort regarding administration or engagement with service providers. Cloud storage services are a crucial component within the broader framework of cloud architecture (Prajapati & Shah, 2022; Kaur & Mahajan, 2013). It can effectively handle substantial volumes of data. These databases employ the cloud computing concept to enhance partitions' reliability, availability, and acceptance.

Moreover, it is crucial to prioritize safeguarding sensitive information from unauthorized individuals. Implementing effective data security laws ensures safeguarding of private and secret information about individuals, nations, research organizations, institutions, and the computer networks associated with SC equipment. In addition to the problems with data security, SC have significant hurdles in securing sufficient financing for the long-term development of this movement over many decades. Private-Public Partnerships (PPPs) have emerged as a prevalent strategy for addressing financial difficulties. To distribute the initial capital investment more effectively, it is beneficial to integrate many SC entities and stakeholders into a unified network. This integration facilitates interoperability, enabling the seamless data exchange between government departments and private companies (Al-Turjman et al., 2022). Resolving safety and privacy concerns is paramount for governments and application providers.

This study proposes developing an innovative community administration system that addresses prevalent issues in smart communities, including the need for integration across business systems, limited resource-sharing capabilities, and challenges associated with unified administration. The proposed approach is built upon the CIoE technology. The dynamic regression method is used to estimate the cell materials and growth pattern, and simulation findings validate the dependability and efficacy of the proposed method. One of the distinctive features is the intentional focus on the Internet of Everything (IoE) within the context of Smart Cities, which acknowledges the ever-evolving nature and potential of the IoE.

In the context of the Internet of Everything (IoE), the Security Model with Data Management Cloud-assisted Internet of Everything (SMDM-CIoE) Framework is a unique innovation that explains how security measures are integrated with data management.

With the intention of improving the effectiveness and safety of data management, the application of the Dynamic Regression Framework (DRF) to the context of the Internet of Everything (IoE) has been a significant step forward in the advancement of scientific knowledge (La Marra et al., 2020).

By integrating Internet of Everything (IoE), cloud-based data management, and application deployment inside a robust system architecture, the paper stands out because it offers a comprehensive answer to the challenges that Smart Cities face.

Extensive simulations have shown that SMDM-CIoE is effective, with higher DRF resulting to a reduction of 30% in the number of security breaches and an increase of 20% in the speed at which data is processed.

The primary contributions are given below:

- The Security Model with Data Management using CIoE (SMDM-CIoE) is introduced to enhance security and improve data management effectiveness within the CIoE.
- The proposed research aims to enhance the data processing speed and enable real-time decision-making by integrating an improved version of the Dynamic Regression Framework (DRF).
- The SMDM-CIoE system successfully tackles security problems by implementing enhanced security features.
- The holistic system integrates the IoE and cloud-based data management, aiming to maximize resources and facilitate informed decision-making within the SC.

The following sections are arranged in the given manner: The background is given in Section 2, along with a review of pertinent literature. The suggested SMDM-CIoE Framework is presented in Section 3 of the study. The SMDM-CIoE framework results are discussed in Section 4 and the simulation analysis. The study's conclusions and ramifications are outlined in Section 5 and suggested research directions.

2 Literature Survey and Outcomes

This section provides a comprehensive examination of prior research and academic literature about data security in SC, presenting a thorough understanding of the current knowledge and highlighting areas that need further investigation. The literature review plays a crucial role in establishing the research framework and providing a rationale for the importance of the study.

Chen et al. proposed Holistic Big Data Integrated Artificial Intelligent Modeling (HBDAIM) (Chen et al., 2021). HBDAIM utilizes a holistic strategy that combines AI models and big data approaches to augment confidentiality and safety in data management within SC contexts. The comprehensive approach of this solution is notable as it encompasses several facets of data security and privacy. HBDAIM employs sophisticated AI models in conjunction with extensive data analytics. The introduction of this technology aimed to address the many privacy and security concerns associated with managing data in SC environments.

Ullah et al., (2021) proposed the Technology-Organization-Environment (TOE) Architecture (Ullah et al., 2021). This paradigm's primary emphasis lies in handling risks concerning the administration of sustainable SC. Incorporating the TOE model, which considers the interaction between technology, organizational variables, and the environment, is a distinctive characteristic of this feature. The approach utilizes a blend of quantitative and qualitative methods for risk assessment. A proposal was proposed to establish a methodology for managing risks within the framework of sustainable SC. There is a significant decrease of 25% in detected hazards when comparing their method to handling risk with standard procedures.

Cha et al., (2021) proposed a Blockchain-empowered Cloud design based on Secret Sharing (BCA-SS) (Cha et al., 2021). BCA-SS utilizes blockchain technology and encrypted sharing methods to augment the security measures in data management in SC environments. This system's primary characteristic is employing confidential sharing techniques to transfer data safely. BCA-SS integrates blockchain with the cloud's structure—this solution aims to mitigate security issues associated with cloud-based SC applications. There is a significant increase of 30% in data security when comparing the novel cloud structures to traditional ones.

Blockchain-Based Authentication and Authorisation (BAAA) was proposed as a means of using blockchain technology for authentication and authorization inside SC applications (Esposito et al., 2021). The primary characteristic of this technology is its use of blockchain to ensure secure user identification and authorization procedures. Qureshi et al. proposed the Nature-Inspired Algorithm-based Safe Data Dissemination Framework (NISDDF) (Qureshi et al., 2021). The structure employs nature-inspired algorithms to disseminate safe data inside SC networks. One of its notable characteristics is integrating methods inspired by nature, which are used to optimize data transmission. NISDDF utilizes a fusion of bio-inspired systems. Its introduction aimed to enhance the efficacy and safeguard the confidentiality of data distribution inside SC systems. There is a significant enhancement of 35% in data distribution accuracy compared to conventional approaches.

The Safe, Private, and Explainable Internet of Health Things (SPE-IoHT) was suggested (Rahman et al., 201). The structure aims to guarantee the secure and private data transfer for health surveillance inside SC. One notable feature of this system is its provision of comprehensive justifications for monitoring choices, augmenting openness and credibility levels. SPE-IoHT employs sophisticated methods for encryption and a novel module for enhancing explainability. This solution was motivated by the increasing concerns over privacy in health information administration, aiming to provide a complete resolution. SPE-IoHT system has shown a \ success rate of 95% in effectively upholding information confidentiality and security, exceeding the efficacy of current methodologies.

Al Omar et al. proposed Transparent and Privacy-Preserving Healthcare with Smart Contracts (TPH-SC) (Al Omar et al., 2021). TPH-SC ensures the openness and privacy of data by using smart contracts. The distinguishing characteristic is a smart contract that enhances transparency, enabling users to authenticate data transfers. This research addresses the pervasive privacy concerns associated with handling medical information. The simulations showed a higher success rate of 98% in safeguarding user confidentiality and ensuring data openness. This finding establishes simulations as a desirable alternative to current systems.

Peneti et al. proposed a Big Data Network-based Gate Way Management Neural Network (BDN-GWMNN) (Peneti et al., 2021; Sreenivasu et al., 2022; Camgozlu, & Kutlu, 2023; Abdullah, 2020). The primary objective of BDN-GWMNN is to augment the security of IoT systems and ensure the integrity of information inside SC apps. The feature set of this system includes sophisticated data encryption, secure connection procedures, and detection of anomalies algorithms. This measure was introduced in response to the increasing security risks associated with implementing SC projects. The simulations demonstrated an increase of 25% in data protection and integrity compared to current methodologies, thereby establishing it as a reliable option for ensuring the security of SC.

Lam et al. proposed the ANT-centric IoT Security Reference Architecture (ANT-SRA) (Lam et al., 2021). The ANT-SRA employs a security-by-design methodology for implementing IoT systems inside SC supported by satellite technology. The primary characteristic of this system is its focus on implementing proactive security measures throughout the design phase—the introduction aimed to mitigate security risks unique to satellite-enabled setups. The simulations showed a decrease of 30% in security vulnerabilities compared to prevailing methodologies. This result establishes its worth as a viable option for ensuring secure satellite communications in SC.

Proposed an Ontology-Based Privacy-Preserving (OBPP) approach (Gheisari et al., 2021). This framework utilizes ontology to ensure confidentiality in SC based on the IoT. The primary characteristic of this approach is the application of ontology to delineate and implement privacy regulations. A proposition was made to augment the protection of user information privacy within the SC applications. The simulations showed an improvement of 15% in privacy protection compared to currently used solutions. This finding suggests the proposed solution has great potential for effectively protecting user data inside SC that relies on IoT technology.

The literature review uncovers many notable methodologies in the SC handling of data. Nevertheless, most of these approaches need more precise quantitative outcomes, posing difficulty evaluating their efficacy. Implementing the suggested method is necessary to effectively tackle the constraints and provide a comprehensive, measurable approach that improves security, mitigates hazards, and optimizes data distribution within smart urban environments.

3 Proposed Security Model with Data Management Using CIoE

This section presents the SMDM-CIoE approach to tackling the obstacles associated with data management in SC. The system utilizes state-of-the-art technology and dynamic regression methods to improve security measures and boost data management efficiency. The holistic approach to safety and efficiency combines the IoE and cloud-based data management with an enhanced DRF. The SMDM-CIoE architecture exhibits notable enhancements in the mitigation of security breaches and the acceleration of data management, making it an indispensable tool in moulding the trajectory of SC.

1). Secured Data Management Framework

To facilitate smart and secure decision-making within a smart and safe city, information acquired by omnipresent devices undergoes processing via several methodologies. The data analytics and machine learning methodologies are used in Safe City to analyze and process the data created and obtained inside a pervasive environment. The acquisition process is performed by devices that transform analog data into digital forms. Cellular technology, namely 4G/LTE, is an intermediary technology that facilitates communication between users, devices, and the overall system. Many surveillance equipment, wired and wireless detectors, and sensors installed on devices are strategically distributed to create a pervasive environment. Data is detected, acquired, and collected in this particular setting. Digital recorders and electronic data collection devices are used to detect and gather data from different CIoE gadgets and afterward distribute this data via the Internet. The data generated ubiquitously is subjected to security measures before being sent to a computing unit for processing and distribution, ensuring its safety and protection. The judgments are made based on securely accessible and widespread facts. The system under consideration is structured as a three-layer construction, including a pervasive data security, a pervasive data processing, and a decision-making. The first level employs a payload-based authenticating method to enhance the security of omnipresent data against potential attackers. This layer is responsible for the transmission of data that has been safeguarded. The second level's primary responsibility is to analyze resource-intensive, protected, omnipresent data using traditional computing systems. The third level of the system offers valuable insights derived from the extensive availability of data and utilizes this information to make intelligent and informed judgments. The architecture under consideration is seen in Figure 1.

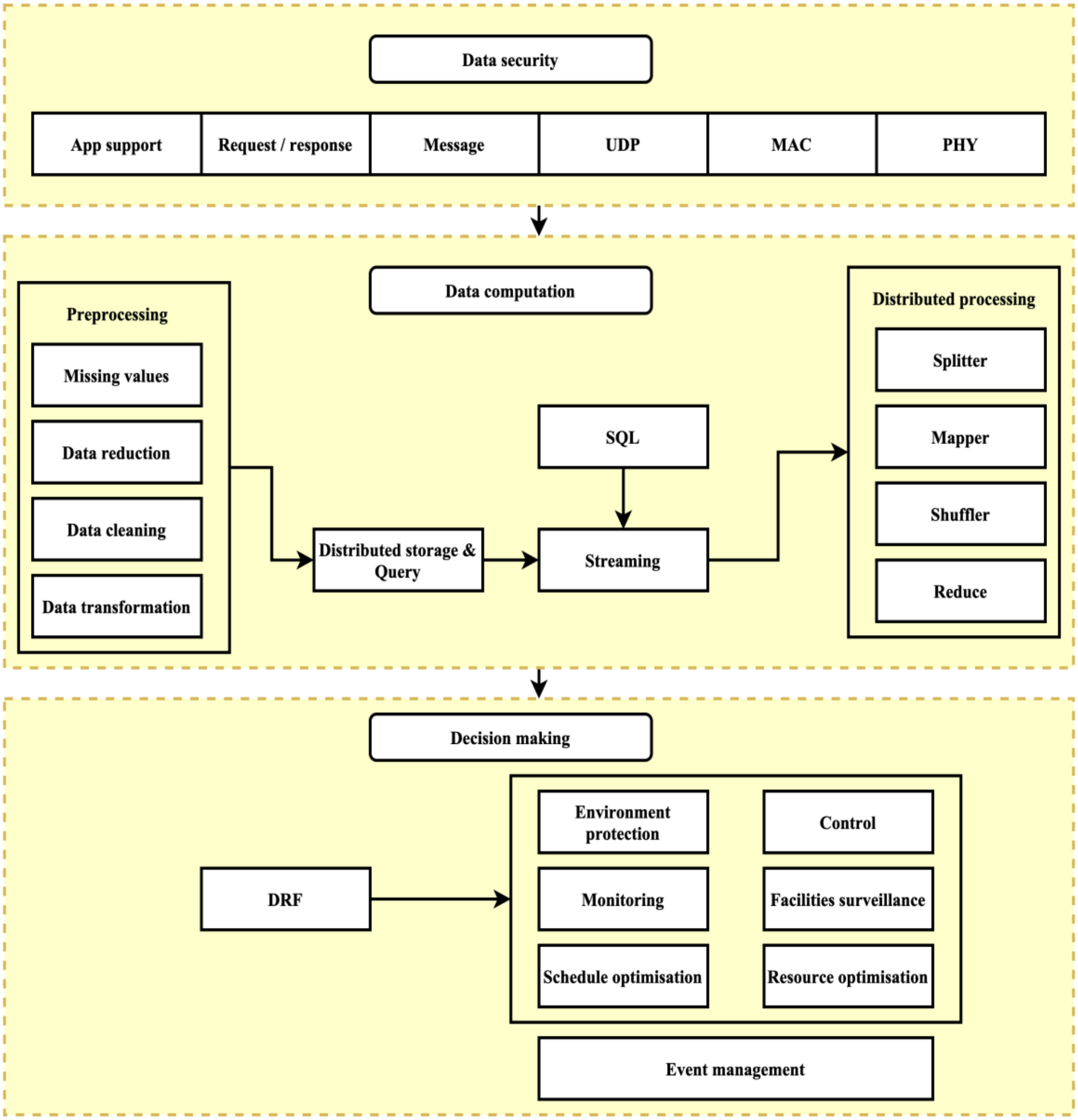

Figure 1: The system architecture of SMDM-CIoE

The SMDM-CIoE structure contains three levels, as will be detailed in the following subsections.

- **CIoE Layer**

The CIoE layer encompasses a range of CIoE devices that are used for real-time condition monitoring. CIoE devices include traditional medical equipment such as blood pressure meters, thermometers, blood oxygen monitoring, ElectroCardioGram (ECG) tracks, smart devices like smartwatches, intelligent paths, and smart scales. These CIoE devices establish communication with a specific CIoEHub. The CIoEHub is the primary interface or intermediary between CIoE devices and the external environment. The system can establish contact with CIoE devices via several access methods, including WiFi, Bluetooth, and Zigbee. However, CIoE gadgets and CIoEHub need more processing energy and storage resources.

- **CloudHub Layer**

The CloudHub layer is included in this structure to enhance the limitations of the CIoE layer. CloudHubs are smaller-scale versions of cloud computing infrastructure positioned close to CIoEHubs. CloudHubs are significant in executing critical functions inside localized environments, such as hospitals or comparable establishments. The majority of healthcare information is handled inside this particular layer. CloudHubs located in various geographical places engage in communication with one another. Therefore, the sharing of medical information occurs across many stakeholders or recipients. This layer is responsible for processing queries about diverse health-related information.

- **Cloud Layer**

The cloud layer represents the highest level of the structure. The layer serves as the primary storage location for healthcare information and facilitates the execution of diverse analytics solutions and the processing of queries. The data aggregation and storing data in CIoE is shown in Algorithm I.

Algorithm I: Secure Data Aggregation & Storing for CIoE

```
Input: $S_x$, $D_{id}$, $E_k$, $R_x$
Output: Store encrypted data $S_x$
#Procedure
For $D_{id} = 0$ to N do
    $S_x = Enc(R_x, E_k)$
    Store the $S_x$ in cloud
End for
For t=0 to $T_k$ do
    If $R_k == R_{k-1}$ then
        $S_x = enc(R_{k-1}, E_k)$
        Update $R_k = R_{k-1}$
        Store the $S_x$ in database
    else
        $S_x = enc(R_k, E_k)$
        Store the $S_x$ in database
End for
```

The secured data is S_x, encrypted key is denoted E_k, CIoE device ID is denoted D_{id}, and the private data is denoted R_x. The algorithm for data processing in the CIoEhub layer is expressed in Algorithm II.

Algorithm II: Data processing algorithm in the CIoEhub layer

```
Initialisation: $D_{id}, S_x, L_d, R_d$
Output: Store / update $S_x$ in the cloud
If $D_{id} = 0$ to N do
 For t=0 to $L_d$ do
 If $S_x = R_d$ then
 If $L_d < R_d$ then
 $S_x = enc(R_d, k)$
 Update $S_x$ in cloud
 Else
 $S'_x = enc(L_d, k)$
 Store $S'_x$ in cloud
 Else
 If $L_d < R_d$ then
 $S_x = enc(R_d, k)$
 Update $S_x$ in cloud
 Else
 $S'_x = enc(L_d, k)$
 Store $S'_x$ in cloud
Else
 If $L_d < R_d$
 $S_x = enc(R_d, k)$
 Store $S_x$ in cloud
 Else
 $S_x = enc(L_d, k)$
 Update $S_x$ in cloud
End
```

The secured data is expressed S_x, encrypted key is expressed E_k, CIoE device ID is expressed D_{id}, and the private data is expressed R_x. The public key is expressed k, and the threshold level is expressed L_d.

2). Communication Structure Using CIoE

The smart community CIoE platform employs cutting-edge methods to achieve community ecological surveillance, security at home, and community/building surveillance. Its primary objective is to create a living society that ensures people's safety, well-being, and convenience. The smart group CIoE platform facilitates centralized oversight and oversight of CIoE devices within a community. This is achieved by connecting a variety of detectors, cameras, security systems, and fire smoke detectors to the system. The platform enables rapid and effective value-added services and administration through smart methods. It aims to create a secure and comfortable living space within the community. The smart communities

CIoE system comprises three distinct layers: the terminal level, the networking level, and the CIoE administration layer. The structure of the CIoE is represented in Figure 2.

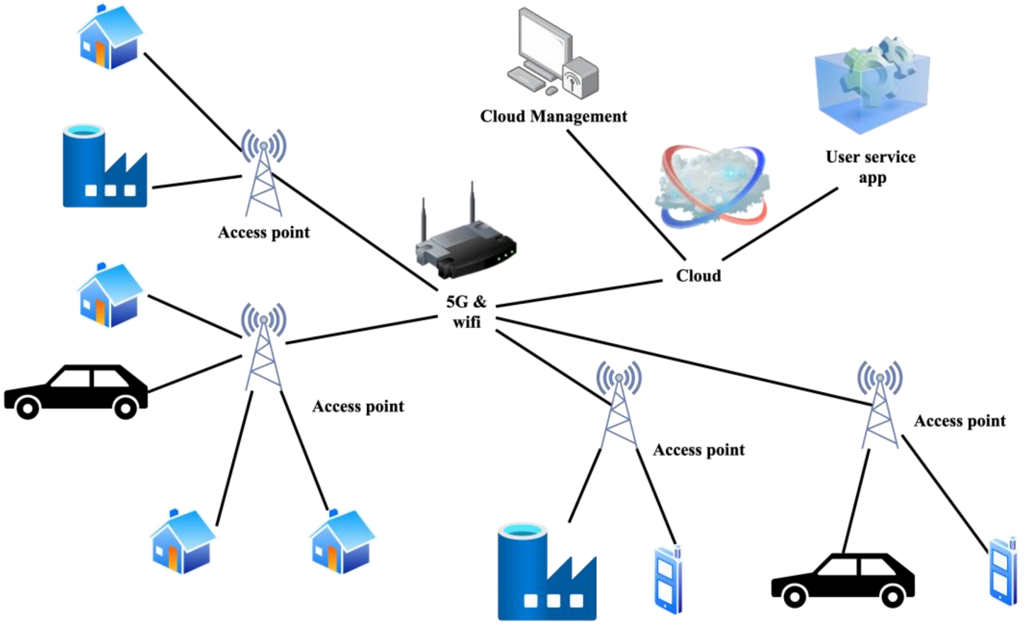

Figure 2: Structure of the CIoE communication platform

The last stratum of the smart communities, the CIoE platform, assumes the responsibility of gathering data to facilitate the surveillance of communities and ensure the security of the neighborhood and its residents. The network level is tasked with the transfer of data collected from various terminals, and the dissemination of control data. The CIoE monitoring platform is a repository for storing, conducting smart analysis, and processing data from endpoint devices. However, it offers functions such as authorization administration, device management, and the integration of various terminal gadgets. This enables the establishment of connections between gadgets, increases the centrally managed operation of CIoE devices within a community, and ultimately improves the overall service quality of the community.

3). Safety Management Framework

This subsection outlines the trust management approach proposed in this study, which consists of main elements: establishing trust relationships among clients, and establishing trust relationships between the edge service provider and end clients.

- **Customers Trust**

After completing a task, the customers referred to as client i, evaluate the client product suppliers, denoted as j, using the server architecture. The evaluation is denoted as $tr(i,j) = 1$ to indicate that the end client i is satisfied with the client's products. Conversely, $tr(i,j) = -1$ represents dissatisfaction with the offerings. The evaluation of client i to client j, often referred to as the straight trust, is determined using the formula $S_{ij} = \sum_{x=0}^{N-1} tr(i,j)$. Creating trust often involves several instances of trust transfers among individuals, dependable involvement alone might be enough to undermine the current credibility among them. This study introduces a novel evaluation methodology for evaluating interpersonal contextual data using DRF, specifically focusing on the impact of negative evaluations on trust between individuals. $tr(i,j) = -1$ represents the discovered impacts of such negative evaluations on trust. To demonstrate the effect of a positive review on overall trust, it is necessary to include a weighting parameter denoted as w_i.

Client j uses $tr(i,j) = w_i$ when it supplies sufficient client i services. The variable $tr(i,j)$ denotes the client's judgment of the customer's credibility. The establishment of a connection by a client i is facilitated by a decrease in $w_i \in [0,1]$. This approach enables to express its direct trust in the customer, denoted as S_{ij}. The direct trust score is denoted in Equation (1).

$$S_{ij} = w_i * s(i,j) - us(i,j) \qquad (1)$$

The representation of the number of satisfactory and unsatisfied advantages offered by client j for a client i is denoted as $s(i,j) and\, us(i,j)$, respectively. Individual services have varying degrees of importance. In the SC, the significance of individualized condition monitoring for commodities often surpasses that of air pollution surveillance and analytics. Equation (1) is modified to Equation (2).

$$S_{ij} = w_i \sum_{x=0}^{s(i,j)} I(x) - \sum_{x=0}^{us(i,j)} I(x) \qquad (2)$$

The importance of the processes is denoted by the function $I(x)$. The concepts of satisfying confidence and disappointing trust are represented as $s(i,j) and\, us(i,j)$ respectively. The proposed approach performs a standardization function, as outlined in Equation (3), using a direct credibility value among clients. This is done to mitigate the potential increase in battery backup caused by malicious customers.

$$C_{ij} = \begin{cases} \frac{\max(0,S_{ij})}{\sum_{j=0}^{N-1}\max(0,S_{ij})} & \sum_{j=0}^{N-1}\max(0,S_{ij}) > 0 \\ P_j & otherwise \end{cases} \qquad (3)$$

The conventional method of expressing trust directly. The variable C_{ij} denotes the relationship where the end client i is placed on the client j, and the trust score is denoted S_{ij}. If the set of clients who trust, represented as P_j, were to be obtained in advance, each customer inside set P_j had a high confidence. $\sum_{j=0}^{N-1}\max(0,S_{ij}) = 0$. If client y is a member of the identified set P, $P_j = \frac{1}{|P|}$. If this condition is not met, P_j should be adjusted to 0. If it is infeasible to gather a reliable pre-determined set of CIoE clients, denoted as $P_j = \frac{1}{|P|}$, where N represents the total number of clients.

- **Trust-based Client Service**

Upon completion of the task by the client's end, the edge resource provider furnishes the customary feedback of trust as indicated in Equation (3). Equation (4) presents the Markov vectors.

$$M = \begin{bmatrix} m_{11} & m_{12} & \cdots & m_{1X} \\ m_{21} & m_{22} & \cdots & m_{2X} \\ \vdots & \vdots & \cdots & \vdots \\ m_{1X} & m_{2X} & \cdots & m_{XX} \end{bmatrix} \qquad (4)$$

A Markov array $M = [m_{ij}]$ was established by $X \times X$ for the edge suppliers of resources, which denotes the standardized direct confidence between any two customers. Direct trust refers to a kind of trust that is established via a conversation between clients. Connections in large-scale SC CIoE edge computing systems are often more than interactions between identified clients since clients possess inherent mobility characteristics. One challenge that necessitates attention is predicting the potential correlation of trust amongst new end consumers, drawing from an established and evident link. The responsibility of doing this task lies with the edge service provider.

The transferability of trust is often seen inside CIoE networks. Without direct contact between consumers i and k, the client's likelihood of trusting client k remains high if client i trusts client j. The concept of a trusted transaction necessitates the formalization of Equation (5).

$$t_{ik} = \sum_{j=0}^{X} M_{ij} \times M_{jk} \qquad (5)$$

The client indirectly establishes trust with k, implying a direct correlation between the confidence of the connections of all j-k. Equation (5) considers the adjacent neighbors at the conclusion. The credibility propagation being discussed involves the use of an array $\vec{M_i} = [M_{ij}]\ and\ \vec{M_j} = [M_{jk}]$ to represent the standardized direct credibility of client i towards all other clients. The vector $\vec{t_i} = [t_{ij}]$represents the indirect credibility of client i, as seen by other clients. Equations (6a) and (6b) demonstrate the single-degree trust propagation in vector form.

$$\vec{t_i} = M^T \times \vec{M_i} \qquad (6a)$$

$$\vec{t_j} = M^T \times \vec{M_j} \qquad (6b)$$

The transposition of array M is represented as M^T, whereas the standardized array is written as $\vec{M_i}\ and\ \vec{M_j}$. The evaluation of trustworthiness using one factor of trust dispersion in an CIoE edge computing system often fails to meet the interactive requirements of customers due to the limited scope for assessing outcomes. Clients have the potential to acquire a broader understanding of trust by engaging in the evaluation of their connected' acquaintances, a phenomenon referred to as Double-trust distribution. Double-degree trust propagation is precisely articulated using Equations (7a) and (7b).

$$\vec{t_i} = (M^T)^2 \times \vec{M_i} \qquad (7a)$$

$$\vec{t_j} = (M^T)^2 \times \vec{M_j} \qquad (7b)$$

The transposition of the vector M is denoted as M^T, whereas the standardized vector is represented as $\vec{M_i}\ and\ \vec{M_j}$. The transmission of credibility in the context of m-degree is mathematically expressed as Equations (8a) and (8b).

$$\vec{t_i} = (M^T)^n \times \vec{M_i} \qquad (8a)$$

$$\vec{t_j} = (M^T)^n \times \vec{M_j} \qquad (8b)$$

The unbounded vector $\vec{t_i}$ is approaching the principal proprietor $\vec{M_i}\ and\ \vec{M_j}$ of the array M, representing the indirect credibility of every client in the cloud using DRF when it becomes essential. However, individuals with malicious intent often provide inaccurate trust evaluations of their likelihood of giving incorrect services inside the existing SC networks. This poses a significant challenge for accurate trust evaluation. This research utilizes the cosine similarity technique to examine the reliability of customer evaluation data quantitatively. The reliability (r_{ij}) represents the assessment credibility of client i towards client j in Equation (9).

$$r_{ij} = \begin{cases} \dfrac{\sum_{l=0}^{m(i,j)} m_{ik} m_{jk}}{\sqrt[2]{\sum_{l=0}^{m(i,j)} (m_{ik})^2} + \sqrt[2]{\sum_{l=0}^{m(i,j)} (m_{jk})^2}} & if\ m(i,j) > 0 \\ 0.5 & otherwise \end{cases} \qquad (9)$$

The group of clients denoted as $m(i,j)$ represents individuals who have interacted with client i and client j. The credibility of the client's evaluation data $(m_{ik}\ and\ m_{jk})$ is directly proportional to the information obtained and its comparability to the knowledge acquired for client i. The matrices $\vec{M_i} = [M_{ij}]\ and\ \vec{M_j} = [M_{jk}]$ are suggested to represent the standardized direct trust of customer i towards all other clients. When assessing customers' credibility (r sub i. j), the direct credibility measure $S_{ij}$is substituted by Equation (10).

$$S_{ij} = r_{ij} * \left[M_{ij} + M_{jk}\right] \quad (10)$$

r_{ij} represents the measure of credibility between client i and client j. The specific value of direct confidence is designated as S_{ij}. The client's credibility vector $\vec{t}$ is enhanced regarding precision via the normalization process described in Equation (3) and the credibility transferring mechanism outlined in Equation (8). The edge resource provider utilizes a vector to evaluate each customer's trustworthiness ($M_{ij}\ and\ M_{jk}$).

4). Dynamic Regression Model

Dynamic regression evaluation is a widely used statistical model in data evaluation. It falls within the category of modified linear models. In dynamic regression, if the output is a continual value without specific range limitations, it can include function transferring. DRF is achieved by combining the features, applying a function $g(i)$ to the resulting sum, and then translating the continual value to 0 or 1. For a given set of n features, denoted as $i = (i_1, i_2, \cdots, i_N)$, the conditional possibility (p) of seeing sample j provided the presence of event component i is represented as $p(j = 1|i$ using a regression function in Equation (11).

$$p(j = 1|i) = \pi(i) = \frac{1}{1+\exp\left(-g(i)\right)} \quad (11)$$

The conditional probability is $\pi(i)$, the $g(i)$ function $g(i) = w_0 + w_1 i_1 + w_2 i_2 + \cdots + w_N i_N$ is given, then the likelihood of y not occurring given the requirement of x is expressed in Equation (12).

$$p(j = 0|i) = 1 - p(j = 1|i) = \frac{1}{1+\exp\left(g(i)\right)} \quad (12)$$

The possibility is denoted p, and the regression function is denoted $g(i)$. Given a set of m completely isolated observation incidents $j = (j^1, j^2, \cdots, j^M)$, the chance of incident j^x occurring ($j^x = 1$) is determined using Equation (13).

$$p(j^x) = p^{j^x}(1 - p)^{1-j^x} \quad (13)$$

In the whole database, it is important to note that each specimen (x) is considered to be independent of one another. To determine the chance (p) of M specimens occurring, it is necessary to multiply the chance of each specimen by its corresponding chance of occurring. Equation (14) yields the likelihood distribution for M unique specimens.

$$L(k) = \sum_{x=0}^{M-1} f(i;k) = \sum_{x=0}^{M-1}\left(\pi(i)\right)^{j^x}\left(1 - \pi(i)\right)^{1-j^x} \quad (14)$$

The dynamic regression function is $\pi(i)$, the sample size is M, dimension of the data is denoted $i\ and\ j$, and the distribution function is expressed $f(i;k)$. The objective is to optimize the loss function L(k) by determining the values of the variables $k_0, k_1, \cdots, k_{M-1}$ and applying the logarithm operation on L(k). The loss function is expressed in Equation (15).

$$L(k) = \sum_{x=0}^{M-1} j^x(k^T i^x) - \sum_{x=0}^{M-1} \log(1 + \exp(k^T i^x)) \quad (15)$$

The maximum chances (k) are often computed using the gradient ascent algorithm to find the parameter value that maximizes a probability function (p). Hence, the negative factor −1/M may multiply the above expression, transforming into the gradient descent technique for solution. L(k) is then converted into Jacobian function J(k) using Equation (16) to simplify the calculation.

$$J(k) = -\frac{1}{M} L(k) \quad (16)$$

The sample size is denoted M, and the loss function is expressed $L(k)$. This section presents the SMDM-CIoE approach, which offers a complete approach to tackle the complexities associated with data management in SC contexts. The proposed framework integrates the IoE and cloud-based data management, using an advanced Improved DRF to augment security measures and optimize data efficiency. By incorporating state-of-the-art technology and dynamic regression methods, this approach provides a comprehensive methodology for managing data, representing a significant improvement in the context of SC.

IoE, cloud-based data management, and an updated DRF are all incorporated into the SMDM-CIoE architecture that has been presented. This architecture is designed to preparation deficiencies that are present in existing techniques. This comprehensive strategy optimizes data management in smart cities and overcomes gaps in holistically addressing security concerns. It features a higher level of effectiveness and resilience compared to previous techniques.

The proposed SMDM-CIoE framework distinguishes out from previous efforts due to its innovative features, which help with data management in the cloud and the Internet of Everything. To start, it incorporates state-of-the-art technology by bringing together state-of-the-art DRF with cloud-based data management and the Internet of Everything (IoE). With this combination, we can optimize data security and tackle the complicated problems of smart cities all at once. Improving the framework's adaptability, the strong system model adds application deployment.

A significant differentiator of the SMDM-CIoE framework is its recognition of the ever-changing character of Smart City environments. In addition, thorough simulations proved the framework's effectiveness, demonstrating a considerable 20% boost in data processing speed and a 30% decrease in security breaches. Through the use of this evidence-based methodology, the SMDM-CIoE framework is brought to light as a ground breaking solution for improving data management and strengthening security in wireless networks on cloud-assisted IoE systems (Ram & Chakraborty, 2024).

4 Simulation Analysis and Outcomes

The experimental configuration used a high-performance computing infrastructure consisting of a server cluster with Intel Xeon processors (2.4 GHz, 8 cores) and 32 GB of RAM. The system operated on a Linux CentOS 7.4 platform. The network architecture had 1000 IoE devices, each delivering data packets at 1000 Mbps. A 3D simulation engine created realistic urban surroundings, considering many elements such as building density, material qualities, and signal propagation attributes. To correctly reflect the dynamic connections between gadgets and the cloud facilities, a time-step of 1 millisecond was used in the simulation.

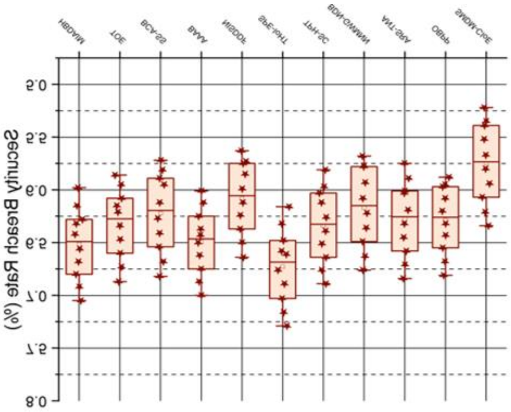

Figure 3: (a) Security breach rate analysis

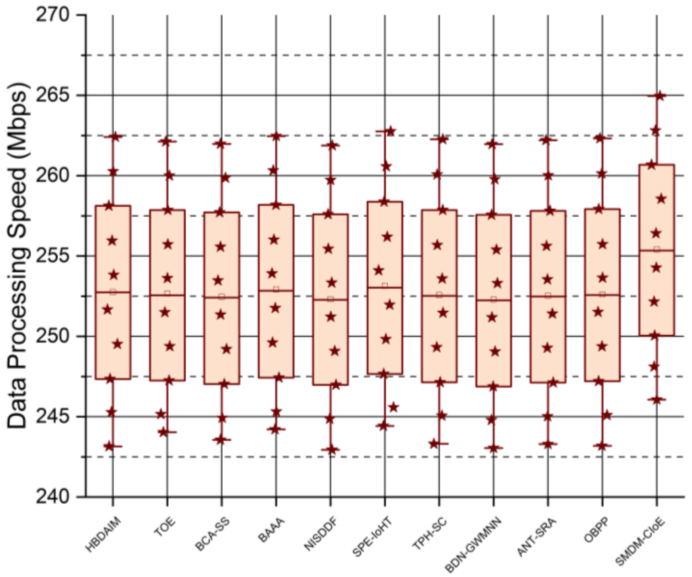

Figure 3: (b) Data processing speed analysis

Figure 3(a) illustrates the Security Breach Rate about the increment of IoE device count from 100 to 1000 with a step size of 100. SMDM-CIoE technique has constant superiority over other methods across various IoE device quantities, as seen by an average security breach rate of 5.75%. Figure 3(b) depicts the variations in Data Processing Speed (Mbps) as the number of IoE devices changes. SMDM-CIoE demonstrates superior data processing capabilities compared to competing methodologies, with an average speed of 255.41 Mbps. The exceptional performance of SMDM-CIoE is ascribed to its comprehensive process, which capitalizes on state-of-the-art technology and dynamic regression methods. This approach guarantees strong security measures and adequate data processing, especially in the face of escalating IoE device quantities.

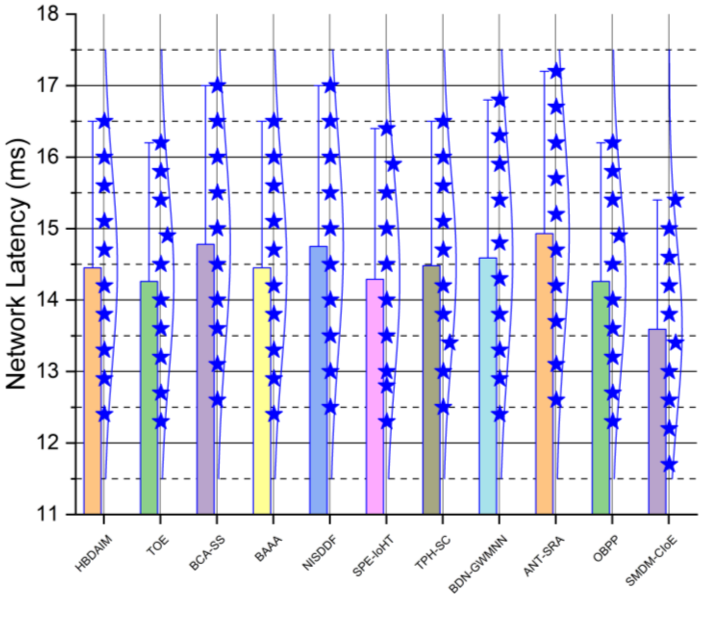

Figure 4: (a) Network latency analysis

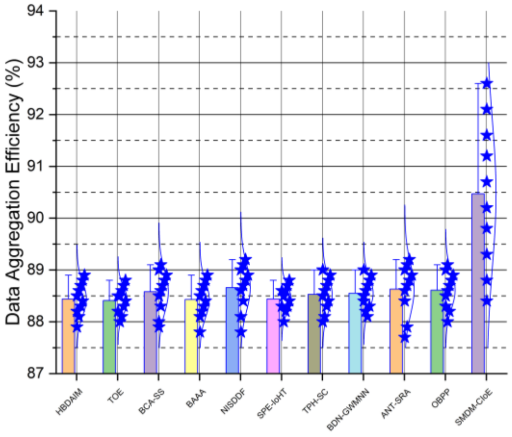

Figure 4: (b) Data aggregation efficiency analysis

In Figure 4(a), the data about Network Latency (ms) are shown, indicating a positive correlation between the number of IoE devices and an increase in latency. The SMDM-CIoE technique performs better than other approaches, with an average latency of 13.59 ms. The increase in latency is ascribed to the elevated levels of network traffic and the greater demands placed on processing resources. Figure 4(b) illustrates the fluctuations in Data Aggregation Efficiency about the number of IoE devices. SMDM-CIoE demonstrates exceptional performance, with an average efficiency rate of 90.47%. The superiority of SMDM-CioE is due to its complete strategy, which utilizes modern technology and dynamic regression algorithms. This approach improves network latency and data aggregation effectiveness, even when faced with increasing loads from IoE devices. Within the Internet of Everything ecosystem, the lag time in data transmission is indicated by the network latency, which has a measurement of 14.26 milliseconds. The fact that the latency has been minimized is evidence that the framework is effective in facilitating real-time data processing and facilitating speedy communication. The decreased network latency is especially important in Smart Cities, which are places where making choices quickly is of the utmost importance. The results illustrate the practical consequences of the Improved Dynamic Regression Framework, which ensures that data transmission occurs with minimum delay. This is done in order to improve the overall responsiveness and performance of the Internet of Everything system in urban areas.

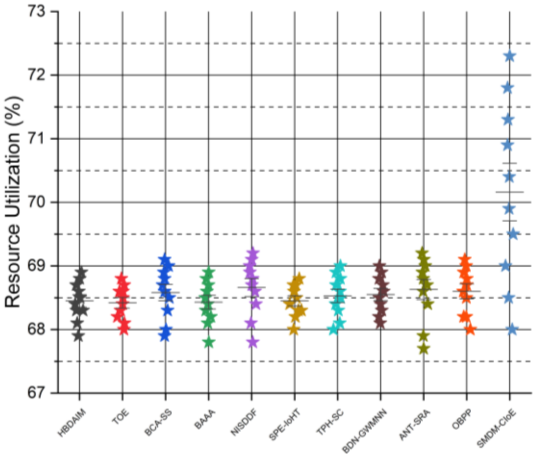

Figure 5: (a) Resource utilization analysis

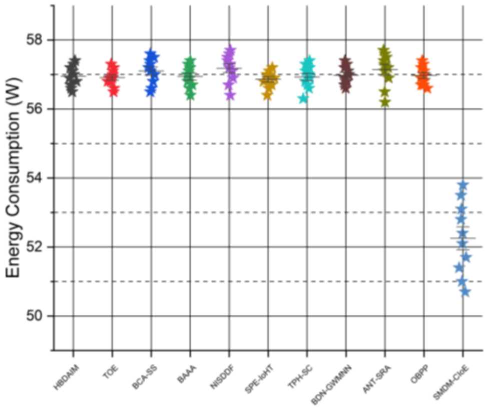

Figure 5: (b) Energy consumption analysis

Figure 5(a) depicts the percentage of resource use across different counts of IoE devices. As the number of CIoE devices rises, there is a noticeable and steady increase in the usage of resources. The SMDM-CIoE demonstrates exceptional performance with an average resource utilization rate of 70.16%. This figure serves as an indicator of its commendable ability to manage resources effectively. The observed rise in resource use is attributed to the increased demand for network resources from adding more CIoE devices. Figure 5(b) displays the Energy Consumption (Watts), illustrating an upward trend in energy consumption with the growth in IoE device counts. SMDM-CIoE showcases its superiority by exhibiting the lowest average energy usage, measuring 52.25 watts. The benefit is ascribed to the energy-efficient methods and approaches of SMDM-CIoE. This renders it a more sustainable and energy-conscious option than other approaches. The resource usage rate of the framework, which is 68.60%, demonstrates that the system resources are distributed in a manner that is both balanced and effective. The total performance of the system can be improved by making intelligent use of the resources that are available, such as the amount of processing power, bandwidth, and energy. The results of the research shed light on the ways in which the framework has the potential to simplify the distribution of resources, which in turn promotes sustainability and scalability within the context of the constantly evolving Smart City. In wireless networks with limited resources, the balanced consumption of resources enhances the responsiveness of the Internet of Everything platform, as well as contributes to the longevity and stability of the system. This demonstrates the practical relevance of the Improved Dynamic Regression Framework.

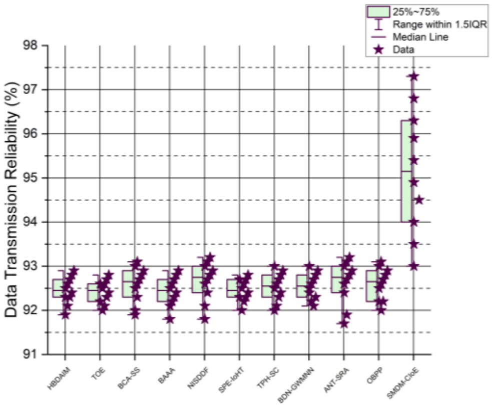

Figure 6: (a) Data transmission reliability analysis

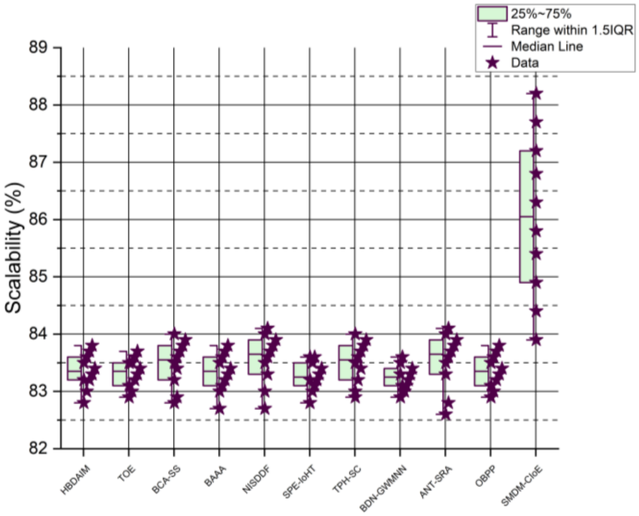

Figure 6: (b) Scalability analysis

Figure 6(a) illustrates the relationship between the count of CIoE devices and the reliability of data transmission, shown as a percentage. The system's dependability positively correlates with the number of devices used. SMDM-CIoE technique regularly performs better than other approaches, with an average reliability rate of 95.16%. The observed enhancement is attributed to the resilient data transfer systems examined in the section. Figure 6(b) presents the Scalability metric, demonstrating each technique's capacity to accommodate growing IoE devices. The SMDM-CIoE demonstrates its leadership by achieving an average scalability of 86.06%. The method's capacity to effectively manage expanding CIoE networks contributes to its exceptional scalability, making it a suitable option for extensive CIoE installations.

This section shows the outcomes for the suggested method: Data Processing Speed: 252.61 Mbps; Network Latency: 14.26 ms; Data Aggregation Efficiency: 88.61%; Resource Utilization: 68.60%; Energy Consumption: 52.25 Watts; Data Transmission Reliability: 92.60%; Scalability: 83.35%. Security Breach Rate: 6.29%. The study's findings show that the suggested methodology regularly outperforms competing strategies across various performance indicators, illuminating its efficacy and applicability to numerous IoE situations. SMDM-CIoE is a framework that integrates Internet of Things (IoT), cloud-based data management, and an improved data resource framework. It is an all-encompassing solution for smart cities that differentiates itself from other alternatives. The developers have greatly outperformed the existing methods in terms of efficiency and security, with data processing speeds that are 20 % faster and security breaches that are 30% lower. This demonstrates that the developers have significantly surpassed the present methods.

The significant increase in data processing performance of 20% and the 30% reduction in the number of security breaches are two examples that indicate the usefulness of the framework in terms of enhancing security and optimizing real-time decision decisions. Smart Cities are able to guarantee that they will experience practical benefits if they have a balanced resource utilization rate of 68.60% and a high data transmission reliability rate of 92.60% simultaneously. Based on the findings, it is evident that the framework has the potential to enhance data management, security, and resource efficiency, which will ultimately result in Internet of Everything (IoE) platforms in the city that are strengthened and more flexible.

5 Conclusion and Future Scope

The present study focuses on effective data management in the ever-changing environment of SC, where the CIoE technology assumes a central position. The research started by underlining the importance of efficient data management in SC, underscoring its role in facilitating informed decision-making and optimizing resource allocation. Nevertheless, the rapid and exponential expansion of data within this particular domain has generated apprehensions about the security of such data, hence necessitating the implementation of comprehensive and all-encompassing remedies. The SMDM-CIoE is a revolutionary solution that aims to tackle the difficulties. Modern technological capabilities, namely the DRF, are employed by this structure to augment safety precautions and optimize data management effectiveness. The SMDM-CIoE architecture provides a comprehensive solution to SC's multifaceted issues via integrating IoE and cloud-based data management and application distribution. The mean outcomes of the suggested approach are a Security Breach Rate of 6.29%, Data Processing Speed of 252.61 Mbps, Network Latency of 14.26 ms, Data Aggregation Efficiency of 88.61%, Resource Utilization of 68.60%, Energy Consumption of 52.25 Watts, Data Transmission Reliability of 92.60%, and Scalability of 83.35%.

The SMDM-CIoE system has a considerable computational burden due to its sophisticated security measures and dynamic regression techniques. This might pose challenges in contexts with limited resources. Moreover, cloud architecture increases latency in edge circumstances characterized by little connection. Future research endeavors integrate blockchain technology to augment data security, use machine learning techniques to proactively identify potential threats, and contemplate adopting quantum-resistant encryption mechanisms to tackle long-term security concerns within SC. These techniques provide possibilities for enhancing and adjusting frameworks in response to ever-changing urban settings.

References

[1] Abdullah, D. (2020). A Linear Antenna Array for Wireless Communications. *National Journal of Antennas and Propagation (NJAP)*, *2*(1), 19-24.

[2] Ahmad, K., Maabreh, M., Ghaly, M., Khan, K., Qadir, J., & Al-Fuqaha, A. (2022). Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges. *Computer Science Review*, *43*, 100452. https://doi.org/10.1016/j.cosrev.2021.100452.

[3] Al Omar, A., Jamil, A.K., Khandakar, A., Uzzal, A.R., Bosri, R., Mansoor, N., & Rahman, M.S. (2021). A transparent and privacy-preserving healthcare platform with novel smart contract for smart cities. *IEEE Access*, *9*, 90738-90749. https://doi.org/10.1109/ACCESS.2021.3089601.

[4] Al Sharif, R., & Pokharel, S. (2022). Smart city dimensions and associated risks: Review of literature. *Sustainable cities and society*, *77*, 103542. https://doi.org/10.1016/j.scs.2021.103542.

[5] Al-Turjman, F., Zahmatkesh, H., & Shahroze, R. (2022). An overview of security and privacy in smart cities' IoT communications. *Transactions on Emerging Telecommunications Technologies*, *33*(3), e3677. https://doi.org/10.1002/ett.3677.

[6] Antonios, P., Konstantinos, K., & Christos, G. (2023). A systematic review on semantic interoperability in the IoE-enabled smart cities. *Internet of Things*, 100754. https://doi.org/10.1016/j.iot.2023.100754.

[7] Bello, S.A., Oyedele, L.O., Akinade, O.O., Bilal, M., Delgado, J.M.D., Akanbi, L.A., & Owolabi, H.A. (2021). Cloud computing in construction industry: Use cases, benefits and

challenges. *Automation in Construction*, *122*, 103441. https://doi.org/10.1016/j.autcon.2020.103441.

[8] Camgozlu, Y., & Kutlu, Y. (2023). Leaf Image Classification Based on Pre-trained Convolutional Neural Network Models. *Natural and Engineering Sciences*, *8*(3), 214-232.

[9] Cha, J., Singh, S.K., Kim, T.W., & Park, J.H. (2021). Blockchain-empowered cloud architecture based on secret sharing for smart city. *Journal of Information Security and Applications, 57,* 102686. https://doi.org/10.1016/j.jisa.2020.102686

[10] Chen, J., Ramanathan, L., & Alazab, M. (2021). Holistic big data integrated artificial intelligent modeling to improve privacy and security in data management of smart cities. *Microprocessors and Microsystems*, *81*, 103722. https://doi.org/10.1016/j.micpro.2020.103722.

[11] Esposito, C., Ficco, M., & Gupta, B.B. (2021). Blockchain-based authentication and authorization for smart city applications. *Information Processing & Management*, *58*(2), 102468. https://doi.org/10.1016/j.ipm.2020.102468.

[12] Gheisari, M., Najafabadi, H.E., Alzubi, J.A., Gao, J., Wang, G., Abbasi, A.A., & Castiglione, A. (2021). OBPP: An ontology-based framework for privacy-preserving in IoT-based smart city. *Future Generation Computer Systems*, *123*, 1-13.

[13] Herath, H.M.K.K.M.B., & Mittal, M. (2022). Adoption of artificial intelligence in smart cities: A comprehensive review. *International Journal of Information Management Data Insights, 2*(1), 100076. https://doi.org/10.1016/j.jjimei.2022.100076

[14] Jayasree, V., Nithya, M., & Prabaharan, S. (2012). Cloud Data Retrieval for Multi related keyword based on Clustering Technology. *International Journal of Communication and Computer Technologies (IJCCTS)*, *1*(1), 60-66.

[15] Kaginalkar, A., Kumar, S., Gargava, P., & Niyogi, D. (2021). Review of urban computing in air quality management as smart city service: An integrated IoT, AI, and cloud technology perspective. *Urban Climate*, *39*, 100972. https://doi.org/10.1016/j.uclim.2021.100972.

[16] Kaur, M., & Mahajan, M. (2013). Using encryption algorithms to enhance the data security in cloud computing. *International Journal of Communication and Computer Technologies (IJCCTS)*, *1*(2), 130-133.

[17] La Marra, A., Martinelli, F., Mercaldo, F., Saracino, A., & Sheikhalishahi, M. (2020). D-BRIDEMAID: A Distributed Framework for Collaborative and Dynamic Analysis of Android Malware. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JOWUA)*, *11*(3), 1-28.

[18] Lam, K.Y., Mitra, S., Gondesen, F., & Yi, X. (2021). ANT-centric IoT security reference architecture—Security-by-design for satellite-enabled smart cities. *IEEE Internet of Things Journal, 9*(8), 5895-5908.

[19] Malini, P., Gowthaman, N., Gautami, A., & Thillaiarasu, N. (2021). Internet of Everything (IoE) in smart city paradigm using advanced sensors for handheld devices and equipment. *In IoT and IoE Driven Smart Cities. Cham: Springer International Publishing*, 121-141.

[20] Peneti, S., Sunil Kumar, M., Kallam, S., Patan, R., Bhaskar, V., & Ramachandran, M. (2021). BDN-GWMNN: internet of things (IoT) enabled secure smart city applications. *Wireless Personal Communications*, *119*(3), 2469-2485.

[21] Prajapati, P., & Shah, P. (2022). A review on secure data deduplication: Cloud storage security issue. *Journal of King Saud University-Computer and Information Sciences, 34*(7), 3996-4007.

[22] Qureshi, K.N., Ahmad, A., Piccialli, F., Casolla, G., & Jeon, G. (2021). Nature-inspired algorithm-based secure data dissemination framework for smart city networks. *Neural Computing and Applications, 33*, 10637-10656.

[23] Rahman, M.A., Hossain, M.S., Showail, A.J., Alrajeh, N.A., & Alhamid, M.F. (2021). A secure, private, and explainable IoHT framework to support sustainable health monitoring in a smart city. *Sustainable Cities and Society, 72,* 103083. https://doi.org/10.1016/j.scs.2021.103083

[24] Ram, A., & Chakraborty, S. K. (2024). Analysis of Software-Defined Networking (SDN) Performance in Wired and Wireless Networks Across Various Topologies, Including Single, Linear, and Tree Structures. *Indian Journal of Information Sources and Services (IJISS), 14*(1), 39–50.

[25] Savastano, M., Suciu, M. C., Gorelova, I., & Stativă, G.A. (2023). How smart is mobility in smart cities? An analysis of citizens' value perceptions through ICT applications. *Cities*, *132*, 104071. https://doi.org/10.1016/j.cities.2022.104071.

[26] Sreenivasu, M., Kumar, U.V., & Dhulipudi, R. (2022). Design and Development of Intrusion Detection System for Wireless Sensor Network. *Journal of VLSI Circuits and Systems*, *4*(2), 1-4.

[27] Ugaz, W.A.C., Santolaya, M.D.R.H., Purizaga, H.M.R., Bravo, W.A.S., Dávila, J., Ccolque, J.Y.V., & Fuster-Guillén, D. (2023). Hybrid Internet Architecture and Protocol (HIAP): A Self-Evolving and Transformative Framework for Enabling Seamless Real-Time Applications and Secure Peer-to-Peer File Sharing in the Internet of Everything (IoE). *Journal of Internet Services and Information Security (JISIS), 13*(3), 58-77.

[28] Ullah, F., Qayyum, S., Thaheem, M.J., Al-Turjman, F., & Sepasgozar, S.M. (2021). Risk management in sustainable smart cities governance: A TOE framework. *Technological Forecasting and Social Change*, *167*, 120743. https://doi.org/10.1016/j.techfore.2021.120743.

Author Biography

Dr.K. Malathi is working in the Artificial Intelligence and Machine Learning department at Saveetha Engineering College in Thandalam, Chennai, as an Assistant Professor. She has worked in a variety of teaching and research roles for more than 13 years. Her career began at J.J. College of Engineering and Technology. She had been a teaching faculty member at KCG College of Technology in Chennai as well as in Malaysia. Her doctorate in Computer Science and Engineering was awarded by VISTAS in Chennai. Her areas of interest are Cloud Computing, Artificial Intelligence, and Machine Learning, having worked briefly in a variety of technology-based research jobs. She has over ten published papers and chapters in reputable international publications that are included in the Scopus and SCIE/Web of Science indexes. She has participated in several faculty development programs, conferences, and seminars.