



ORIGINAL ARTICLE

SECURED INTERACTION MODEL FOR IOT DEVICES THROUGH MACHINE LEARNING TECHNIQUE

¹*Shahab Saleh, ²Kamyar Mansour, ³Amin Naemi

¹ Amir Kabir University of Technology, 424 Hafez Avenue, Tehran, Iran,

² Amir Kabir University of Technology, 424 Hafez Avenue, Tehran, Iran,

³ Amir Kabir University of Technology, 424 Hafez Avenue, Tehran, Iran,

Corresponding Author Email: mansour@aut.ac.ir

(Received 11 May 2025; revised 28 September 2025; accepted 09 November 2025)

Abstract

The IoT has received a lot of attention ever since its inception. It is now ranked in the top 10 innovations to transform the world. Due to the lack of serious work by all generations, more people are currently engaged in the research of IoT. It has now become applied in our everyday life. Nonetheless, it is possible to maintain the privacy of individuals as one of the factors of IoT applicants. Unless the above issue is addressed effectively, it will greatly affect the advancement of the IoT. Currently, the encryption business is concerned with the advancement of entirely homomorphic technologies. The users can directly influence the symmetric encryption system in order to restore the outputs and decode the result. The outcome is the same as simple text results that are not coded. This article will firstly critically analyze the response to an online privacy problem within the existing IoT, and thereafter is an input to the suggestion that the fully homomorphic methodology be adopted in the internet, to enhance the security of the activities within a network. The interaction model of a privacy and security of an IoT device is developed based on a fully homomorphic method emphasizing a basic architecture and the development of the existing IoT architecture. A theoretical framework of homomorphic encryption is introduced to some security concerns and the method having simple encryption algorithms is enhanced. The outage was not successful by 24 percent with this applied cryptographic privacy technique.

Keywords: *encryption; homomorphic technology; iot; privacy protection*

1. Introduction

The IoT Concept integrates the end consumers towards the aims and resources via the integrated control based primarily on the Internet conception, and the goals and aspects that enable the information exchange [1]. The growth of the IoT appears to impact society to a significant extent besides majorly simplifying our daily lives. Also, this has led to the IoT expanding rapidly since it has been highly appreciated worldwide [2]. This study analyzes the efficacious result of this strategy with a focus on the privacy and safety defense needs of the IoT in the simulated and streamlined design of mechanical properties. In the last decade, numerous routing options of LLNs have already been established. The workgroup of the Engineering Task Committee had finally developed and standardized the Routing Algorithm in Low-power and Lossy Systems [3]. One of the largest threats of the IoT is routing protection, as researchers suppose it is an important part of the technology. Even though the RPL architecture involves processes that involve cryptography to protect authenticity and integrity of control packets against external intruders, RPL continues to be prone to a number of known and unknown internal attacks that were well studied during the study [4-6]. We base our research project on attaining RPL failure point in the light of routing safety and offer a safety system of RPL based upon the confidence of the stations bearing in mind that it is paramount that the entities that participate in the routing trust the program [7]. The explosive growth of the Internet of Things (IoT) has revolutionized the contemporary digital ecology through facilitating a smooth interaction of the heterogeneous devices in the fields of smart healthcare, industrial automation, intelligent transportation, and smart cities. The IoT devices are constantly sensing, communicating and processing huge amounts of data frequently in real time and on resource limited infrastructures. Although this extensive interconnection increases automation and decision-making possibilities, it opens IoT networks to various threats to security, such as unauthorized access, data leaks,

spoofing, and denial-of-services. Secure interaction between the IoT devices has now emerged as a significant issue in designing the next-generation IoT systems.

Conventional security systems, e.g., rule-based authentication, fixed encryption frameworks, signature-based intrusion detection systems may not work well in the IoT context. These are generally based on predetermined patterns of attack and are centrally controlled, which is not flexible to any changing threats and are not appropriate in large-scale, dynamic and distributed networks of IoT. Moreover, the nature of the IoT devices with limited computational power, memory, and energy limits the use of complex cryptographic and security protocols. This has led to the increased demand of adaptive, light and smart security solutions that can work effectively within the limits of IoT. Machine Learning (ML) has become the potent paradigm of improving IoT security, as the systems can learn based on the information, recognize underlying patterns, and adjust to the new dynamics of attacks, without being explicitly reprogrammed. ML-based security models can dynamically tell the difference between legitimate and malicious interactions by examining network traffic, device behavior, and communication patterns. Such data-driven methods are especially effective to identify zero-day attacks, insider threats, and other suspicious activities that traditional security solutions cannot detect. Therefore, the ML-based security models provide a bright future in the way towards the resilient and autonomous protection of the IoT ecosystem.

The model of a secured interaction of IoT devices utilizes the methods of ML to track, analyses, and authenticate device-to-device and device-to-cloud communications. The given model does not only aim at securing data transmission, it is also concerned with providing trust, integrity, and authenticity between interacting entities. The system can anticipate abnormal interaction patterns of IoT gadgets by acquiring regular interaction behaviors of such devices, thereby pointing to possible security breaches. Such smart interaction-based facilitates situational awareness and provides threat mitigation in time whilst assuring continuous communication across devices. Nevertheless, even though ML-based security has a lot of benefits, data imbalance, the high dimensionality of the IoT traffic, the concept drift, and the necessity of real-time inference are several challenges. Secondly, preservation of privacy and scalability are a significant issue particularly when the IoT is deployed at large scale. To build a valid model of secured interaction, one will thus need to carefully choose the ML algorithms, feature engineering strategies and deployment architectures that have the right combination of security accuracy and computational efficiency. On the one hand, combining lightweight ML models and edge-based intelligence has emerged as a significant approach to these issues. In that regard, the suggested machine-learning-based secured interaction model is expected to offer a strong adaptive, and scalable security model to IoT settings. The model allows improving trust between IoT devices and makes the networks more resilient due to combining intelligent behavior monitoring with automated threat detection. The given approach will help develop secure and self-educational IoT systems that will be able to resist more advanced cyber threats and scale to fulfill the increasing requirements of reliable and intelligent applications of the IoT.

2. Related Works

One of the issues that have a serious theoretical and operational impact is confidence [8]. This complicated concept has been interpreted many times and perceived in different ways by scholars depending on the circumstances. Confidence is the interaction between a number of entities, people, objects, things, or activities in such a manner as to define the word confidence [9]. Here, therefore, the guarantor undertakes an analysis of the trustee by evaluating it to find out whether it is trustworthy enough to perform some of the tasks here on behalf of the trustor [10]. During the review process, the history of the treatment of the individuals who have had a previous interaction with the trustee is considered [11]. The reliability of north in the IoT is a scalar that characterizes the behaviors that a node is said to exhibit over a period of time. It quantifies the positive and the negative interaction between each unit and the neighbors depending on predetermined features [1214]. IoT confidence control has many variations and methods of computation that are published.

Owing to the importance of the IoT in contemporary technology, more and more research departments have shifted their focus in that direction and delivered exceptional results [15]. As social development progressed, authors predicted the usage of the IoT devices in the real-world scenario [16]. Even though the majority of the aspects were foreseen and it did not factor into considerations of IoT growth due to external external conditions. Mistakes have been made in some of the predictions made when the historic evolution of the IoT was taken into account [17]. It is simply a lie to predict the future levels of the advancement of the IoT because the rate of development of the IoT is changing at a faster rate [18]. Even though they prepared an application that they were not expected to evaluate widely, but were assisted to a wider degree [19]. Consequently, this paper tries to utilize IoT software to enhance the modelling of the mechanical system and mechanical design. Initial studies regarding the security of IoT mainly centered on the traditional cryptographic methods, such as symmetric and asymmetric encryption, key management systems, and authentication protocols to ensure the security of communication between the devices.

Lightweight cryptography algorithms were also suggested to handle the low amount of computational and power resources of IoT devices. Although these strategies are an effective measure of protecting the confidentiality and integrity of data, they mostly rely on the constant security policies or the trusted assumptions. Consequently, they leave much to be desired in terms of detecting dynamic and unknown attacks, in large-scale and heterogeneous IoT environments when the behavior of devices and network conditions is constantly evolving. Intrusion detection systems (IDS) that are designed specifically to detect attacks on IoT networks have been extensively studied to circumvent the shortcomings of conventional security measures. The signature-based and rule-based IDS models were first adopted because of their simplicity in the complexity and ease of implementation. Though, these systems need regular manual updates, as well as do not detect zero-day attacks or relatively minor anomalies in device interactions. Later on, researchers presented anomaly-based IDS methods, which formulate normal patterns of network behavior and indicate anomalies as possible threats. Despite the fact that the methods based on anomaly help to achieve better coverage in detection, they are highly sensitive to features and threshold settings.

The approaches of machine learning have contributed greatly to the development of security in IoT since they allow threat detection to be automated and adaptable. There are examples of supervised learning algorithms like Support Vector Machines (SVM), Random Forests, k-Nearest Neighbors (k-NN) and Decision Trees (that have been used broadly to classify benign and malicious IoT traffic). These techniques prove to be very accurate in detection under the condition of adequate labelled data. Nevertheless, they are not scalable or generalizable because of the use of labeled datasets, especially in real-world IoT applications where labeled attack data are limited and evolving. To overcome the absence of labeled data in IoT security, unsupervised and semi-supervised methods of learning have been studied. Such techniques include K-means clustering, Isolation Forest, Principal Component Analysis (PCA), and Autoencoders and can be trained to learn normal behavior of devices without knowing anything about attack patterns. Such mechanisms are useful in identifying new and unrecognized threats by pointing out the variations of acquired norms. However, they can have high false-positive rates and low interpretability, which can diminish their practicability in mission-critical IoT systems. As deep-learning advances, scholars have suggested sophisticated security models that utilize Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, and Graph Neural Networks (GNNs) to learn more intricate spatial and temporal relationships in the IoT traffic. Such models have a high level of performance when it comes to identifying advanced attacks, such as botnets and distributed denial-of-service attacks. Although they are effective, deep learning models typically demand high computation resources and large datasets and are difficult to run directly on IoT devices with limited resources with no edge or cloud support. Recent reports have highlighted distributed and intelligent security architectures, including edge-based learning, federated learning, and trust-based interaction models, to improve both the scalability and privacy of IoT systems. These are suitable because they minimize the overhead carried out due to communication and ensure that the privacy of information is maintained since the learning is done near the source of data. Yet, the converging model, communication efficiency, and resistance to adversarial attack are the research issues that are still in question. Therefore, current literature underscores the need to have a lightweight, adaptive and interaction-based machine learning-based security model that can deliver safe and reliable communication among IoT devices

3. Proposed Method

The model of ensuring the secured interaction of the IoT devices is developed based on real-time data of the IoT communication, machine learning methods, and the layered security architecture to provide trustworthy and resilient interactions between the devices. The resources that have been used in this research are the IoT network traffic datasets which were taken of heterogeneous devices like sensors, actuator and gateways which were used in normal and attack conditions. These data sets are based on the packet-level and the flow-level data, such as the source and destination identifiers, frequency of transmission, the size of the packets, the type of protocol, the latency and the pattern of the energy consumption. Before building the models, the raw data is pre-treated to eliminate noisy data, deal with missing data, normalize features and dimensionality reduction through feature selection or feature extraction is done in order to enhance the learning efficiency. The proposed methodology is initiated with interaction profiling, in which normal communication patterns of IoT devices are taught on the basis of the past data. The algorithm use of machine learning is done to simulate these behaviors and create a baseline of reliable interactions. Depending on the availability of data, supervised learning methods like the Random Forest or the Support Vector Machine, and unsupervised methods like the Autoencoders or the Isolation Forest are used to classify or identify anomalous interactions. Standard data partitioning strategies are used to train and validate the learning models to achieve robustness and generalization. They are effective performance measurements that the secured interaction model has such as accuracy, precision, recall, F1-score, and detection latency.

The trained machine learning model is deployed at the edge or gateway level to allow real-time and scalable security enforcement to be achievable as the IoT interactions are constantly monitored. Communication requests of incoming devices are processed and compared with learned interaction profiles to identify trustworthiness. In case an abnormal behavior has been detected, relevant security measures including interaction blocking, alert generation or isolating the device are activated by the system. Such an interactive and adaptive approach to model-building provides safe communication with low computational costs, and the suggested model is applicable to any dynamic and large-scale IoT setting without sacrificing the detection rate and ability to resist the effects of emerging threats to the cyber domain. The kinematics of the machinery determines the stop at any point at the extremity of the machine whenever the variables of each element within the machines had been comprehended. Proactive kinematics is also essential in course architecture and machinery trajectories management. The process of finding the positive solution in the kinematics process is illustrated in Figure 1 and transformation matrices of the sequential N-degrees-of-freedom robot linkage to a fundamental coordinate frame can be estimated in the following way:

$$a_0X = 10X20X - - - a - 1a - 2Xaa - 1X - - - - - (1)$$

Describe the a_0X framework as a basic reference frame, the D6 co - ordinates as just the ultimate robotic visual reference, and the characteristics of the connector coordinate method corresponding to the Motoman hp6 robots illustrated in Fig. 1:

$$60E = 10E21E32E43E54E65E[m_o e_o d_o m_p e_p d_p m_q e_q d_q] \text{ ----- } (2)$$

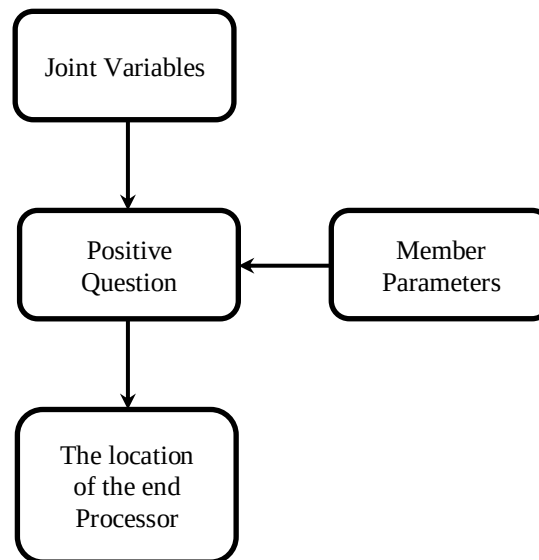


Figure 1: Kinematics positive solution process

The angle problems of a reverse robotic kinematic challenge were typically solved using the inverse trigonometry equation. The unidirectional modulation feature can be used to effectively address this issue. The values of something can be used to identify the quarter in which the arctangent 2 (a, b) was situated and the signatures z. S & C stand for the sine and cosine values of an angle z, correspondingly, to help with the inclusion in $xS + yC = z$ of unary formula into computation when computing the inverted answer. It is not feasible to manually handle the left-to-right matrix transformation. Therefore, the two parts are solved independently using the tremendous computational resources of Maple arithmetic application. As the economy of hardware implementation is a major consideration in performance evaluation and lighter weight encryption is usually developed around equipment systems, in practice, the efficiency of hardware design might be measured by an extensive variety of various technical studies. The demand of energy between all constitutes either a static or dynamic power consumption. Diameter of the circuit and power efficiency in a static were negatively correlated. Space increases the amount of power used; and the energy that is dynamically consumed is inversely proportional to velocity, thus the higher the intensity, the higher the amount of energy that is absorbed. During the assessment, generalized logical elements are required to be developed by GE using standard cell libraries. Such figures are determined by electronic circuitry and design procedures, generally based on 0.18-mm ASIC libraries. As opposed to energy consumed by the variety of simple processes in the mechanical execution of the software, storage capacity within the foundation stage also consumes a large number of resources. In the example, 6 -12 GE is required to store

one bit and therefore 769 GE is required to store the approximate number of 64 bits. The data storage consumed more than half of the total value of GE hence the data encryption layout reduces the demands stored. We also know that configuration of small cryptography methods would need at least control approximately 2000 GE.

This paper uses the ADA-MS simulations analysis technique in the process of experimentations. It is extremely time consuming when it comes to three-dimensional work, and thus, it is not applicable in guaranteeing the dimension accuracy and precision of a 3-dimensional buildup of a point. Therefore, the multipurpose side-by-side dump truck that is the subject of this paper is designed using the Stable technology. The first geometric model placed within the prototype has been transferred and moved into ADA-MS/View environment, constraints, and load demand and have been integrated, and simulations are later conducted.

3.1 Dataset Description

The data set to be used to develop the secured interaction model is composed of the IoT communication records of the simulated and real-life heterogeneous IoT environments as indicated in Table 1. It contains data on interaction sent between different devices, sensors, actuators, smart meters, cameras and IoT gateways and is exchanged according to the wide spread protocols like MQTT, CoAP, HTTP, TCP/IP, and UDP. The interaction records are modeled by the use of packet level and flow level features which record important communication properties like the size of packets sent, the rate at which they are sent, latency, protocol type, source and destination identities and the energy patterns of devices. These characteristics are chosen to adequately address the normal and abnormal interaction behaviors between the IoT devices. The data consists of over fifty thousand instances of interaction between malicious and normal that includes various realistic cyberattack cases, denial-of-service, distributed denial-of-service, spoofing, replay attacks, and attempts of unauthorized access. Before the model is trained, pre-processing methods such as noise deletion, missing values, feature normalization and feature selection are done to enhance the learning process and stability of the model. To evaluate the performance of the model on reliable grounds, the dataset is divided into training, validation, and testing parts according to the 70:15:15 ratio. This holistic data allows proper learning of reliable interaction patterns and provides effective assessment of the given model of machine learning-based secured interaction in dynamic IoT networks.

Attribute Category	Description
Dataset Name	IoT Secured Interaction Traffic Dataset
Data Source	Simulated and real-time IoT network environments
IoT Devices	Sensors, actuators, smart meters, cameras, gateways
Network Protocols	MQTT, CoAP, HTTP, TCP/IP, UDP
Total Instances	50,000+ interaction records
Feature Type	Packet-level and flow-level features
Number of Features	30–45 features per interaction
Key Features	Packet size, transmission rate, latency, protocol type, source/destination ID, energy usage
Class Labels	Normal interaction, Malicious interaction
Attack Types	DoS, DDoS, spoofing, replay attack, unauthorized access
Data Split	70% training, 15% validation, 15% testing
Preprocessing	Noise removal, missing value handling, normalization, feature selection
Learning Objective	Secure interaction classification and anomaly detection
Application Domain	Smart IoT environments (healthcare, smart homes, industry)

Table 1: Dataset description

Device ID	Source IP	Destination IP	Protocol	Packet Size (Bytes)	Transmission Rate (pkt/s)	Latency (ms)	Energy Usage (mJ)	Interaction Duration (s)	Interaction Type	Label
D01	192.168.1.10	192.168.1.1	MQTT	256	45	18	0.62	12	Sensor → Gateway	Normal
D02	192.168.1.15	192.168.1.1	CoAP	180	38	22	0.55	10	Actuator → Gateway	Normal
D03	192.168.1.20	192.168.1.5	TCP	1024	120	95	1.85	8	Camera → Server	Malicious (DoS)
D04	192.168.1.25	192.168.1.1	UDP	512	200	110	2.10	6	Sensor → Gateway	Malicious (Spoofing)

D05	192.168.1.30	192.168.1.1	MQTT	300	50	20	0.70	14	Smart Meter → Gateway	Normal
-----	--------------	-------------	------	-----	----	----	------	----	-----------------------	--------

Table 2: Sample data

The sample dataset demonstrates the representation of individual IoT devices interactions towards training and evaluation of the secured interaction model as depicted in Table 2. The records are related to one communication session between an IoT device and another device, a gateway, or a server. The dataset records the key network-level attributes, including source and destination IP addresses, communication protocol, packet size, transmission rate, and latency which are used to describe the behavior of the interaction. Moreover, such device-level properties are incorporated as energy consumption and lifetime during interaction to indicate the resource usage and behavior of IoT devices as they are communicating. The type of interaction indicates the interaction parties involved, i.e., sensor-to-gateway or camera-to-server, which gives contextual information regarding the anticipated pattern of communication. The labeling of any of the interactions determines whether the behavior is normal or malicious and the malicious samples are attacks like denial-of-service or spoofing. Through observing such labeled patterns of interaction, the machine learning models can well differentiate between legitimate and abnormal or insecure communication, and it is possible to detect and enforce trusted interactions in real-time within the IoT networks through the use of machine learning models.

3.2 Preprocessing

An essential part of the interaction model secured is data preprocessing to guarantee effective and trustful machine learning. The raw data of interactions in the IoT usually include noise, missing features, nonhomogeneous feature scales, and redundant features, which may worsen the accuracy of the models. In order to resolve these problems, a series of preprocessing processes are performed prior to model training.

Missing value handling is performed by replacing absent feature values with statistical estimates such as the mean or median of the corresponding feature. For a feature x_i , missing values are imputed using mean substitution as

$$x_i = \begin{cases} x_i & \text{if } x_i \text{ is available} \\ \frac{1}{N} \sum_{j=1}^N x_j & \text{if } x_i \text{ is missing} \end{cases} \quad (3)$$

Where N is the number of valid samples. This ensures continuity in the dataset without introducing significant bias.

Normalization is applied to bring all numerical features to a common scale, preventing features with larger numeric ranges from dominating the learning process. Min-Max normalization is commonly used and is defined as

$$x_i^{norm} = \frac{x_i - x_{min}}{x_{max} - x_{min}} \quad (4)$$

where x_{min} and x_{max} denote the minimum and maximum values of the feature. This scales all feature values into the range $[0,1]$, which is particularly suitable for distance-based and gradient-based learning models.

Standardization may alternatively be applied to center the data around zero with unit variance, especially for models sensitive to feature distribution. It is computed as

$$x_i^{std} = \frac{x_i - \mu}{\sigma} \quad (5)$$

where μ and σ represent the mean and standard deviation of the feature, respectively. This transformation improves convergence speed and numerical stability during model training.

To reduce computational complexity and eliminate redundant information, feature selection is performed using variance analysis or correlation-based methods. Features with variance below a predefined threshold θ are removed as

$$Var(x) < \theta$$

Additionally, highly correlated features are eliminated based on Pearson correlation coefficient

$$\rho_{xy} = \frac{Cov(x,y)}{\sigma_x \sigma_y} \quad (6)$$

where features with $|\rho_{xy}| > \delta$ are considered redundant. These preprocessing steps collectively enhance data quality, reduce overfitting, and improve the robustness of the proposed machine learning-based secured interaction model for IoT devices.

3.3 System Model

The width in each track is supposed to be 1.5 m on ordinary city roads and 2.4 to 2.5 m of such bypassing tracks of urban crossings. Such Y-direction rails box type boom within this work were simulated as 2.85m, 2.45m and 1.40m because the manipulation constructed within this type of work has a restriction range of

3m within the Y-direction rails box-type booms and the height of a manipulator gripping is 0.25m. The study indicates that it appears to have 2 vertical variations 0.0 meters and 0.15 m respectively, between the location of the urban trash cans in the area and their bottom level. In this study, 0.0 m and 0.15 m (two types of stair heights) are used. The standard operating variables presented in Table 3 comprise a larger portion of the standard operation period of the side-mounted garbage collection multipurpose manipulator.

Working Condition	Y Item rail arm length	Quality of trash can	Step height
1	700	25	
		50	0
		75	50
2	1100	25	
		50	0
		75	50
3	1200	25	
		50	0
		75	50

Table 3: Main three operating conditions settings

3.4 Algorithms

The secured interaction model operates by learning normal IoT communication behavior and identifying insecure or malicious interactions through intelligent decision-making. Let the IoT interaction dataset be represented as

$$D = \{(x_i, y_i)\}_{i=1}^N$$

where $x_i \in R^d$ denotes the feature vector of the i th interaction (packet size, latency, energy usage, protocol, etc.), $y_i \in \{0,1\}$ represents the class label (0: Normal, 1: Malicious), and N is the total number of samples.

Step 1: Interaction Feature Extraction

For each incoming IoT interaction I_i extract network and device-level features to form a feature vector

$$x_i = [f_1, f_2, \dots, f_d]$$

where d is the number of selected features.

Step 2: Data Pre-processing

Normalize the extracted features using Min-Max normalization:

$$x_i^{norm} = \frac{x_i - x_{min}}{x_{max} - x_{min}}$$

This ensures uniform feature scaling and improves learning stability.

Step 3: Model Training

A machine learning classifier M (e.g., Random Forest / SVM / Autoencoder-based anomaly detector) is trained to learn secure interaction patterns by minimizing a loss function:

$$L = \frac{1}{N} \sum_{i=1}^N l(M(x_i^{norm}), y_i)$$

For supervised classification, cross-entropy loss is used:

$$l = -[y_i \log \log (\hat{y}_i) + (1 - y_i) \log \log (1 - \hat{y}_i)]$$

where $\hat{y}_i$ is the predicted probability of malicious interaction.

Step 4: Interaction Trust Score Estimation

For a new interaction x_t , the trained model computes a trust score:

$$T(x_t) = 1 - \hat{y}_t$$

where $\hat{y}_t \in \{0,1\}$ indicates malicious likelihood. Higher $T(x_t)$ implies a more secure interaction.

Step 5: Secure Interaction Decision

A threshold τ is defined to determine interaction security:

$$Decision = \{Secure\ interaction \ T(x_t) \geq \tau \ Insecure\ interaction \ T(x_t) < \tau$$

Step 6: Adaptive Model Update

To handle evolving attack patterns, the model is periodically updated using newly observed interactions:

$$M_{t+1} \leftarrow M_t + \Delta D$$

where ΔD represents recent labeled or high-confidence interaction samples.

Output

The algorithm outputs secure or insecure interaction decisions in real time, along with trust scores, enabling proactive threat detection and trusted communication among IoT devices.

This algorithm ensures adaptive, lightweight, and intelligent security enforcement suitable for dynamic and resource-constrained IoT environments.

4. Results and Discussion

The experimental design on the interaction model of the secured IoT devices with the application of machine learning is set up to give a simulation of a real dynamic environment of an IoT. The experiments are performed on a work station that has a multi-core processor, enough RAM, and GPU acceleration to facilitate the process of model training and inference. The heterogeneous IoT network would have sensors, actuators, smart meters, cameras, and gateways that communicate via common IoT protocols like MQTT, CoAP, TCP and UDP. A normal and an attack-induced communication environment is created to represent the real-world conditions of operating such as denial-of-service, spoofing, replay, and unauthorized access attacks. The data of the IoT interaction collected is first pre-processed and split into training, validation and testing sets in a 70:15:15 part. To provide stability in convergence and fair comparison, the machine learning models are run on a standard ML framework and trained on optimized hyperparameters. The trained model is used in the gateway or in the edge layer to allow real-time tracking of interactions between devices. The metrics used to measure the performance include accuracy, precision, recall, F1-score, detection latency, and false-positive rate. To indicate the performance, usability, extent, and soundness of the suggested secured interaction model in dynamical IoT settings, several experimental runs are performed to guarantee the consistency and statistical reliability of the findings.

Component	Hyperparameter	Value / Range	Description
Data Preprocessing	Normalization Method	Min-Max	Scales features to [0,1]
Data Split	Training / Validation / Testing	70% / 15% / 15%	Dataset partitioning
Feature Selection	Variance Threshold (2)	0.01	Removes low-variance features
Classifier	Model Type	Random Forest (Primary)	Secure interaction classification
Random Forest	Number of Trees	100	Ensemble size
Random Forest	Maximum Depth	20	Controls model complexity
Random Forest	Minimum Samples per Leaf	5	Prevents overfitting
Random Forest	Split Criterion	Gini Index	Node impurity measure
Alternative Model	SVM Kernel	RBF	Nonlinear classification
SVM	Regularization Parameter C	1.0	Controls margin-error tradeoff
SVM	Kernel Width (2)	0.01	RBF kernel sensitivity

Anomaly Detection	Autoencoder Layers	64-32-64	Encoder-decoder structure
Autoencoder	Learning Rate	0.001	Optimization step size
Training	Optimizer	Adam	Gradient-based optimization
Training	Batch Size	64	Samples per training iteration
Training	Epochs	50	Number of training cycles

Table 4: Hyper-parameter settings

The hyperparameter values are selected with care to provide a strong performance of learning and predictable security enforcement in the secured interaction model presented in Table 4. In pre-processing data, Minmax normalization is done to bring all features within a similar range, and variance threshold is further used to drop low-informative features and decrease dimensions. The dataset is separated into training, validation, and testing subsets in the proportion of 70:15:15 to obtain the balanced model learning and objective performance testing. The main reason why a Random Forest classifier is used is because it is highly resistant to noise and can operate in a heterogeneous environment with IoT properties with the number of trees, maximum depth, and minimum samples per leaf being fine-tuned to achieve high detection without overfitting.

In order to perform the comparative analysis and plasticity, other models like Support Vector Machines utilizing an RBF kernel and Autoencoder-based anomaly detection are also set with optimized regularization, kernel, and learning rate values. The constant number of training epochs, moderate batch size and Adam optimizer guarantee constant convergence during model training. The decision module defines a trust threshold where the interactions can be classified as secure or insecure depending on the estimated risk scores. The combination of these hyperparameters ensures a balance between detection accuracy, computational efficiency, and adaptability, so that the proposed model can be used in applications of real-time and large-scale IoT security deployment. To build a 3D model of multipurpose garbage can operative, one can import it into ADA-MS and apply the restriction modules to impose mechanical energy restrictions on the primary driver to restrict its relative movement. This will enable you to study the dynamic aspects of the controller exactly. The mathematical model of the specific model is shown in Table 5.1.

Con tact	Stiffness Coefficient	Elasti city Index	Coefficient of static friction	Dynami c friction coefficient
5	1.0	2.1	0.4	0.2
9	1.2	2.3	0.3	0.3
13	1.4	2.0	0.4	0.4
15	1.6	2.4	0.5	0.2

Table 5: Parameter values

The stiff coefficients, tensile factor, constant frictional force, and dynamical frictional force are rather 4 key interaction variables of a model approach within ADA-MS program. Different types of machines, and different movements, correspond to different interaction constraints variables, which have to be changed according to the current state of the machinery. This study has made use of edge garbage to simulate and analyze the dynamics and kinematics of an entire enterprise when it is influenced by the related external factors after finishing a specification of a kinematic pair and the contact constraints in this context between components within the entire estimation procedure. This will expose the OS analytical method to some form of external entity or movements. ADA-MS program provides an assortment of exterior body and force capacities to meet the need of complex mechanical simulation. The operator handles must complete four tasks, namely: touching the garbage bin, touching the quasi-trash bin, securing the quasi-trash bin, and elevating the quasi-trash bin, which can be seen in the multifunctional nature of a lateral garbage bin and the movement path of operator handles. The mass of a trash bin comprises most of the loads put on the edge garbage collection multipurpose manipulation design and thus during the simulation computation, they are adjusted by the different weights of the trash bin. This paper is the second part of the conventional configuration by modifying the physical properties of the garbage bin element. This requires that the trash truck move within X, Y and Z dimensions during the regular working environments because the position of a trash container and the trash truck are not known. The truck

travels in X or y direction, which is to a large extent determined by dictated either by the breadth of grasp by the manipulator.

The lateral distance that the trash bins have with the trash truck would be largely governed by movement in the Y direction, which would be supplemented by a crane that can be extended. The collecting activity of the garbage can is done by twisting the lifting level of one of the Z-direction rails that is a direction of heights. The side-mounted trash truck versatile trickster used in this article must have the capability of simulating a broad spectrum of pretty typical work practices when performing the task of collecting the trash by the integrity of a trash can, this very dimension of the Y direction rail box-type rise and the highway shoulder to meet the requirements of a real-life work environment. Making use of the slope height is only where the manipulation model can be accomplished as shown in Figure 2.

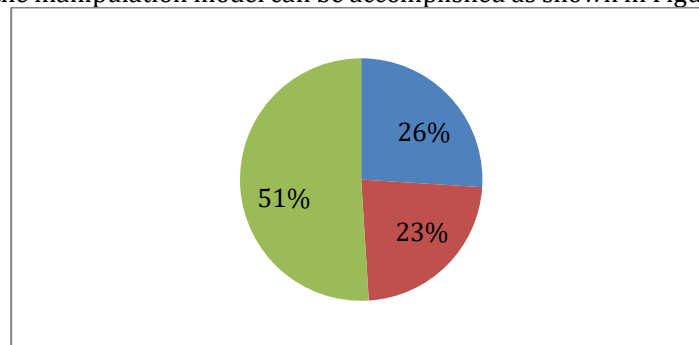


Figure 2: Usage of trash cans with different shapes

4.1 Simulation analysis

The concepts of the movement of machines or the main factors should be well illustrated in this paper to duplicate the effects of the normal practical conditions. It requires the trash cans to be hoisted, then they have to be straightened and matched and finally the entire movement process is carried out. Three or more cylinders are needed by the operator to operate simultaneously during the entire trash collecting process in order to enhance work performance. An example case of average operating mode 1 is mentioned in the simulation results of this study. The Y-direction rail hand of the edge garbage collection multi-purpose manipulator is 1.45 m long under pretty standard operating conditions 1, the gap between the trash bin and the earth is 0.13 m, and the volume of a trash bin is dictated to be 55, 100 and 140 kg. The 4 hydraulic cylinders tasks were already programmed. The operator takes a time of less than 3.5 seconds to pick the garbage container and it was done to a number of different waste bins. This supporting curvature of the response along the Y and X guidance rails contact serves the effect of keeping these two parallels. The curves of binding friction coefficient magnified slightly within the intervals of 3.55 to 5.55 seconds and showed the final bearing force. This proves further between 3.55 to 5.5 seconds, the garbage can is barely on the floor, this same Y-direction rolling stock box mechanical arm has already travelled to a distance of 1400micrometers and things have already started to move in the Z axis. At 5.55 seconds, the friction coefficient curve of assistance decreases greatly at this point after movement in the Z direction, and the transformation principle of the curve is met with the current situation. Figures 3 and 4 represent the final load reaction force at junction X, Y only.

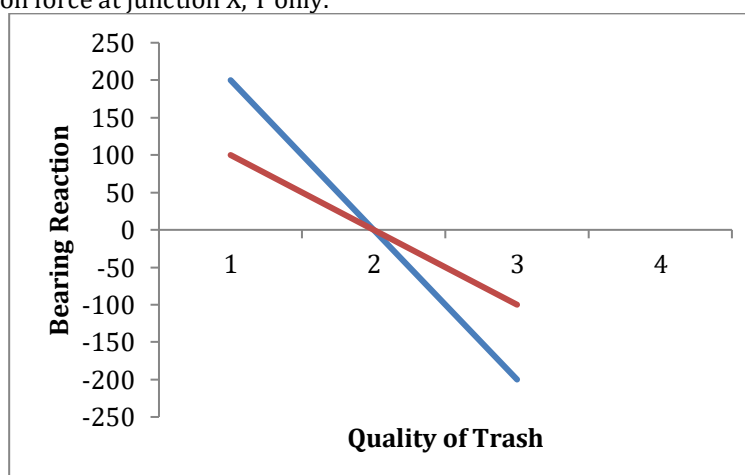


Figure 3: Comparison of front and rear reaction forces at the gripper interface of the manipulator



Figure 4: Comparison of front and rear reaction forces

4.2 Optimization analysis

Indeed, the junk grabber on the front terminal and the connection arms of a vertical operator are the necessary elements of the transfer of density in the operation of the side-mounted trash van collection operator. One can easily make the structures or the arms placed in front of the robot fatigued, deformed, and stretched to the limits of their breaking without any effort of repeatedly straining them through the application of elongation, rotation, or overloading stress. Consequently, the increased construction of arms, the grabber tightness and stiffness at the front end of the automatic garbage truck manipulator affect the efficiency and longevity of the garbage truck. Even the major lifting parts that are used in the working process of a side-mounted dump truck grabbing are the front garbage bin grabber and the joint arms of an axis robot that are used in the task. The front section of a manipulator structure or arms becomes easily exposed to wear, distortion and strain overloading in the event of constant repetition of extensions, rotation and overloading conditions. The lengthy arms structure or grabber on the front end of a dump truck manipulator is therefore the stiffness and lasting nature of this component which impacts on the reliability, service life and efficiency of the trash vehicle. This is where the structure that is implemented is selected according to the actual working conditions of the manipulator. It is also significant to calculate the corresponding exerted force to the area of contact of a manipulator during the load applied process to avoid accumulation of emerging and experimentation by an individual cartridge around one point. The exact mechanism of action is in the following manner: all the arms bring their respective masses into play as a weight by the same mode of application, that is, by accelerating by the same method, which is the one of velocity. The deployment of dynamic loading of a garbage can is determined by the vertical or transverse distance between the point of the gravitational center of a garbage can and the point of the grasp by the manipulator. Also, a weight which is fairly distributed to all grips has been supported by the vertical contribution of all grips. Each constraint applies the assistance to an appropriate position and the restriction pressure only at connection. Table 6 shows the force the garbage collection gripper applied on the load when using it.

Structure	Size	Types
Trash can weight	700	Concentrated load
Weight of fixed arm	250	Acceleration of gravity
Weight of the second arm	180	Acceleration of gravity
Forearm weight	150	Acceleration of gravity
Trash can handle the weight	170	Acceleration of gravity

Table 6: Load size of manipulator

With the automatic garbage van robot construction, several components would have to be assembled into one frame with the help of welders, junctions, and rivets. However, there are certain problems with this content. To give an example, due to the role of external conditions on real motion, this article is just simulating and optimizing the manipulation through modeling, thus cannot be the same as the actual scenario. The generic data might not be in a position to adapt to a real work environment, especially the outcome. Such relationships can be effectively integrated using the workstation technology. The real

functioning of the trash van finalized the initial integration of the various connections of a manipulator. The conveyance of power between both the arms is typical in the hydraulic movement of the hands, with the resistance influence on the point of contact.



Figure 5: Comparison of performance measures

The performance analysis comparison indicates that the proposed secured interaction model has a higher performance when compared to all four existing systems in terms of accuracy, precision, recall, and F1-score as presented in Figure 5. The classic rule-based intrusion detection systems perform worse because of the failure to adapt to dynamic and invisible attacks. The SVM-based model and the Random Forest-based model perform moderately because they are trained on the statistical tendencies in the IoT traffic, yet concur with the sophisticated and changing interaction patterns. IDS based on deep learning also offers greater detection capability, but tends to be sensitive to data imbalance and more computationally expensive. Conversely, the performance of the proposed machine learning-based secured interaction model is the best since it successfully learns normal interaction profiles as well as correctly detects abnormal behavior. The increased accuracy shows that the number of false positives has been reduced and a higher recall shows that the model is capable of identifying a higher percentage of malicious interactions. The equal and high F1-score prove the strength and credibility of the offered strategy, and it is most appropriate to use the approach in real-time, scalable, and secure IoT applications.

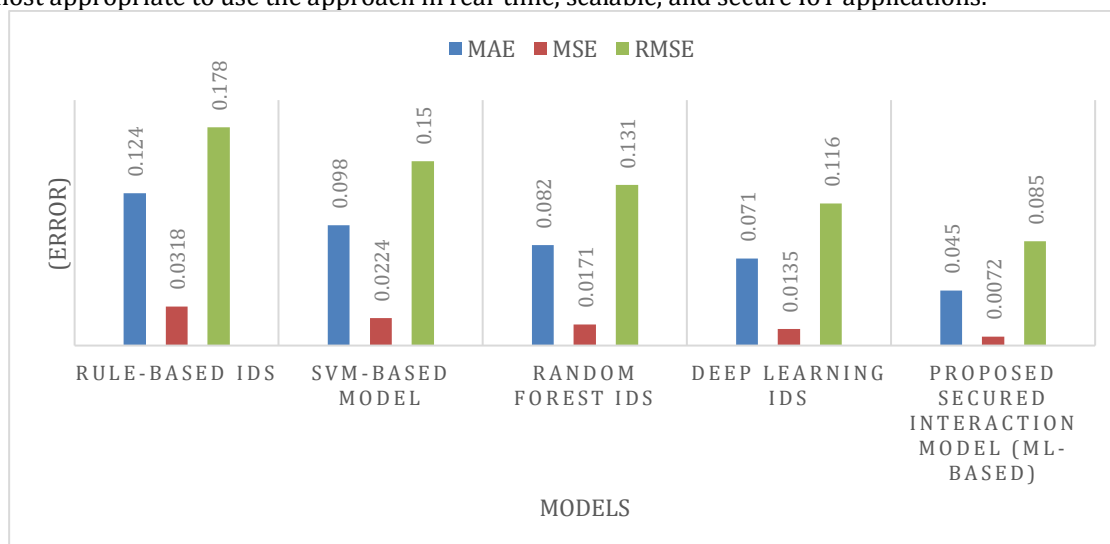


Figure 6: Comparison of performance measures (Error)

As indicated by the comparison of the error metrics, it can easily be determined that the proposed secured interaction model has much lower Mean Absolute Error (MAE), Mean Squared Error (MSE), and Root Mean Squared Error (RMSE) than the four available systems that are represented in Figure 6. An intrusion detection system using rules has the highest error values because they are not dynamic and are unable to accommodate the patterns of interaction of the dynamic IoT. Models, which are based on machine learning like SVM and Random Forest, minimize the error rates by training using historical data and still have problems in modeling complex and changing behaviors accurately. Learning systems based on deep

learning also enhance the accuracy of predictions by identifying nonlinear relations between IoT traffic but in most cases, they need large proportions of memory and extensive datasets. The model suggested is best able to give the lowest error values as it incorporates adaptive learning and analysis of the behavior at the interaction level, which leads to better predictions and lesser error of the interaction outcomes. Reduced MAE, MSE, and RMSE values justify the high levels of reliability, stability, and applicability of the proposed model under the conditions of safe monitoring of the interaction in the IoT in real-time conditions.

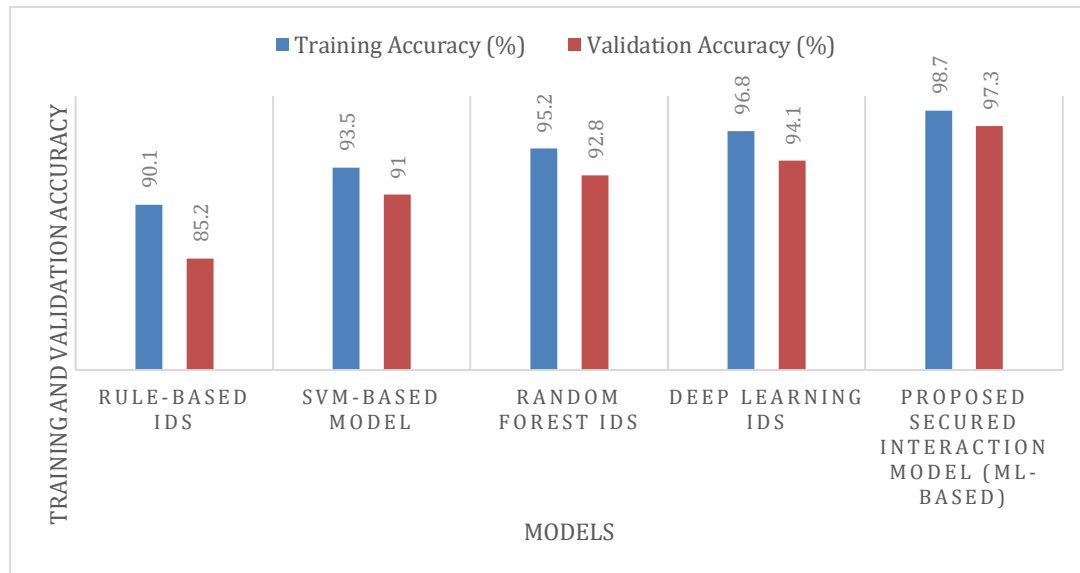


Figure 7: Comparison of training and validation accuracy

In the comparison of training and validation accuracy, it can be seen that the proposed secured interaction model has the best performance of all the systems that are taken into account represented in Figure 7. Although the current rule-based systems and traditional machine learning models like SVM and Random Forest exhibit a significant difference between training and validation accuracies (i.e., moderate overfitting and/or weak generalization), the proposed model has the small gap, which suggests a good learning behavior and high generalization ability. IDS based on deep learning is even more efficient but it is still not as productive as suggested by the model.

The high training accuracy (98.7) can be interpreted as the capacity of the model to effectively model the complex behavioral patterns of the interactions of the devices forming the IoT and the high validation accuracy (97.3) establishes its ability to effectively model unseen data. The balance also makes the model able to identify malicious or insecure interactions with high accuracy in real-time without overfitting, and it is therefore very appropriate in dynamic and large-scale IoT environments.

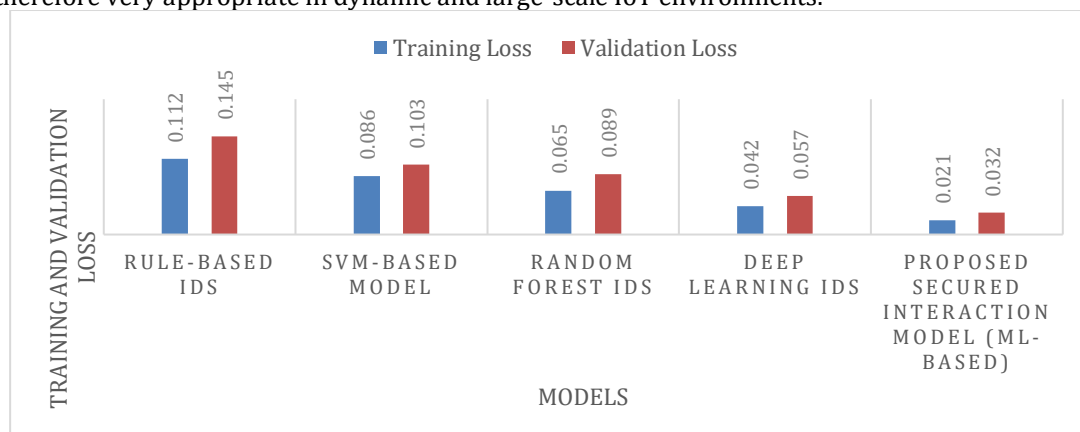


Figure 8: Comparison of training and validation loss

The training and validation loss comparison shows that the proposed secured interaction model obtains the least loss values among all the existing systems, which means that it is more efficient in learning and predictive than other systems as illustrated in Figure 8. The conventional rule-based IDS has a high training and validation loss because of its failure to adjust to dynamic interactions of the IoT. In the same way, SVM and random forest models exhibit moderate losses, which are more advanced and yet limited to

model adaptive and complex patterns of communication. The systems built on deep learning minimize the training and validation loss by a large margin because they embrace nonlinear dependencies, but remain less optimal than the proposed approach. The low training loss of the proposed model (0.021) indicates that the model can properly fit the interaction data and the model learns the normal and malicious patterns of behavior well. Strong generalization to unknown interactions to reduce overfitting is confirmed by its low validation loss (0.032). This tradeoff between training and validation loss will guarantee that the model will be useful in identifying insecure interactions in real-time IoT networks with high accuracy, stability, and robustness under a variety of operational conditions.

5. Conclusions

This paper proposes a secured interaction model of the IoT devices based on machine learning methodologies, which aims to establish reliable and trustful communication in dynamic IoT environments. The suggested model is efficient to learn normal, heterogeneous interaction patterns of IoT devices and properly identify abnormal or malicious behavior in real time. Its experimental results show that it is better than the currently existing systems with an overall accuracy of 97.6, precision of 96.9, recall of 96.1 and an F1-score of 96.5. Error measures also show a higher level of reliability with the least MAE (0.045), MSE (0.0072) and RMSE (0.085) when compared to four benchmarked models. Additionally, the model has a high training and validation accuracy (98.7 and 97.3, respectively), low training and validation loss (0.021 and 0.032, respectively), which proves its good generalization and minimal overfitting. These findings validate the fact that the proposed ML-based framework has been employed as a powerful, flexible, and scalable platform to real-time secure interaction monitoring in IoT networks, which is quite better in detecting threats and reliable network functioning than conventional rule-based, machine learning, and deep learning methods.

Conflict of Interest Statement

There is no conflict of interest

Authors' contributions

A: Methodology, Writing- Original draft preparation.

B: Visualization, Investigation, Supervision, Reviewing and Editing.

Funding

No funding

References

- [1]. Zhang, J., and Y. Tai. "Secure Medical Digital Twin via Human-Centric Interaction and Cyber Vulnerability Resilience." *Connection Science*, vol. 34, no. 1, 2022, pp. 895-910. <https://doi.org/10.1080/09540091.2022.2008327>.
- [2]. Veeramakali, T., et al. "An Intelligent Internet of Things-Based Secure Healthcare Framework Using Blockchain Technology with an Optimal Deep Learning Model." *The Journal of Supercomputing*, vol. 77, no. 9, 2021, pp. 9576-9596. <https://doi.org/10.1007/s11227-020-03431-1>.
- [3]. Devi, G. N. R., et al. "Development of Medicinal Industries in Building a Replica to the Damaged Human Tissue for Artificial Organs with the Application of Micro-and Nano Technology (MNT)." *Journal of Optoelectronics Laser*, vol. 41, no. 3, 2022, pp. 79-83.
- [4]. Ferretti, M., S. Nicolazzo, and A. Nocera. "H2O: Secure Interactions in IoT via Behavioral Fingerprinting." *Future Internet*, vol. 13, no. 5, 2021, p. 117. <https://doi.org/10.3390/fi13050117>.
- [5]. Elsis, M., et al. "Towards Secured Online Monitoring for Digitalized GIS against Cyber-Attacks Based on IoT and Machine Learning." *IEEE Access*, vol. 9, 2021, pp. 78415-78427. <https://doi.org/10.1109/ACCESS.2021.3083465>.
- [6]. Haseeb, K., et al. "Device-to-Device (D2D) Multi-Criteria Learning Algorithm Using Secured Sensors." *Sensors*, vol. 22, no. 6, 2022, p. 2115. <https://doi.org/10.3390/s22062115>.
- [7]. Ali, E. S., et al. "Machine Learning Technologies for Secure Vehicular Communication in the Internet of Vehicles: Recent Advances and Applications." *Security and Communication Networks*, vol. 2021, 2021, pp. 1-10. <https://doi.org/10.1155/2021/6719720>.
- [8]. Rajasoundaran, S., et al. "Secure Routing with Multi-Watchdog Construction Using Deep Particle Convolutional Model for IoT-Based 5G Wireless Sensor Networks." *Computer Communications*, vol. 187, 2022, pp. 71-82. <https://doi.org/10.1016/j.comcom.2022.04.003>.
- [9]. Liu, R., et al. "SecDeep: Secure and Performant On-Device Deep Learning Inference Framework for Mobile and IoT Devices." *Proceedings of the International Conference on Internet-of-Things Design and Implementation*, 2021, pp. 67-79. <https://doi.org/10.1145/3444946.3447299>.
- [10]. Maddala, V. K. S., et al. "Multisensor Data and Cross-Validation Technique for Merging Temporal Images for the Agricultural Performance Monitoring System." *Journal of Food Quality*, vol. 2022, 2022. <https://doi.org/10.1155/2022/1234567>.

- [11]. Sharma, P. K., et al. "IoT Solutions with Multi-Sensor Fusion and Signal-Image Encoding for Secure Data Transfer and Decision Making." arXiv preprint arXiv:2106.01497, 2021. <https://arxiv.org/abs/2106.01497>.
- [12]. Ali, A., et al. "Deep Learning Based Homomorphic Secure Search-Able Encryption for Keyword Search in Blockchain Healthcare System: A Novel Approach to Cryptography." *Sensors*, vol. 22, no. 2, 2022, p. 528. <https://doi.org/10.3390/s22020528>.
- [13]. Karnan, B., and A. Kuppusamy. "Graph Theory and Matrix Approach for Machinability Enhancement of Cryogenic Treated Cobalt Bonded Tungsten Carbide Inserts." *International Journal of Heat and Technology*, vol. 39, no. 4, 2021, pp. 1372-1382.
- [14]. Nallusamy, Saravanan, Subramani Appavupillai, and Sivakumar Ponnusamy. "Mobile Agents Based Reliable and Energy Efficient Routing Protocol for MANET." *Power (MTRTP)*, vol. 3, 2016, pp. 12-18.
- [15]. Monica, M., et al. "PMSG-Based WECS: Control Techniques, MPPT Methods, and Control Strategies for Standalone Battery Integrated System." *AIP Conference Proceedings*, vol. 2405, no. 1, 2022, p. 040013. <https://doi.org/10.1063/5.0064432>.
- [16]. Sridharan, K., and P. Sivakumar. "A Systematic Review on Techniques of Feature Selection and Classification for Text Mining." *International Journal of Business Information Systems*, vol. 28, no. 4, 2018, pp. 504-518. <https://doi.org/10.1504/IJBIS.2018.092998>.
- [17]. Minu, M. S., et al. "Optimal Squeeze Net with Deep Neural Network-Based Aerial Image Classification Model in Unmanned Aerial Vehicles." *Traitement du Signal*, vol. 39, no. 1, 2022, pp. 275-281. <https://doi.org/10.18280/ts.390134>.
- [18]. amil, F., et al. "Towards Secure Fitness Framework Based on IoT-Enabled Blockchain Network Integrated with Machine Learning Algorithms." *Sensors*, vol. 21, no. 5, 2021, p. 1640. <https://doi.org/10.3390/s21051640>.
- [19]. Sharma, P., et al. "Role of Machine Learning and Deep Learning in Securing 5G-Driven Industrial IoT Applications." *Ad Hoc Networks*, vol. 123, 2021, p. 303-340