International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(6s) 2026 pp. 1099-1112
https://doi.org/10.70917/ijcisim-2026-3020
Article

A Trust-Based Secured Cloud Data-Processing Model for E-Waste Management

Vijayakumar S Malagitti [1]*, Mahantesh C Elemmi [2], Jagadeesha S [3], Girish Saunshi [4]

[1]Department of Computer Science and Engineering, Tontadarya College of Engineering, Visveswaraya Technological University, Belagavi-590018
[2]Department of Computer Science and Engineering, Navkis College of Engineering, Hassan
[3]Department of Electronics and Communication Engineering, AMC Engineering College, Bangalore
[4]Department of Computer Science and Engineering, KLEIT Hubballi
*** Corresponding author's Email**: vijayakumarmalagitti@gmail.com

Abstract: Electronic Waste (e-waste) generation has increased significantly due to rapid technological advancements, leading to security concerns related to data privacy and unauthorized access. Managing e-waste efficiently requires secure data transmission and processing mechanisms to prevent cyber threats. Existing security solutions for E-Waste Management (EWM) rely on blockchain approaches, which are computationally complex and not optimized for cloud environments. Additionally, data processing within a connected network remains vulnerable to attacks, exposing sensitive information. Hence, this work aims to develop a lightweight and secure model for e-waste data transmission and cloud data processing, called as Trust-based Secured Cloud Data-Processing for EWM (TSCD-EWM) model, which ensures protection against cyber threats while maintaining computational efficiency. This model integrates trust-based security for data transmission and a secured cloud data processing mechanism. The model enhances encryption effectiveness while reducing computational overhead. The TSCD-EWM model achieves better results in terms of information entropy (7.9999), Number of Pixel Change Rate (NPCR) (99.77%), and Uniform-Average Changing Intensity (UACI) (33.1073%), demonstrating high randomness, strong diffusion, and effective confusion properties. Unlike existing methods, TSCD-EWM balances security and computational efficiency, making it an optimal choice for secure e-waste data management. The TSCD-EWM provides a robust and lightweight security solution for e-waste management, ensuring secure transmission and cloud processing.
Keywords: -E-waste, Security, Trust-based Model, Cloud Data Processing, Encryption.

1. Introduction

Electronic waste, commonly known as e-waste, refers to discarded electronic and electrical devices such as smartphones, computers, televisions, and other consumer electronics. As technology advances and electronic devices become obsolete at an increasing rate, e-waste has emerged as a significant environmental and health challenge [1]. Unlike traditional waste, e-waste contains hazardous materials such as lead, mercury, and cadmium, which can cause severe environmental pollution if not disposed of properly. However, e-waste also contains valuable materials such as gold, silver, and copper, making its management crucial for both economic and environmental sustainability [2]. Over the past decade, the global production of e-waste has surged due to the rapid consumption and disposal of electronic devices. According to the Global E-Waste Monitor 2020, the world generated approximately 53.6 million metric tons (Mt) of e-waste in 2019, marking a 21% increase in just five years [3]. With rising consumer demand, reduced product lifespans, and limited recycling facilities, e-waste is projected to exceed 74 Mt by 2030. Countries with high technological adoption, such as the United States, China, and India, are among the largest contributors to e-waste [4]. This alarming increase in e-waste necessitates robust management strategies to minimize environmental impact and recover valuable resources. Hence, E-Waste Management (EWM) approaches have been established.

EWM involves the collection, transportation, processing, recycling, and proper disposal of electronic waste. Effective EWM systems ensure that hazardous materials are safely handled while valuable components are recovered for reuse. Various strategies have been implemented globally, including extended producer responsibility (EPR), consumer awareness programs, and the establishment of recycling facilities. Despite these efforts, e-waste recycling rates remain low, with only 17.4% of e-waste being properly recycled worldwide [5]. Recognizing the growing threat

of e-waste, several countries have introduced policies and technological solutions to manage e-waste effectively. The European Union has established the Waste Electrical and Electronic Equipment (WEEE) Directive, mandating electronic manufacturers to take responsibility for product disposal [6]. Similarly, China has implemented the "Circular Economy" strategy, which includes e-waste recycling initiatives [7]. In India, the government has enforced EWM rules, requiring companies to follow collection and recycling norms [8]. Furthermore, countries like Japan and South Korea have developed automated e-waste recycling facilities that enhance resource recovery and minimize environmental damage [9]. A normal EWM system involves multiple stakeholders, including manufacturers, retailers, consumers, smart bin operators, collectors, recyclers, and destruction units. Manufacturers design and produce electronic goods, while retailers distribute these products to consumers. Consumers use electronic devices and discard them once they reach the end of their life cycle. Smart bins facilitate the collection of e-waste, which is then transported by collectors to recycling or destruction units for further processing. Each stakeholder plays a crucial role in ensuring efficient EWM.

To streamline EWM, stakeholders share real-time data, including text and images, through connected networks. For instance, smart bins update collectors regarding the amount of e-waste collected, while recyclers share data on recovered materials with manufacturers. This interconnected system enables efficient tracking and processing of e-waste. However, as stakeholders rely on digital platforms for data exchange, security concerns arise due to the increasing risk of cyberattacks. Due to this issue, e-waste data is highly vulnerable to cyberattacks, as attackers can exploit unsecured networks to steal sensitive information [10]. An attacker can manipulate data related to e-waste collection, recycling, or destruction, leading to financial losses and disruptions in the EWM process. Additionally, attackers may misuse confidential consumer data associated with discarded devices, posing privacy risks. Given these threats, robust security measures are necessary to protect data transmission and processing in EWM. Several security solutions have been introduced to safeguard e-waste data transmission and processing. Blockchain and role-based access control (RBAC) have been widely adopted to enhance security and transparency [11], [12]. Blockchain ensures tamper-proof data storage and verification, while RBAC restricts access to authorized personnel only. However, these approaches increase computational complexity and require significant processing power, making them inefficient for lightweight applications. To address these challenges, trust-based security models have been proposed [13], [14]. These models assess the trustworthiness of stakeholders before allowing data exchange, reducing the risk of malicious activities. However, trust-based methods are computationally intensive, as they require multiple trust evaluations and authentication processes. Moreover, most e-waste data is processed in connected networks or cloud-based platforms. While cloud computing offers scalability and accessibility, it also exposes data to potential attacks during transmission and processing [15]. Attackers can infiltrate cloud systems, intercept sensitive data, or manipulate processing algorithms, leading to security breaches. Despite the growing adoption of cloud computing in EWM, limited security solutions have been developed to protect data during processing.

To overcome the aforementioned security challenges, this work presents a novel model called Trust-based Secured Cloud Data-Processing for EWM (TSCD-EWM). The proposed model integrates a trust-based security mechanism for secure data transmission between stakeholders and a secured cloud data processing approach to prevent unauthorized access during data processing. By leveraging trust-based authentication and encryption techniques, TSCD-EWM ensures the integrity and confidentiality of e-waste data while minimizing computational overhead. This approach enhances the overall security and efficiency of EWM, contributing to a more sustainable and reliable system. The contributions of the work are as follows

- A trust-based security approach is introduced to ensure secure data transmission between stakeholders and cloud in the EWM architecture. Unlike blockchain and role-based access control methods that increase computational complexity, the proposed approach is more efficient and lightweight.
- The work integrates both direct and indirect trust mechanisms to dynamically assess stakeholder interactions and establish secure connections. Trust values are updated based on stakeholder interaction history, ensuring a dynamic and adaptive security framework.
- A robust secured cloud data processing mechanism is presented to protect e-waste data from attacks during processing. A pseudo-random sequencing function and confusion-diffusion mechanism are employed for encrypting image-based e-waste data. The proposed security model ensures that even if attackers attempt to exploit e-waste data, encrypted storage and transmission prevent unauthorized access.
- The e-waste architecture is designed to handle large volumes of e-waste data efficiently while maintaining security. The architecture enables seamless and secure communication among manufacturers, retailers, customers, collectors, recyclers, and destruction units. Unlike traditional methods that focus on transmission

security, this work addresses vulnerabilities in data processing, making it a unique contribution in EWM security.

The manuscript is organized in the following manner. In Section II, the different trust-based security and image-based security approaches for providing security are discussed in detail. The Section III presents TSCD-EWM approach, where architecture, trust-based security and secured cloud data processing is discussed. In Section IV, the results of TSCD-EWM are discussed and compared with the existing approaches presented in literature survey. Finally, Section V presents the conclusion and future work.

2. Literature Survey

This section discusses the different trust-based and image-based security approaches which have been presented in recent years for providing security. S. T. Alshammari et al. [16], for providing security within cloud for data transmitted by owners, this work presented a Task-Role-Based Access Control Approach (T-RBAC). The main aim of this approach was to provide trust-based security for cryptographic approaches which provide data privacy and gives access to only authorized users. The trust model in T-RBAC included role-behavior analyzer, task behavior analyzer and trust decision engine, on basis of which the roles and security was provided. Also, this work presented a recommendation trust approach for protecting data from attacks on basis of multiple trust functions. Evaluations were conducted on basis of feedback, attack detection and attacker behavior and other security metrics, where T-RBAC achieved better outcomes. M. Hegde et al. [17], for providing security during key exchange authentication in cloud-fog architecture, for securing session secrecy and user anonymity, an authentication method on basis of key agreement and management was presented. The approach authenticated all stakeholders present in the cloud-fog architecture including the cloud to provide security using secure keys. Using the following approach, attacks were prevented. Evaluations were conducted in terms of communication cost and computation cost, comparing with other similar approaches. Findings showed that the key generation security provided better outcomes in comparison with other approaches for the cloud-fog layer for protecting and solving problem of data privacy. A. Brighente et al. [18], investigated privacy and security issues in smart waste management system, where reviewed different attacks in cloud layer and at the stakeholder layer. They also discuss how the different attacks affect the data processing in cloud.

W. Alexan et al. [19], presented an approach for encrypting data for securing data from attackers, for which used 4-Dimensional Hyperchaotic Chen-Map of fractional-order in combination with proposed Deoxyribo-Nucleic Acid (DNA) coding and Sine-Chaotic-Map (4D-CMDNASCM). In encryption process, Sine-Chaotic-Map and 4-Dimensional Hyperchaotic Chen-Map with hybrid DNA coding was used. For decryption the process was reshuffled, using which the image was decrypted. Evaluations were conducted on C4L image dataset, considering multiple metrics, which included Peak-Signal to Noise-Ratio (PSNR), Mean-Squared Error (MSE) Information Entropy (IE), Adjacent-Pixel Correlation-Coefficient (APCC), Mean Averaged Error (MAE), time, Uniform-Average Changing Intensity (UACI) and Number of Pixel Change Rate (NPCR). Findings showed that 4D-CMDNASCM achieved 7.997 IP, 99.62% NPCR and 33% UACI. Also, the key space considered in their work was 2^{2744}. D. Huang et al. [20], presented an encryption approach on basis of chaotic approach. This approach generated encryption key using Secure Hash Algorithm 3 (SHA3-256) function, where their main focus was to achieve “one map, one secret”. The chaotic sequences were generated using memristive hyper-chaotic approach and was used for encrypting image. In their encryption approach, column and row disruption was performed, then Arnold disruption was used and finally DNA-level encryption was performed for enhancing diffusion and heterogenous encryption. Evaluations were conducted on MATLAB, where 512×512 size images were considered for evaluation. The approach achieved 33.46% UACI and 99.6064% NPCR. L. Dai et al. [21], presented a double-layer image encryption framework to provide security for images. In first-layer, an enhanced Generative Adversarial Network (GAN) was used. In GAN a novel loss-function, which consisted of identity loss-function, encryption-decryption loss-function, an image space-smoother loss-function, and a generator-veracity improving loss-function was presented. Further, in second-layer, presented a 6-D (6-Dimension) hyperchaotic approach which consisted of 4 Lyapunov positive cells which had image scrambling process. For further scrambling and for diffusion, used classical shuffling approach with combination of Fibonacci Q-matrix approach. Using the following approach, they increased the key space to $2^{388874304}$ using which image encryption providing security was enhanced to different kind of attack. Findings on C4L image dataset showed better outcomes for histogram analysis, APCC, IE, UACI and NPCR for 256×256 images.

Z. Chong et al. [22], for providing security to images, this work presented 5F-Memristive Hyperchaotic (5D-MHC) approach using flux-controlled approach. This work used chaotic mapping, hashing approach, arithmetic and DNA coding, logistic approach and 2-D Hyperchaotic-Map (2D-SFHM) for encrypting the image. Evaluations were conducted on C4L image dataset, where showed 99.62% NPCR and 33.4670% UACI and 7.9994 IE. For this work

they considered key space of 2^{512}. Y. -C. Lan et al. [23], presented novel encryption approach called Generalized-Rectangular-Transform and Penta-Hyperchaotic Map (GRTPHM). The encryption included pixel diffusion and permutation, where GRT was used for permutation for rearranging positions of pixels using a transformed matrix, which efficiently disrupted strong correlation among neighbor pixels and improved histogram analysis. Further, in pixel diffusion included Bit-Level Random-Permutation (BLPR) which used PHM (5-D discrete memristor hyperchaotic map), which was integrated with SHA-512. The BLRP shuffled bits which provided better confusion-diffusion, improving security. Further, for decryption the GRTPHM approach presented a reverse rectangular-transform for image reconstruction. Evaluations were conducted on C4L image dataset where used different metrics for evaluation and findings showed better outcomes in comparison with existing methods. They used key space higher than 2^{100} for providing better security. From the above literature survey, it is evident that no prior work has specifically focused on providing security for EWM. The existing trust-based security approaches, such as T-RBAC by S. T. Alshammari et al. [16] and key agreement authentication by M. Hegde et al. [17], are complex and involve high computational overhead, making them unsuitable for lightweight e-waste applications. Moreover, while several studies, including those by W. Alexan et al. [19], D. Huang et al. [20], and Z. Chong et al. [22], have explored image-based security using hyperchaotic and DNA encryption techniques, these approaches have not been implemented in cloud environments. The encryption frameworks by L. Dai et al. [21] and Y.-C. Lan et al. [23] focus on securing image data but do not address security challenges during data transmission and cloud-based processing, which are crucial for e-waste data protection. Thus, there is a clear gap in research for lightweight security solutions in EWM cloud processing. Hence, this work presents the TSCD-EWM approach which is discussed in detail in the next section.

3. Methodology

Due to the rapid increase in e-waste, an efficient, secured and cloud-integrated EWM system is required as discussed in literature survey. Hence, this work presents a novel approach for providing a secured cloud-based security and data processing for different stakeholders present in the EWM, called as Trust-based Secured Cloud Data-Processing for EWM (TSCD-EWM). This section provides a detailed methodology of TSCD-EWM for providing secured cloud-based security. This methodology first discusses the architecture of the TSCD-EWM. Further, this section discusses the trust-based security used in this work for data transmission from stakeholders towards cloud. Finally, this section discusses the secured cloud data processing approach. In the next section, the architecture of the EWM is discussed.

Architecture

The architecture of TSCD-EWM is presented in Figure 1. The architecture consists of multiple stakeholders (manufacturers, retailers, customers, smart bins, collectors, recyclers, and destruction units). In this EWM architecture, the manufactures produce electronic goods, retailers sell electronic products, customer use electronic devices and discard them in smart bins when they reach end of life, collectors gather e-waste from smart-bins and transfer it to recyclers or destruction units. Every stakeholder is connected to cloud-based data processing system, which ensures real-time updates, data transmission and secured processing. For providing security for data transmission of images data collected from stakeholders towards cloud for data processing, first this work presents a trust-based security approach which establishes a connection for data transmission. The trust-based security model includes two trust-based approaches, direct and indirect trust, which is discussed in detail in Section 3.2. Further, a novel secured cloud-based data processing approach is presented, which is discussed in detail in Section 3.3.

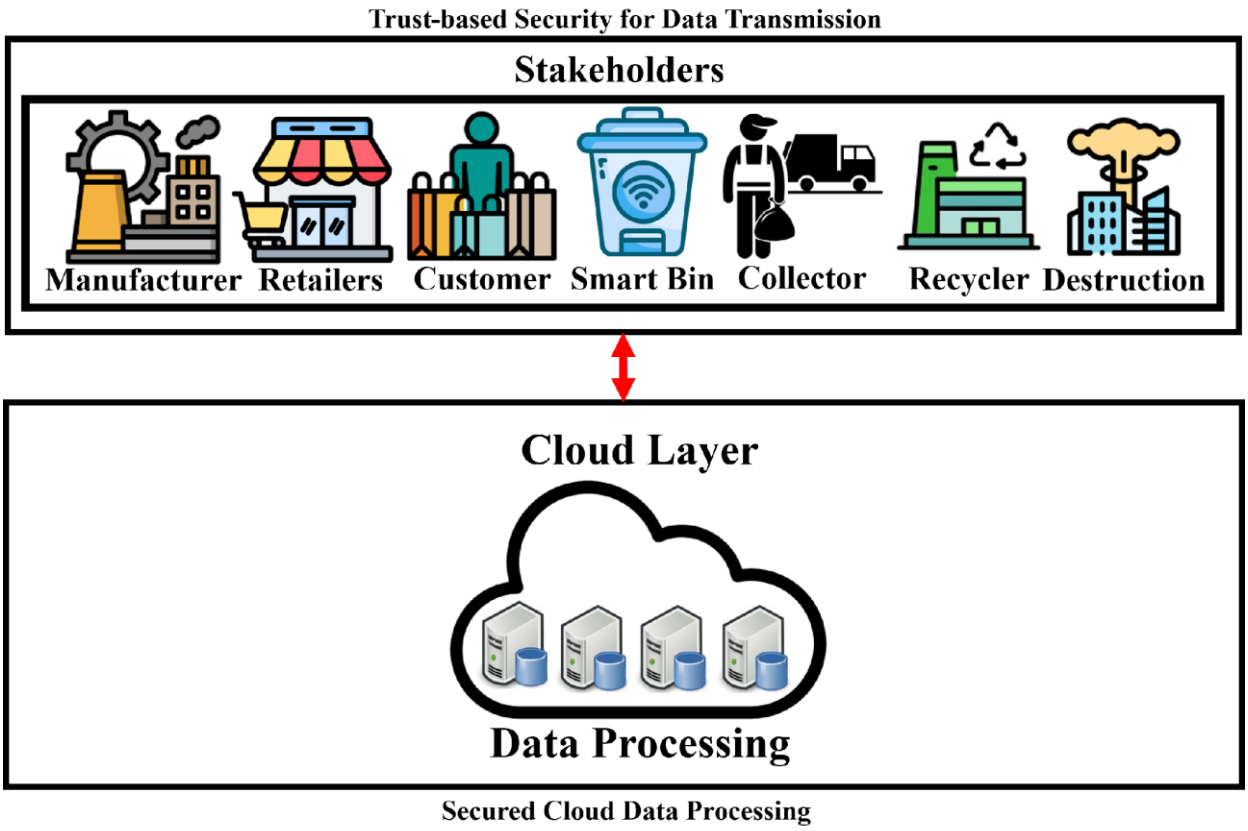


Figure 1. Secured EWM architecture.

Trust-Based Security for Data Transmission

This section discusses the trust-based security for data transmission from stakeholders to cloud. For ensuring trust between stakeholders and the cloud, this work utilizes direct and indirect trust-based security. For establishing direct trust, consider different stakeholders as x and cloud as y. Let the interaction between the x and y for a specific time be denoted as o and overall time for their interaction be u. Hence from this the direct trust between x and y denoted as $D_o^u(x,y)$ is defined as presented in Eq. (1).

$$D_o^u(x,y) = Sec_o^u(x,y) \tag{1}$$

In Eq. (1), $Sec_o^u(x,y)$ is security trust function which is evaluated and defined using Eq. (2) and Eq. (3) respectively.

$$Sec_o^u(x,y) = \gamma * Sec_{rec}(x,y) + (1-\gamma) * Sec_{o-1}^u(x,y) \tag{2}$$

$$Sec_{rec} = \{0, \quad 1, \quad \begin{matrix} interaction\ between\ x\ and\ y\ is\ untrustable \\ interaction\ between\ x\ and\ y\ is\ trustable \end{matrix} \tag{3}$$

In Eq. (2), γ denotes trust-variance parameter which measures trust changes for different time o and compares using a defined threshold H which determines if interaction is trusted or not. In this work, the threshold H and γ are dynamic. Further, $Sec_{rec}(x,y)$ defines whether the interaction among stakeholders x and y is either trustable or not trustable and $Sec_{o-1}^u(x,y)$ denotes previous or historic value of security trust function, which is initially set as 0. Further, this work utilizes indirect trust for establishing connection between different stakeholders denoted as p. The indirect trust denoted as $I_o^u(x,y)$ is established as presented in Eq. (4).

$$I_o^u(x,y) = \{\frac{\sum_{p \in Z-\{x\}} A_o^u(x,p) * D_o^u(x,y)}{\sum_{p \in Z-\{x\}} A_o^u(x,p)}, if\ |Z-\{x\}| > 0\ 0, if\ |Z-\{x\}| = 0 \tag{4}$$

In Eq. (4), Z denotes set of all stakeholders present in EWM architecture, x denotes a particular stakeholder from the following set, $D_o^u(x,y)$ denotes direct trust established from the particular stakeholder x to cloud y and $A_o^u(x,p)$ denotes authentication trust function between the particular stakeholder x and other stakeholder p. The $A_o^u(x,p)$ is evaluated using Eq. (5).

$$A_o^u(x,p) = \{1 - \frac{log\ log\ \left(Sec_o^u(x,p)\right)}{log\ log\ \theta}, if\ R_o^u(x,p) > \theta\ 0, if\ R_o^u(x,p) < \theta \tag{5}$$

In Eq. (5), $Sec_o^u(x,p)$ is security trust function between stakeholder x and other stake holders p, which is evaluated similarly using Eq. (2) and $log\ log\ \theta$ is a threshold which is set on basis of trust-relationship function among the stakeholder x and stakeholder p denoted as $R_o^u(x,p)$.

$$T_o^u(x,y) = \{T_{o-1}^u(x,y) + \frac{1 - T_{o-1}^u(x,y)}{X}, if\ V_o^u(x,y) < H\ T_{o-1}^u(x,y) - \frac{1 - T_{o-1}^u(x,y)}{Y}, \\ if\ V_o^u(x,y) > H \tag{6}$$

In Eq. (6), $T_{o-1}^u(x,y)$ denotes previous or historic authentication trust function value, which is initially set as 0, X and Y denotes reward and penalty variable respectively, which are dynamic and depends on the variance trust function $V_o^u(x,y)$ which is evaluated at every o for measuring how trust of stakeholder x changes with respect to cloud y because of interactions and H denotes threshold which determines if interaction is trusted or not, which is dynamic in this work. The $V_o^u(x,y)$ is evaluated using Eq. (7).

$$V_o^u(x,y) = \sqrt{\frac{\sum_{p \in H} \left(Sec_o^u(x,p) - Sec_o^u(y,p)\right)^2}{|H(x,y)|}} \tag{7}$$

In Eq. (7), $Sec_o^u(x,p)$ is security trust function between stakeholder x and stakeholder p and $Sec_o^u(y,p)$ is security trust function between cloud and stakeholder p. Further, the value of X and Y depends on the following factors

1. If a stakeholder x has historically high trust, then X will be higher and Y will be low.
2. If as stakeholder x has fluctuating or has historically low trust, then Y will be higher and X will be low.
3. If $V_o^u(x,y)$ is small, i.e., if stakeholder interactions with cloud is stable, X will be set high.
4. If $V_o^u(x,y)$ is high, i.e., if stakeholder interactions with cloud is inconsistent, Y will be set low.

Hence, from the following factors, the X and Y are evaluated as presented in Eq. (8) and Eq. (9) respectively.

$$X = a + \beta \cdot V_o^u(x,y) \tag{8}$$

$$Y = b + \delta \cdot V_o^u(x,y) \tag{9}$$

In Eq. (8) and Eq. (9), a and b are base values of X and Y which is set as 0, β and δ are scaling parameters which determine how X and Y quickly change with variance trust function. The security between the stakeholders x and cloud y was given using the trust-based security function as presented in Eq. (10).

$$S_o^u = \frac{\left(W_1 * D_o^u(x,y)\right) + \left(W_2 * I_o^u(x,y)\right)}{2} \tag{10}$$

Using the trust-based security the data transmissions in EWM architecture were secured. The complete flow of the data transmission process is presented in Figure 2.

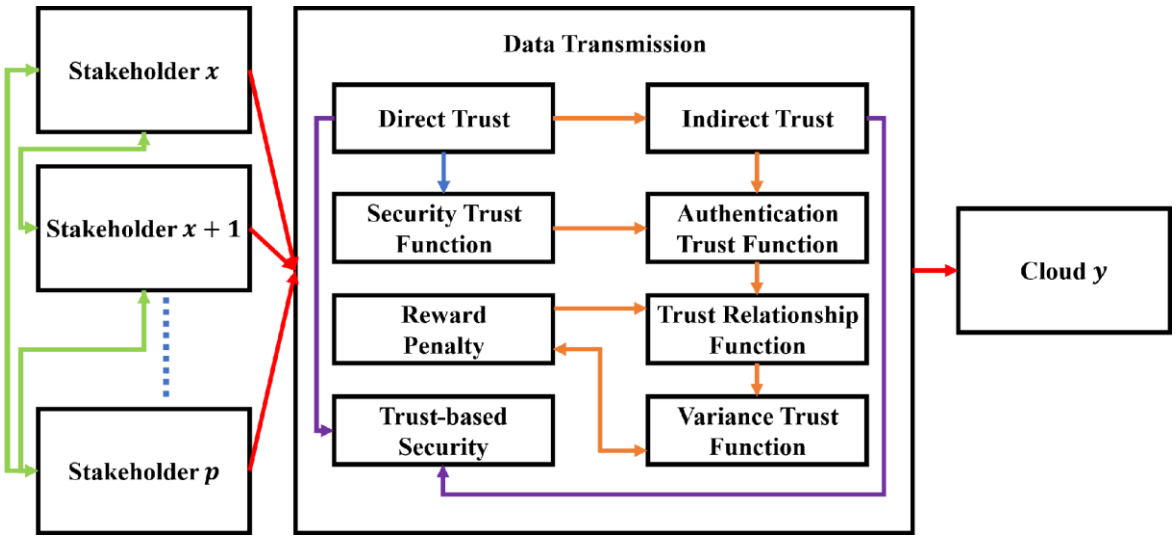


Figure 2. Trust-based security data transmission in EWM architecture.

Further, the next section discusses the secured cloud data processing presented for the EWM architecture.

Secured Cloud Data Processing

This section presents a secured way of processing transmitted data from stakeholders. The complete process of how data is secured before processing in cloud is presented in Figure 3.

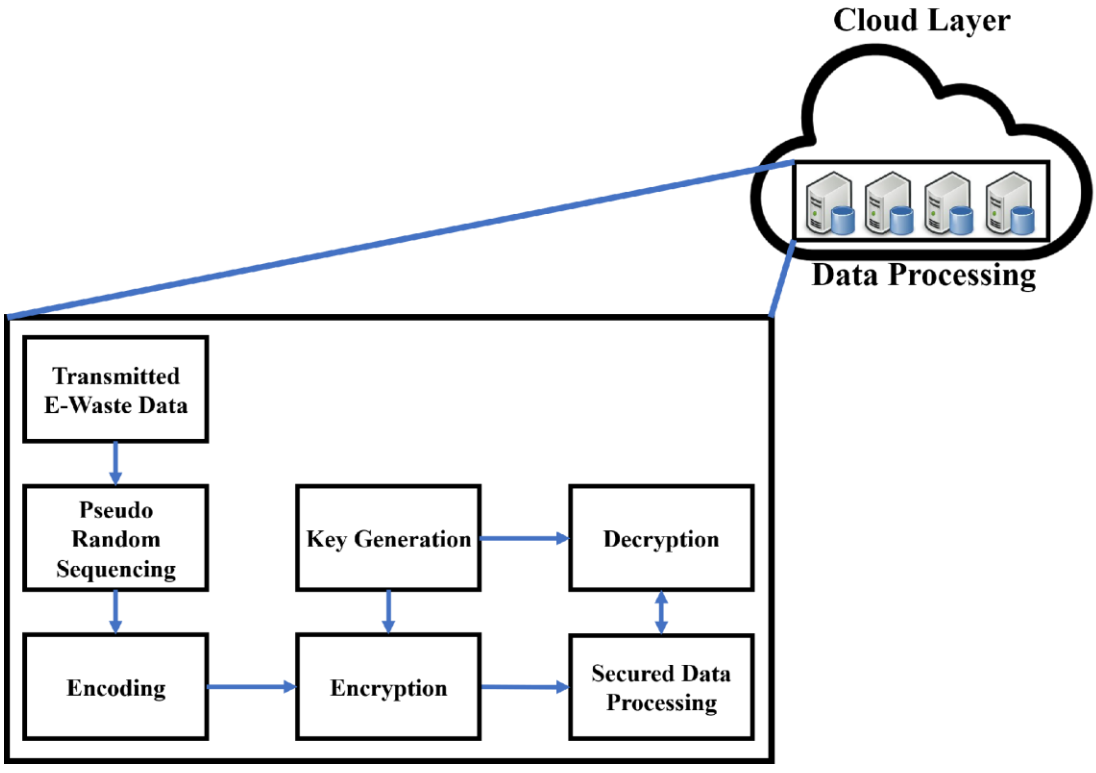


Figure 3. Secured cloud data processing of e-waste data management.

In this secured cloud data processing, first to provide security, the colored secured transmitted e-waste images data were converted to grayscale images and the original coding of color image is stored in key. The main aim of using grayscale encryption is to prevent statistical attacks. Further, the grayscale image was considered which went

through process of pseudo-random sequencing function in cloud y to provide security before processing using Eq. (11).

$$P = cos\ cos\ \left(\pi\left(G\left(b, i_j\right) + H\left(c, i_j\right) + P\right)\right) \tag{11}$$

In Eq. (11), $cos\ cos\ (\cdot)$ function is used for creating non-linearity which ensures output of pseudo-random sequencing function remains in bounded range of $(-1$ to $1)$, π is used for normalization and periodicity of pseudo-random sequences, $G\left(b, i_j\right)$ generates random sequences on basis of parameter b and i_j denotes current state of a random deterministic sequence which exhibits random, unpredictive sequences on basis of b for iteration j. Similar to $G\left(b, i_j\right)$, $H\left(c, y_j\right)$ also generates random sequences on basis of parameter c for adding additional layer of randomness and security. Moreover, the parameter b and c determines and controls behavior of pseudo-random sequences G and H, respectively, influencing randomness and ensuring unpredictability. Finally, the parameter P introduces phase-shift in pseudo-random sequences, thereby increasing security and complexity. Further, the data then goes through encoding process, where bit-scrambling and confusion-diffusion is done using [24] for encrypting data. In this security-based approach, a key is utilized for encrypting and decrypting e-waste data. The key helps in controlling pseudo random sequence generation, bit-scrambling, confusion-diffusion and substitution operations. In this work, the key is generated as 256-bit random number, i.e., 2^{256}, which ensures large key-space for providing security. The key consists of initial states of pseudo-random sequences, which controls $cos\ cos\ (\cdot)$ and P parameters, which thereby controls pseudo-random sequencing confusion-diffusion. Further, key generation for encrypting e-waste image is as follows. First, the key K is generated in a square-matrix as presented in Eq. (12).

$$K = M^2 * M^2 \tag{12}$$

In Eq. (12), M denotes block-size. Consider e-waste image data having size as $N * O$, where N and O are image height and image width. For encrypting the following e-waste data, the block-size M is evaluated using Eq. (13).

$$M = \{\lfloor\sqrt{N}\rfloor, \lfloor\sqrt{O}\rfloor\} \tag{13}$$

In Eq. (13), $\lfloor\sqrt{\mu}\rfloor$ denotes floor-function parameter, which ensures that only integer values are given during key generation. The Eq. (13) divides image to M^2 block, allowing independent scrambling within every block. After dividing, every block consists subsets of pixels which are scrambled separately. For the scrambling, the pseudo-random sequences are generated, where pixel position in every row is permuted randomly. After row-wise permutation, pixel in every block is randomly assigned new positions using pseudo-random sequences. For better understanding, consider an e-waste image as Q having size $N * O$ which is first rotated clockwise by right angle as $Q' = Rotate(Q, 90^{\circ})$. Further, image is divided to blocks using Eq. (13), then every block undergoes random pixel permutation using pseudo-random sequence P using Eq. (11). The complete process is evaluated as presented in Eq. (14).

$$P(i, j) = P \cdot Q' \tag{14}$$

In Eq. (14), $P(i, j)$ denotes permuted pixel values. This process is only satisfied when $M = \sqrt{N} = \sqrt{O}$. This encryption process ensures high non-linear pixel arrangement, which reduces correlation between neighboring pixels. Further, for recovering original e-waste image, the decryption process follows inverse scrambling process using the generated key. As the pseudo-random sequences in the scrambling approach are deterministic, hence, using this the image is restored. Also, the grayscale image is converted to color image using the generated key, which initially stores the coding of original image. The encrypted data is then passed on to cloud, where data processing is done. Using the following approach, the security is provided for data transmission and for data processing. Further, in next section, the results of TSCD-EWM approach are discussed in detail.

4. Results and Discussion

In this section, the results achieved by the TSCD-EWM are discussed and compared with different existing approaches [21], [22], and [23]. For the evaluation, the following metrics were used: histogram analysis, APCC, IE, UACI and NPCR. The TSCD-EWM was developed in MATLAB 2018B. For evaluation of this study, the miscellaneous images from C4L image dataset [25] and e-waste image database [26] were considered. From the C4L image dataset and e-waste image database, standard $256 * 256$ images were considered for evaluation. From the C4L image dataset, Pepper and Cameraman were considered and from image database, Keyboard, Mobile and Mouse images were considered. This section is divided into four sections, where first the histogram performance is evaluated,

followed by information entropy, correlation coefficient and differential attack performance where UACI and NPCR outcomes are discussed.

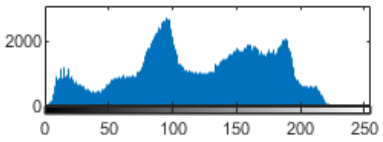
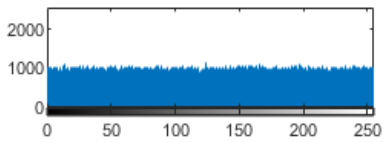
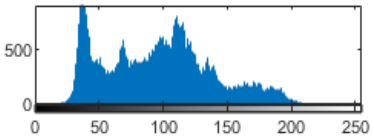
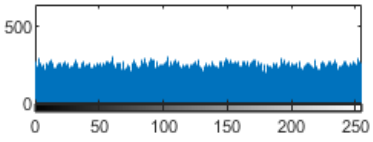
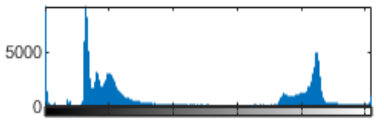
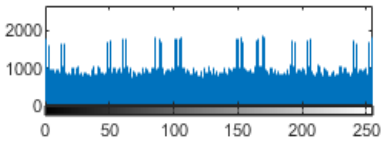
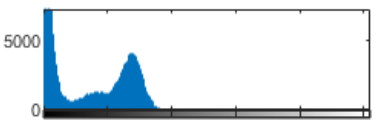
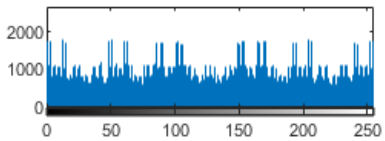
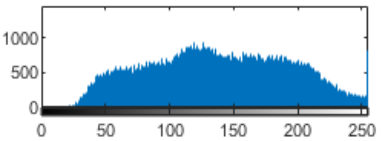
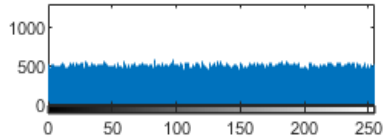
Histogram Analysis

For histogram analysis, the grayscale images of size 256×256 were considered. The main aim of using grayscale encryption is to prevent statistical attacks. The outcome of histogram analysis is presented in Table 1. The results presented in Table 1 show that the TSCD-EWM approach provides better encryption and an attack will not be able to decode the e-waste input or grayscale image without the key. As the TSCD-EWM uses grayscale image for encryption, the encryption outcome is flat. Further, for measuring pixel distribution uniformity of input and encrypted image, histogram variance is evaluated using Eq. (15).

$$V(Z) = \frac{1}{n^2} \sum_{i=0}^{1} \sum_{j=0}^{n-1} \frac{\left(z_i - z_j\right)^2}{2} \tag{15}$$

In Eq. (15), Z denotes histogram variable, where $Z = \{z_0, z_1, z_2, \ldots, z_{256}\}$ of grayscale image, z_i and z_j denotes overall pixel size having grey variable i and j and $n = 256$.

Table 1. Histogram Analysis.

Image Name	Input Image	Input Image Histogram	Encrypted Image Histogram
Pepper			
Cameraman			
Keyboard			
Mobile			
Mouse			

Information Entropy

IE is used for evaluating insecurity degree. For IE evaluation, the Eq. (16) is used.

$$H(m) = -\sum_{k=0}^{2^N-1} p(m_i)p(m_i) \tag{16}$$

In Eq. (16), $p(m_i)$ denotes probability that e-waste data m_i fails to encrypt an is visible. As this work considers grayscale images for encryption, $m_i = 256$ states and highest state and lowest state is 255 and 0 respectively. Using Eq. (16), the IE is evaluated. Also, when the entropy-size was kept at 8, the entropy was random, thereby providing better encryption. The results of IE are presented in Table 2.

Table 2. Information Entropy.

Model	Pepper	Cameraman	Keyboard	Mobile	Mouse
[21]	7.999	7.0097	-	-	-
[22]	-	7.9993	-	-	-
[23]	7.999	-	-	-	-
TSCD-EWM	**7.9999**	**7.9998**	**7.9556**	**7.9422**	**7.9895**

The results from Table 2 indicate that TSCD-EWM model achieves highest IE across all tested images, demonstrating its superior ability to enhance data security. Compared to prior works, TSCD-EWM achieves an entropy value of 7.9999 for Pepper and 7.9998 for Cameraman, which are higher than the values reported by [21], [22], and [23]. Additionally, TSCD-EWM provides entropy values for Keyboard (7.9556), Mobile (7.9422), and Mouse (7.9895), while previous models do not present results for these images. The near optimal entropy value (close to 8) suggests that TSCD-EWM generates more randomness in encrypted data, making it more resistant to attacks like entropy analysis.

Adjacent Pixel Correlation Coefficient

The APCC measures the correlation between neighboring pixels in an image; a lower APCC value indicates better encryption strength by reducing patterns and making the encrypted image more resistant to attacks. For evaluating APCC, the Eq. (17) is used.

$$r_x = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \tag{17}$$

In Eq. (17), $cov(x,y)$ denotes covariance between adjacent pixels x and y, which measure linear dependency, $D(x)$ and $D(y)$ denote pixel variance values in image along Horizontal (H), Vertical (V) and Diagonal (D) direction. In Eq. (17), the $cov(x,y)$, $D(x)$ and $D(y)$ are evaluated using Eq. (18), Eq. (19) and Eq. (20).

$$cov(x,y) = \frac{1}{N}\sum_{i}^{N} \big(y_i - E(x)\big)\big(y_i - E(y)\big) \tag{18}$$

$$D(x) = \frac{1}{N}\sum_{i}^{N} \big(x_i - E(x)\big)^2 \tag{19}$$

$$D(y) = \frac{1}{N}\sum_{i}^{N} \big(y_i - E(y)\big)^2 \tag{20}$$

In Eq. (18), the $E(x)$ and $E(y)$ are evaluated using Eq. (21) and Eq. (22).

$$E(x) = \frac{1}{N}\sum_{i}^{N} x_i \tag{21}$$

$$E(y) = \frac{1}{N}\sum_{i}^{N} \quad y_i \tag{22}$$

Using Eq. (17), the APCC is evaluated for the original and encrypted e-waste images. The result of APCC for the plain image and encrypted image is presented in Table 3 and Table 4 respectively. In Table 3, for plain images, APCC values are close to 1 across all models, indicating strong pixel correlation in the original images. This is expected, as natural images have adjacent pixels with similar intensity values. However, after encryption, the APCC values should ideally approach 0, signifying effective scrambling and reduced correlation.

Table 3. APCC for plain image.

Model	Image	H	D	V
[21]	Peppers	0.9488	0.914	0.9547
	Cameraman	0.9365	0.911	0.9624
[22]	Cameraman	0.9824	0.9724	0.9899
[23]	Peppers	0.92758	0.902429	0.96003
TSCD-EWM	**Peppers**	**0.959022**	**0.930026**	**0.79048**
	Cameraman	**0.959022**	**0.930026**	**0.966395**
	Keyboard	**0.9484**	**0.9136**	**0.9543**
	Mobile	**0.9361**	**0.9106**	**0.962**
	Mouse	**0.982**	**0.972**	**0.9895**

In Table 4, TSCD-EWM achieves APCC values very close to 0 for encrypted images across horizontal (H), diagonal (D), and vertical (V) directions, better than previous models. This indicates that TSCD-EWM provides superior pixel randomness, ensuring better security and resistance against statistical attacks. The model consistently outperforms [21], [22], and [23] in most cases, proving its robustness in reducing correlation and enhancing encryption strength. These results highlight that TSCD-EWM provides better diffusion and confusion properties, making it a more secure approach for encrypting e-waste data in cloud environments.

Table 4. APCC for encrypted image.

Model	Image	H	D	V
[21]	Peppers	0.0005	-0.0048	0.0023
	Cameraman	-0.0001	0.0132	0.0004
[22]	Cameraman	0.0039	0.0067	-0.0000328
[23]	Peppers	0.01	-0.0049	-0.0354
TSCD-EWM	**Peppers**	**0.0009**	**0.004058**	**0.00079**
	Cameraman	**0.003078**	**0.00055**	**-0.00039**
	Keyboard	**-0.00071**	**0.0076**	**0.00034**
	Mobile	**0.0013**	**0.00814**	**0.00118**
	Mouse	**-0.00098**	**0.003369**	**0.002243**

Differential Attack Performance Evaluation

This section studies the differential attack performance considering two metrics, which include NPCR and UACI. NPCR evaluates percentage of pixels that change when a single pixel is modified in original image. A high

NPCR value (close to 99%) indicates that even a minor change in the input image results in drastic differences in the encrypted image, which is essential for resisting differential attacks. The UACI measures the average intensity difference between the original and encrypted images. A higher UACI value indicates a stronger encryption algorithm as it signifies significant intensity changes between corresponding pixels. The ideal UACI value should be close to 33% for a well-encrypted image. The NPCR and UACI is evaluated using Eq. (23) and Eq. (24).

$$NPCR = \frac{\sum_{i,j} \quad D(i,j)}{W * H} * 100 \tag{23}$$

$$UACI = \frac{1}{W * H}\left[\sum_{i,j} \quad \frac{|C(i,j) - C'(i,j)|}{255}\right] * 100 \tag{24}$$

In Eq. (23) and Eq. (24), H and W denotes height and width of grayscale image, C and C' denotes encrypted components on basis of two input image components having single-pixel changes. For image pixels (i,j), if $C(i,j) = C'(i,j)$, then $D(i,j) = 1$, else $D(i,j) = 0$. The results from Tables 5 and 6 indicate that the proposed TSCD-EWM model outperforms existing encryption methods in terms of NPCR and UACI, ensuring higher security and resistance to differential attacks. For NPCR, TSCD-EWM achieves 99.77% for Peppers and 99.7845% for Mouse, which are higher than previous works [21], [22], and [23]. This indicates that even a minor change in the input image leads to a significantly different encrypted output, demonstrating strong diffusion properties and resistance to cryptographic attacks.

Table 5. NPCR Comparison.

Model	Image	NPCR
[21]	Peppers	99.65
[22]	Cameraman	99.609
[23]	Peppers	99.6076
TSCD-EWM	**Peppers**	**99.77**
	Cameraman	**99.7645**
	Keyboard	**99.7235**
	Mobile	**99.7224**
	Mouse	**99.7845**

For UACI, TSCD-EWM achieves values around 33.5755%–33.5782%, which are slightly higher than existing methods, as presented in Table 6. This means that the intensity variations in encrypted images are more significant, ensuring greater randomness and unpredictability. Overall, the TSCD-EWM model enhances confusion and diffusion properties, making it a robust encryption scheme against various cryptanalysis techniques, thereby ensuring secure data transmission and storage in cloud-based EWM systems.

Table 6. UACI comparison.

Model	Image	UACI
[21]	Peppers	33.89
[22]	Cameraman	33.4518
[23]	Peppers	33.4527
TSCD-EWM	**Peppers**	**33.4618**
	Cameraman	**33.5755**

	Keyboard	**33.5773**
	Mobile	**33.5782**
	Mouse	**33.5373**

Comparative Study

The comparative study in Table 7 highlights the effectiveness of the TSCD-EWM model in terms of IE, NPCR, and UACI, despite having a lower key space. TSCD-EWM achieves 7.9999 IE, which is higher than existing approaches [21], [22] and [23], indicating that the encrypted images have an almost uniform distribution of pixel intensities, making them highly resistant to statistical attacks. Additionally, TSCD-EWM attains an NPCR of 99.77%, outperforming prior models, which means it provides better diffusion properties and ensures significant changes in encrypted images even with minor input variations. For UACI, TSCD-EWM achieves 33.1073%, which, although slightly lower than some existing models, still demonstrates a strong confusion property by effectively altering pixel intensities in the encrypted images. Despite having a lower key space (2^{64}) compared to other models (e.g., $2^{388874304}$ in [21]), TSCD-EWM maintains strong encryption security, proving its efficiency in lightweight encryption approach, making it a viable solution for secured cloud-based EWM systems.

Table 7. Comparative Study.

Model	Key Space	IE	NPCR	UACI
[21]	$2^{388874304}$	7.999	99.65	33.89
[22]	2^{512}	7.9993	99.609	33.4518
[23]	$> 2^{100}$	7.9992	99.6076	33.4527
TSCD-EWM	2^{64}	7.9999	99.77	33.1073

5. Conclusion

E-waste has become a significant environmental concern due to the rapid advancement of technology and the increasing disposal of electronic devices. Managing e-waste securely and efficiently is crucial, as sensitive data stored in electronic components can be exploited by attackers. While several security approaches have been proposed for data protection in cloud-based systems, existing models suffer from high computational complexity and inefficiencies in lightweight implementation. Furthermore, trust-based methods are complicated, and image-based security techniques have not been effectively applied to cloud environments. To address these issues, this work presents TSCD-EWM, which integrates a trust-based security approach for data transmission and a secured cloud data processing mechanism to enhance EWM security. The proposed model ensures secure data sharing among stakeholders while mitigating attacks on e-waste data. The experimental results demonstrate the superior performance of TSCD-EWM in various security metrics. The IE of 7.9999 confirms the randomness of the encrypted data, making it highly resistant to statistical attacks. The NPCR value of 99.77% ensures strong diffusion properties, preventing differential attacks. Additionally, the UACI value of 33.1073% indicates effective confusion characteristics, making encryption robust. Compared to existing models, TSCD-EWM achieves these results with a significantly lower key space 2^{64}, proving its efficiency in lightweight encryption approach. The TSCD-EWM enhances data security in EWM by ensuring secure transmission and cloud processing with reduced computational complexity. Future work could focus on improving the security model by integrating AI-driven anomaly detection mechanisms to further strengthen protection against evolving cyber threats in cloud-based EWM systems.

References

1. R. Rajesh, D. Kanakadhurga, and N. Prabaharan, “Electronic Waste: A critical assessment on the unimaginable growing pollutant, legislations and environmental impacts,” Environmental Challenges, vol. 7, no. 100507, p. 100507, Mar. 2022, doi: 10.1016/j.envc.2022.100507.
2. R. Seif, F. Z. Salem, and N. K. Allam, “E-waste recycled materials as efficient catalysts for renewable energy technologies and better environmental sustainability,” Environment, Development and Sustainability, Jan. 2023, doi: 10.1007/s10668-023-02925-7.
3. M. Jain, D. Kumar, J. Chaudhary, S. Kumar, S. Sharma, and A. S. Verma, “Review on E-waste management and its impact on the environment and society,” Waste Management Bulletin, vol. 1, no. 3, pp. 34–44, Dec. 2023, doi: 10.1016/j.wmb.2023.06.004.

4. K. Liu, Q. Tan, J. Yu, and M. Wang, “A global perspective on e-waste recycling,” Circular Economy, vol. 2, no. 1, p. 100028, Feb. 2023, doi: 10.1016/j.cec.2023.100028.
5. K. Fatema, M. N. Hassan, S. Hasan, and H. Roy, “E-waste recycling in an optimized way for copper recovery by leaching and a case study on E-waste generation and management in Dhaka city,” Heliyon, vol. 11, no. 1, p. e41453, Dec. 2024, doi: 10.1016/j.heliyon.2024.e41453.
6. S. P. Grandhi, P. P. Dagwar, and D. Dutta, “Policy pathways to sustainable E-waste management: A global review,” Journal of Hazardous Materials Advances, vol. 16, p. 100473, Nov. 2024, doi: 10.1016/j.hazadv.2024.100473.
7. R. Bleischwitz et al., “The circular economy in China: Achievements, challenges and potential implications for decarbonisation,” Resources, Conservation and Recycling, vol. 183, p. 106350, 2022, doi: 10.1016/j.resconrec.2022.106350.
8. S. P. Grandhi, P. P. Dagwar, and D. Dutta, “Policy pathways to sustainable E-waste management: A global review,” Journal of Hazardous Materials Advances, vol. 16, p. 100473, Nov. 2024, doi: 10.1016/j.hazadv.2024.100473.
9. A. L. Srivastav et al., “Concepts of circular economy for sustainable management of electronic wastes: challenges and management options,” Environmental Science and Pollution Research, vol. 30, Feb. 2023, doi: 10.1007/s11356-023-26052-y.
10. N. Kapoor, P. Sulke, and A. Badiye, “E-waste forensics: An overview,” Forensic Science International: Animals and Environments, vol. 1, p. 100034, Nov. 2021, doi: 10.1016/j.fsiae.2021.100034.
11. A. U. R. Khan and R. W. Ahmad, "A Blockchain-Based IoT-Enabled E-Waste Tracking and Tracing System for Smart Cities," in IEEE Access, vol. 10, pp. 86256-86269, 2022, doi: 10.1109/ACCESS.2022.3198973.
12. A. A. Alarood, A. Abubakar, A. Alzahrani, and F. S. Alsubaei, “Electronic Waste Collection Incentivization Scheme Based on the Blockchain,” Sustainability, vol. 15, no. 13, p. 10209, Jan. 2023, doi: 10.3390/su151310209.
13. M. H. Shirvani and M. Masdari, “A Survey Study on Trust-based Security in Internet of Things: Challenges and Issues,” Internet of Things, p. 100640, Nov. 2022, doi: 10.1016/j.iot.2022.100640.
14. R. Wang, C. Li, K. Zhang, and B. Tu, “Zero-trust based dynamic access control for cloud computing,” Cybersecurity, vol. 8, no. 1, Feb. 2025, doi: 10.1186/s42400-024-00320-x.
15. M. Dawood, S. Tu, C. Xiao, H. Alasmary, M. Waqas, and S. U. Rehman, “Cyberattacks and Security of Cloud Computing: A Complete Guideline,” Symmetry, vol. 15, no. 11, pp. 1–33, Nov. 2023, doi: 10.3390/sym15111981.
16. S. T. Alshammari, M. Al-Razgan, T. Alfakih and K. A. AlGhamdi, "Building a Comprehensive Trust Evaluation Model to Secure Cloud Services From Reputation Attacks," IEEE Access, vol. 12, pp. 150754-150775, 2024, doi: 10.1109/ACCESS.2024.3471337.
17. M. Hegde, R. R. Rao and R. Bhat, "Design of an Efficient and Secure Authentication Scheme for Cloud-Fog-Device Framework Using Key Agreement and Management," in IEEE Access, vol. 12, pp. 78173-78192, 2024, doi: 10.1109/ACCESS.2024.3407103.
18. A. Brighente, M. Conti, G. D. Renzone, G. Peruzzi and A. Pozzebon, "Security and Privacy of Smart Waste Management Systems: A Cyber–Physical System Perspective," in IEEE Internet of Things Journal, vol. 11, no. 5, pp. 7309-7324, 1 March1, 2024, doi: 10.1109/JIOT.2023.3322532.
19. W. Alexan, M. Gabr, E. Mamdouh, R. Elias and A. Aboshousha, "Color Image Cryptosystem Based on Sine Chaotic Map, 4D Chen Hyperchaotic Map of Fractional-Order and Hybrid DNA Coding," IEEE Access, vol. 11, pp. 54928-54956, 2023, doi: 10.1109/ACCESS.2023.3282160.
20. D. Huang, Z. Zhang, Y. Tu and L. Xie, "Colour Image Encryption System Based on Four-Dimensional Memristor Hyperchaotic," IEEE Access, vol. 12, pp. 161530-161544, 2024, doi: 10.1109/ACCESS.2024.3439191.
21. L. Dai, L. Hu, L. Chen, C. Wang and F. Lin, "An Image Double Encryption Based on Improved GAN and Hyper Chaotic System," in IEEE Access, vol. 12, pp. 135779-135798, 2024, doi: 10.1109/ACCESS.2024.3462547.
22. Z. Chong, C. Wang, H. Zhang, P. Ma and X. Li, "Image Encryption Algorithm Based on a Hybrid Model of Novel Memristive Hyperchaotic Systems, DNA Coding, and Hash Functions," Complex System Modeling and Simulation, vol. 4, no. 3, pp. 303-319, September 2024, doi: 10.23919/CSMS.2024.0015.
23. Y. -C. Lan and C. -M. Wang, "A Novel Multi-Image Encryption Scheme Using Generalized Rectangular Transform and Advanced 5-D Hyperchaotic Map," in IEEE Access, vol. 13, pp. 43316-43337, 2025, doi: 10.1109/ACCESS.2025.3547891.
24. P. N. Andono and D. R. I. M. Setiadi, "Improved Pixel and Bit Confusion-Diffusion Based on Mixed Chaos and Hash Operation for Image Encryption," in IEEE Access, vol. 10, pp. 115143-115156, 2022, doi: 10.1109/ACCESS.2022.3218886.
25. Jeffrey Bush, February 7, 2021, "C4L Image Dataset", IEEE Dataport, doi: 10.21227/bc9m-f507.
26. E-waste Object Detection Dataset (v1, E-waste) by new-workspace-f7og7, “E-waste Object Detection Dataset (v1, E-waste) by new-workspace-f7og7,” Roboflow, 2022. https://universe.roboflow.com/new-workspace-f7og7/e-waste-mx8fq/dataset/1 (accessed Mar. 19, 2025).