Machine Learning Model in Satellite Data Security Analysis using Remote Sensing Network

Gagan Kumar Koduru[1,*], P. Chinnasamy[2], S. Kalaimagal[3], Karri Nagaraju[4], V. Bhaskara Murthy[5], Shivanadhuni Spandana[6], M. Rajesh[7]

[1]Associate Professor, Department of Computer Science and Engineering, MLR Institute of Technology, Hyderabad, India

[2]Associate Professor, Department of Computer Science and Engineering, School of Computing, Kalasalingam Academy of Research and Education, Srivilliputtur, India

[3]Professor, Department of AI & DS, Panimalar Engineering College, Chennai, Tamil Nadu, India

[4]Assistant Professor, Computer Science and Engineering, Vishnu Institute of Technology, Andhrapradesh, India

[5]Professor and HOD, Department of MCA, B V Raju College Vishnupur, Bhimavaram, Hyderabad, India

[6]Assistant Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad-500043, Telangana, India

[7]Department of Computer Science and Engineering, Aarupadai Veedu Institute of Technology, Vinayaka Mission's Research Foundation (DU), Tamilnadu, India

Emails: gagan.koduru@gmail.com; chinnasamyponnusamy@gmail.com; drsivamunikalaimagal@gmail.com; nag2230@gmail.com; murthy.vb@bvrice.edu.in; s.spandana@klh.edu.in; rajesmano@gmail.com

Abstract

Over uncovered and under-covered areas, satellite communication provides the potential for ubiquity, scalability, and service continuity. However, before these benefits may be fully realized, a number of obstacles need to be overcome. Satellite networks present more difficulties than terrestrial networks in terms of spectrum management, energy consumption, network control, resource management, and network security. The goal of this research is to create a novel way to remote sensing network security modelling by utilizing machine-learning techniques to analyses the security of satellite data. In order to provide an intrusion detection technique for the modern network environment, this study considers data from both terrestrial and satellite networks. Here the remote sensing network security analysis is carried out using quantum federated encryption algorithm and data security has been analysis by quantile regression adversarial convolutional neural networks. Experimental analysis has been carried out in terms of data integrity, latency, random accuracy, QoS, AUC. Proposed technique Data integrity of 93%, LATENCY of 95%, QOS of 96%, random accuracy of 98%, AUC of 92%.

Keywords: Satellite data; Federated encryption; Remote sensing network; Machine learning techniques; Adversarial convolutional

1. Introduction

Either imaging satellites are used to create earth observation satellite images and the private sector or government owns these imaging satellites. All these images were obtained through remote sensing technology. Remote Sensing, as it is known, can be defined as the technique of obtaining and processing information about an object, location or phenomena in the environment without a physical presence. This is especially true when the RS data is integrated with other technologies like artificial intelligence; land-use classification is just one of the many fields that has found

DOI: https://doi.org/10.54216/JCIM.170106
Received: February 09, 2025 Revised: May 23, 2025 Accepted: July 01, 2025

enormous application in RS data. With the ever-increasing user demand for quality photographs, Satellite imageries have consequently become immense in size. Correspondingly, the ever-increasing sizes of RS data have facilitated the investigation of numerous complex research problems [1]. Nevertheless, it is often required to utilize more sophisticated RS images with deep learning techniques that have complex architecture and require high computational capabilities. To do this, a large number of researchers utilize deep learning (DL) techniques on cloud computing platforms, which allow them to extract meaningful information and insights. However, because the tools used to handle the data and the public nature of the data processing itself can raise privacy concerns in some situations, data workflows may be affected. In this case, data leakage is possible and data privacy cannot be guaranteed. Cloud computing does, however, still have a number of advantages, including cost savings, scalability, flexibility, and masking architectural complexity. Therefore, the best course of action is to find a way to offset the drawbacks while still reaping the rewards. However, there are also a number of privacy issues that need to be resolved, especially when satellite photos are transferred or stored using open data approaches [2]. Al-Rubaie and Chang give an overview of privacy-preservation deep learning (PPDL) algorithms that can be used to protect individual or company users' privacy. Such work shows that PPDL approaches can be applied to secure sensitive information against unlawful use and unauthorized access, and to reap the benefits of public data analytics without compromising data leaks [3]. On-board Deep Learning (DL) models can evaluate data obtained by the sensors or received by the satellite to automate, adapt, and improve measurements, location, resource management, diagnostics, and communication of the satellite. The proliferation of IoT devices and the increasing prevalence of smart environments have raised concerns about IoT cybersecurity and related fields. When such flaws are exploited, an attacker can covertly update a device's firmware, changing its behavior and leading it to store fabricated data that could subsequently influence the status of a smart environment [4]. The Mirai botnet is one well-known instance of an IoT-specific botnet. Furthermore, hackers have the ability to "brick" Internet of Things devices in order to permanently disable them, steal confidential information from them, or infect them with malware to make them a part of a botnet—a collection of compromised devices launch massive Distributed Denial of Service (DDoS) attacks against Internet. Smart satellites are particularly vulnerable to cyber-attacks due to their extensive broadcast range, regular use in transmitting network traffic, and ability to collect sensory data, all of which might extend the attack's effective range. The primary function of most conventional satellites is to serve as a transmission link, enabling communication to distant or inaccessible sites. However, Internet of Things (IoT) sensors integrated into their design [5] enhance smart satellites.

2. Related works

In order to recognize clouds, some researchers have looked at machine learning and cloud properties. In work [6], Support Vector Machine (SVM) and Back Propagation Neural Network (BP-NN) approach were compared with training set numbers for cloud identification. It was discovered that SVMs outperform BP-NN method when sample size is limited. Author [7] used spectral and spatial data to create a neural network method for cloud detection in Landsat images. In work [8], the Gaussian-RBF kernel, Polynomial, and Linear SVMs were tested, and it was found that the combination of texture and Linear SVM produced a 92.30% correct classification rate in cloud identification. In order to detect clouds on RGB photos, the author [9] employed texture-based SVM classification in addition to color-and line-based removal. While a lot of research is done on feature-based cloud detection classification techniques, most of these algorithms rely on spectral and texture data and do not take advantage of additional aspects like shape and NDVI or combine multiple features in machine learning. In addition to enabling features to work in concert with one another, the integration of ML as well as multi-feature approaches for cloud detection might fully utilize the information contained in remote sensing images. [10] shown how spoofing attacks might target satellite communications, namely the downlink satellite system's information signaling (SIS). A PLA suggestion was put up to use the Doppler frequency shift (DS) to verify the validity of satellites [11] used in-phase and quadrature (IQ) signal levels to acquire the Iridium LEO satellite fingerprints. These satellites can move at speeds of up to 25,000 km/h, which results in unusual attenuation and fading characteristics for their transmissions [12].

3. Proposed satellite data security analysis with remote sensing network security

Figure 1 depicts first n phases of a communication session, which is anticipated to contain 2n−1 phases. A brief summary of the methods used to process satellite data is provided below: Data was taken from an image product that was downloaded. The first step in the processing process is to identify real-world data as follows: The steps involved in this method are extracting photos, locating the study region, identifying the composite band for satellite processing, constructing layers, and identifying the classifiers. For every image captured by every satellite, the overall classification accuracy and statistical outcomes are computed.

DOI: https://doi.org/10.54216/JCIM.170106
Received: February 09, 2025 Revised: May 23, 2025 Accepted: July 01, 2025

- Packet decoder: this module sends the appropriate data to the pre-processing module after receiving raw network traffic packets.
- Pre-processing: this model gets a fraction of network traffic data as well as prepares appropriate normalized feature vectors, which is important for learning-based methods in detection model.
- Classifier system: this module's job is to use the prepared data to create a model that distinguishes between harmful and benign instances.
- Detection and recognition: after any malicious behavior is detected, method can recognize different types of abnormality. This module defines two phases: (i) detects malicious instances as a binary decision issue as well as transmits an alert to a method administrator for making a reaction.

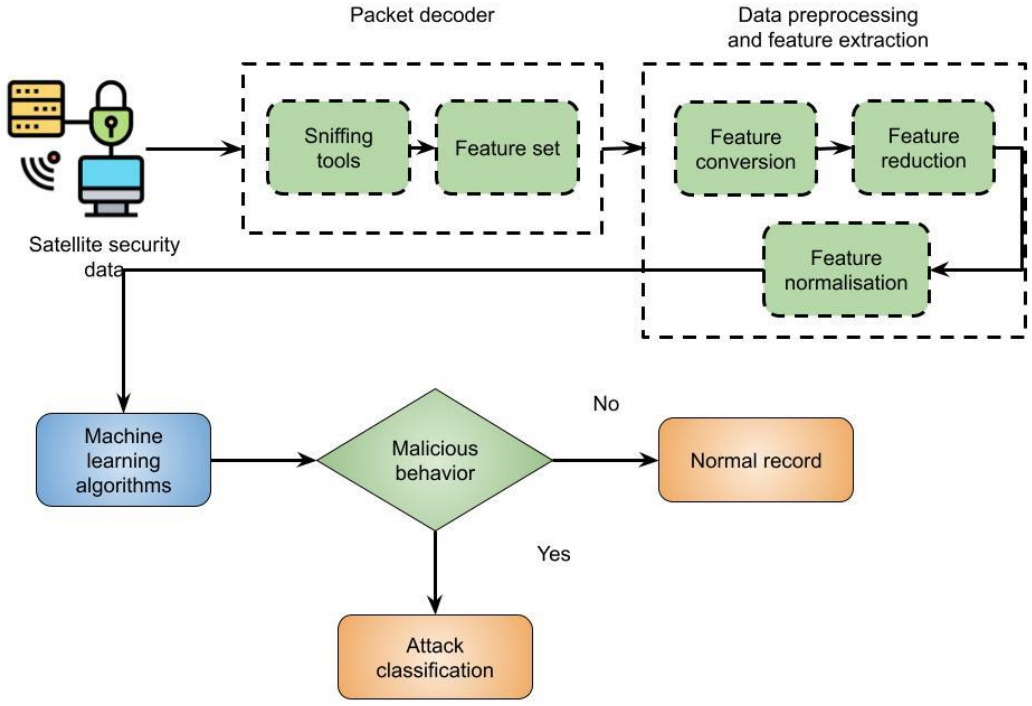


Figure 1. Proposed satellite data security analysis with remote sensing network security

Between March 2014 and May 2016, 102 photographs were obtained for the testing. Every scene's training data is selected at random from the scene itself. To expedite the detecting process, each testing image is a 2000 × 2000 pixel inset of the scene, meaning that clouds do not completely cover the image. Carefully chosen testing insets covering a range of underlying surface environments are included. The examined photos had a correction level of Level 1A, and the GF-1/2 image resolution is 8 meters and 4 meters. Not all images have been resampled.

4. Quantum federated encryption algorithm (QFEA)

We introduce the QFL, an architecture for privacy computing in decentralized data. A server and multiple clients make up the federated learning process. To evaluate the VQA circuit in every training cycle, the local client uses private data and sends model parameters to the server. Either quantum computers or quantum simulators serve as these local customers in this study. The server distributes the output to all local clients after it has combined all of the parameters it has received. Following the receipt of local quantum data DN, each local model Qlocal N, $\forall N \in \{1, 2,...,n\}$, predicts the result. The notation ωlocal N represents the model parameters, and the local prediction of Qlocal N is a set of client N optimal solutions. To aggregate shared parameters, the server is given the input ωlocal N. It then outputs ωshared N to optimize Qlocal N. The following are the federated learning scenario and quantum model. First, QFL allows participants with varying sample sizes to work together to solve same issue. For instance, quantum devices located in various locations resolve quantum chemistry, combinatorial optimization, and classification issues. Second,

DOI: https://doi.org/10.54216/JCIM.170106
Received: February 09, 2025 Revised: May 23, 2025 Accepted: July 01, 2025

every player gets the most recent method from server. Additionally, encrypted method gradients from local data training are transferred to server, which aggregates each user's gradients to update method specifications. To reach convergence, every participant repeats previous stages while updating the local model parameters. At the same time, data is sensitive to privacy and enormous in comparison to number of method specifications. During local training, private information cannot be logged to other devices. In contrast to distributed computing, it has a number of important characteristics. First off, since real-world quantum computing c apability varies amongst clients, non-i.i.d. is satisfied by the training data. Here, we address efficient communication and non-i.i.d. and imbalanced quantum data. Quantum encoding can be implemented in a variety of methods, such as digital and analogue encoding. In this case, digital encoding stores data as qubit strings, while analogue encoding stores data as amplitudes of states. The following is the construction of an N-qubit quantum state required by traditional QML by eqn (1)

$$|\psi\rangle = \sum_{j=1}^{N} c_j |j\rangle \quad (1)$$

where classical input data {cj}N j=1 is normalized to satisfy ΣN j=1|cj | 2 = 1. The widespread application of this encoding technique on quantum hardware raises certain questions, though. Let A be the original image, where A(i, j) ∈ [0, 255] and its size is m × n. A three-digit number represents every pixel in A(i, j). If needed, complete vacancy filling process such that the number is always three digits, like 000, 001, 002,..., 254, 255. S-Box column position, indicated as col, is indexed using first 2 digits of every pixel A(i, j), and index position of rows, indicated as row, is represented by the third digit by eqn (2)

$$\text{column} = [\mathbf{B}(x,y) - \text{reminder}(\mathbf{X}(x,y),20)]/20$$

$$\text{rownumber} \in [0,26] \text{ \& row number} \in \mathbf{Z}^{+}$$

$$\text{rownumber} = \begin{matrix} \text{rownumber} \in [0,25] \& \\ \text{rem}(\mathbf{A}(i,j),10) \\ \text{col} \in [0,9] \& c \end{matrix} \quad (2)$$

By providing any pixel A(i, j), pixel-wise decomposition can be used to determine the matching col and row. Let S = [S (row, col)] be matrix of a single S-Box that has been created. Next, use S(row, col) to search for the row and col index values to begin the index search process. The unique encrypted S-box picture, designated as C1 by eqn (3)

$$\mathbf{C}_1(i,j) = \mathbf{S}(\text{ row , col }) = \mathbf{S}([\mathbf{A}(i,j) - \text{rem}(\mathbf{A}(i,j),10)]/10 + 1, \text{rem}(\mathbf{A}(i,j),10) + 1) \quad (3)$$

(1) System initialization: the method returns the master key and system parameters params after receiving security parameter k as input. The description of ciphertext space C and plaintext space M is one of the system parameters. PKG is the only one who knows the master key; params can be made public; algorithm is executed by PKG. (2) Key extraction: method returns key XSID and secret value xID of ID after receiving parameters and the user's ID as input. The secret value and key are generated by algorithm and can be executed either using the user ID or PKG. (3) Public key extraction: algorithm outputs the user ID's public key PID after receiving parameters as well as secret value xID as input. User ID is used to run the algorithm, public key PID that is produced is released. (4) Encryption: parameters, plaintext M ∈ M, user ID's public key PID are entered into the method.

5. Quantile regression adversarial convolutional neural networks (QRACNN) based data security analysis

we can write $\sigma(x_{it}, z_{it}, \delta_i) = a_0 + a_x x_{it} + a_z z_{it} + a_i \delta_i$ Finally, we assume the population model that describes their relationship is given as eqn (4)

$$y_i = b_0 + b_x x_{it} + b_z z_{it} + \delta_i + \sigma(x_{it}, z_{it}, \delta_i) v_{it} \quad (4)$$

Finding the impact of x on the distribution of y is the main objective given a p-dimensional covariate vector x = (x1,..., xp) T ∈ R p with x1 > 1. There is a univariate response variable, y ∈ R. Given x, Fy|x(·) is the conditional distribution function of y. F −1 y|x (τ), for 0 < τ < 1, is the conditional quantile functions of y given x that adequately reflect the dependence between y and x. We consider a linear quantile regression method at a given τ ∈ (0, 1), where the τ-th conditional quantile function is given by eqn (5).

$$F_{y|x}^{-1}(\tau) = \langle \boldsymbol{x}, \boldsymbol{\beta}^*(\tau) \rangle \quad (5)$$

where the genuine quantile regression coefficient is denoted by T ∈ R p and β ∗ (τ) = (β ∗ 1 (τ),..., β∗ p (τ)). Consider a random sample from (y, x) = {(yi, xi)} n i=1. The typical estimation for quantile regression is given by eqn (6)

$$\widehat{\boldsymbol{\beta}}(\tau) \in \min_{\boldsymbol{\beta} \in \mathbb{R}^p} \hat{Q}(\boldsymbol{\beta}) = \min_{\boldsymbol{\beta} \in \mathbb{R}^p} \frac{1}{n} \sum_{i=1}^{n} \rho_\tau(y_i - \langle \boldsymbol{x}_i, \boldsymbol{\beta} \rangle) \quad (6)$$

DOI: https://doi.org/10.54216/JCIM.170106
Received: February 09, 2025 Revised: May 23, 2025 Accepted: July 01, 2025

The description of the τ-quantile loss function, often known as the check function, is ρτ(u) = u{τ − 1(u < 0)}. A thorough investigation has been conducted into the statistical aspects of βb(τ). Let the quantile loss function for the population be Q(β) = E{Qb(β)}. In moderate conditions, Q(·) is twice differentiable and strongly convex in the neighbourhood of β ∗, and it has the following Hessian matrix: With ε = y − hx, β ∗ (τ)i being random noise, and fε|x(·) being the conditional density of ε given x, J:= ∇ 2Q(β ∗) = E{fε|x(0)xT }. However, the empirical quantile loss Qb(·) exhibits a single point of concentration for its "curvature energy" and will not be differentiable at β ∗. Compared to other often used loss functions, like the squared or logistic loss, which are at least locally highly convex, this is significantly different. Not only does the no smoothness condition provide difficulties for theoretical analysis, but it also hinders the efficiency of gradient-based optimization techniques. It suggested smoothing the check function ρτ(·) is given by eqn (7)

$$\ell_h^{\text{Horo}}(u) = u\{\tau - \mathcal{G}(-u/h)\} \qquad (7)$$

where h > 0 is a smoothing parameter/bandwidth and G(·) is a smooth function with values in the range of 0 to 1. Conversely, the population parameter β ∗ fulfills moment condition according to first-order condition is given by eqn (8)

$$\nabla Q(\boldsymbol{\beta}^*) = \mathbb{B}[\{1(y < \boldsymbol{x}^{\mathrm{T}}\boldsymbol{\beta}) - \tau\}\boldsymbol{x}]|_{\boldsymbol{\beta}=\boldsymbol{\beta}^*} = \mathbf{0}. \qquad (8)$$

This characteristic serves as the driving force behind a smoothed estimating equation (SEE) estimator, which is the smoothed moment condition's solution is given by

$$\tfrac{1}{n}\textstyle\sum_{i=1}^{n} [\mathcal{G}\{(\langle \boldsymbol{x}_i, \boldsymbol{\beta}\rangle - y_i)/h\} - \tau]\boldsymbol{x}_i = \mathbf{0}. \qquad (9)$$

The previously described SEE estimator can be formulated similarly from an M-estimation perspective as a minimizer of empirical smoothed loss function is given by eqn (10)

$$\hat{Q}_h(\boldsymbol{\beta}) = \tfrac{1}{n}\textstyle\sum_{i=1}^{n} \ell_h(y_i - \langle \boldsymbol{x}_i, \boldsymbol{\beta}\rangle) \text{ with } \ell_h(u) = (\rho_\tau * K_h)(u) = \int_{-\infty}^{\infty} \rho_\tau(v) K_h(v-u)\mathrm{d}v \qquad (10)$$

where the convolution operator is indicated by ∗. Conquer estimation that follows is provided by eqn (11)

$$\widehat{\boldsymbol{\beta}}_h = \widehat{\boldsymbol{\beta}}_h(\tau) \in \underset{\boldsymbol{\beta}\in\mathbb{R}^p}{\operatorname{argmin}} \hat{Q}_h(\boldsymbol{\beta}). \qquad (11)$$

As we will see later, since quantile level τ is predetermined and fixed, optimal bandwidth selection should adjust to sample size n and dimension p. Therefore, it will be assumed that βbh and Qbh(·) rely on τ without being shown. \ This clarifies the connection between the conquer and SEE strategies. The computing efficiency of first-order gradient-based techniques is improved by the smoothness and convexity of Qbh(·), particularly for large-scale smoothed quantile regressions. Conversely, a domain discriminator network aids in determining if the features that are extracted are part of the target domain or the source domain. It uses a binary classification strategy to train a logistic regress or that maps features in the [0,1] range. Reverse gradient layers are cleverly used to trick the feature extractor into believing that the source features closely resemble the target maps. As a result, a classifier can use existing information to classify unlabelled defects in the target domain. Lastly, optimization goal of adversarial domain network is shown as a binary cross entropy loss as follows by eqn (12)

$$\mathcal{L}_d(x^s, x^t) = -\mathbb{E}_{x'\in\mathcal{D}_x}\left[\log D\left(G(x^s)\right)\right] - \mathbb{E}_{x'\in\mathcal{D}_t}\left[\log\left(1 - D\left(G(x^t)\right)\right)\right] \qquad (12)$$

where D(.) takes 0 or 1 as input and G(.) is the feature extractor. An adjacency matrix is described by multiplying feature vector and its transpose, as seen below. Every feature vector is represented as a node whose feature vectors originate from output of a dense layer by eqn (13)

$$X = \text{CNN}(\text{ InputData })$$

$$\hat{X} = FC1(X)$$

$$A = \mathcal{N}\left(\hat{X}\hat{X}^T\right) \qquad (13)$$

where the normalizing function is denoted by N(). Making the adjacency matrix sparse will help you save money on computing. K(.) thus returns k-largest members of supplied adjacency matrix, as shown below in (14).

$$\hat{A} = \text{Top} - K(A) \qquad (14)$$

DOI: https://doi.org/10.54216/JCIM.170106
Received: February 09, 2025 Revised: May 23, 2025 Accepted: July 01, 2025

The following is a definition for the formula (15)

$$X_j^l = f\left(\sum_{i\in M_j} X_i^{l-1} \cdot \omega_{ij}^l + b_j^l\right) \quad (15)$$

where bl j stands for bias, f(·) for AF, Xl j for the jth element of the lth layer, Xl1 i for element, and Xl ij for weight matrix. Mj stands for the (l-1)th layer's jth convolution area. The most widely used ReLU AF is provided by equation (16).

$$f(\mathrm{x}) = \max(0, x) \quad (16)$$

In order to achieve "dimension reduction of feature maps and maintain the invariance of characteristic scales," pooling layers frequently come after convolution layers. Max Pooling (MXP), Mean Pooling (MNP), Stochastic Pooling (SP) are the three most used pooling techniques. Pooling layers are often solely used to perform dimension reduction without updating weights.

Fully-connected layers (FC): Following the alternating propagation of input images by convolution and pooling conduction, the FC net is utilised to classify the retrieved information and features. 1-D feature vectors are weighted sums, and this is the input data for FC layers is given by eqn (17)

$$y^n = f(w^n x^{n-1} + b^n) \quad (17)$$

where yn is the entire connection layer's output, xn1 is the 1-D feature vectors, xn stands for weight coefficients, bn for biases. Additionally, n is sequence number of net layers. Softmax is most widely utilized AF f (·).

6. Experimental analysis

During flight, the Bebop 2 records its attitude angles and GPS locations for later confirmation. Bebop 2 Software Development Kit (SDK) 2 is used to interface with the ROS Airborne autonomous driver1. For UAV communication, WiFi frequencies of 2.4 and 5 GHz are used. This ROS Kinetic setup is running on Ubuntu 16.04. The ground control station's Nvidia 940MX and Core Intel Core i5-7500U MB central processing unit are necessary for the intricate mathematical computations required by the detection method.

Description of the dataset: In order to assess crop health, Sentinel-2 photos were processed using the following vegetation indices: Normalized Difference Vegetation Index, Green Normalized Difference Vegetation Index 2, Modified Soil Adjusted Vegetation Index, and Soil Adjusted Vegetation Index.

Three components make up the GNSS Dataset: a GNSS receiver located on the fifth level of Yunnan University's Science Hall recorded the data. HackRF One uses spoofing signals and commercial jammers use suppression jamming to assault the receiver. The provided datasets will be of interest to research teams studying GNSS security, monitoring, anti-jamming, and anti-spoofing technologies.

ESA Satellite Orbit DecAy (SODA) Service: Included in the data are the study results from the 116 interplanetary coronal mass ejections (ICMEs) that were analysed to develop the satellite orbit DecAy forecasting service (SODA), available via the Expert Service Centre Ionosphere of ESA Space Service Network.

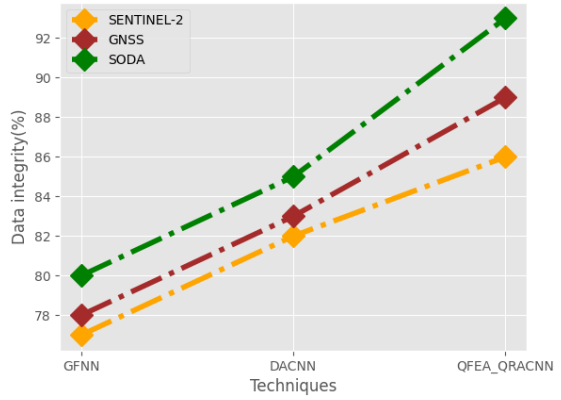
Table 1: Comparative analysis based various satellite data

Dataset	Techniques	Data integrity	Latency	QOS	Random accuracy	AUC
SENTINEL-2	**GFNN**	77	74	72	76	75
	DACNN	82	78	75	81	79
	QFEA_QRACNN	86	84	83	85	86
GNSS	**GFNN**	78	79	74	84	73

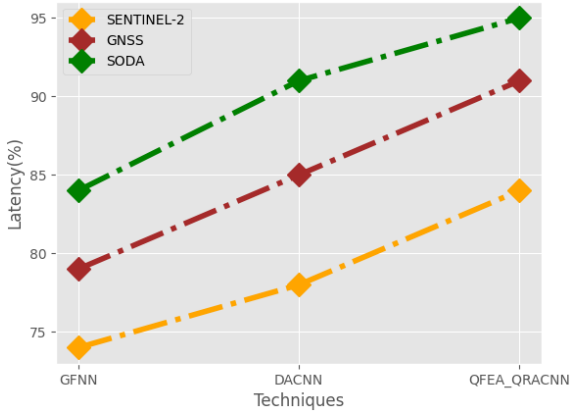
DOI: https://doi.org/10.54216/JCIM.170106
Received: February 09, 2025 Revised: May 23, 2025 Accepted: July 01, 2025

	DACNN	83	85	78	88	77
	QFEA_QRACNN	89	91	84	93	87
SODA	**GFNN**	80	84	87	86	82
	DACNN	85	91	90	90	87
	QFEA_QRACNN	93	95	96	98	92

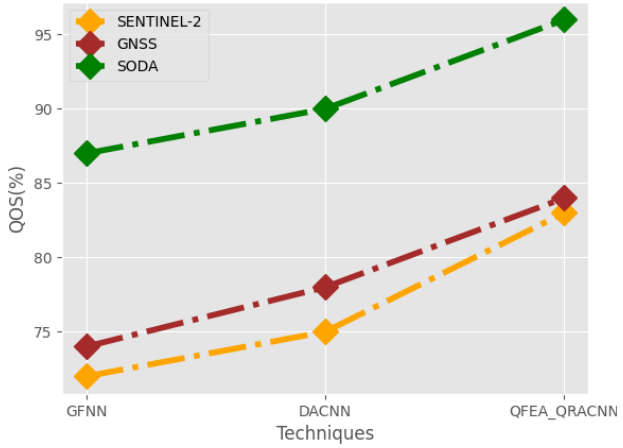
The table-1 shows comparative analysis based on various satellite data. Dataset analyzed are SENTINEL-2, GNSS, and SODA dataset. The parameters analyzed are Data integrity, LATENCY, QOS, random accuracy, AUC.



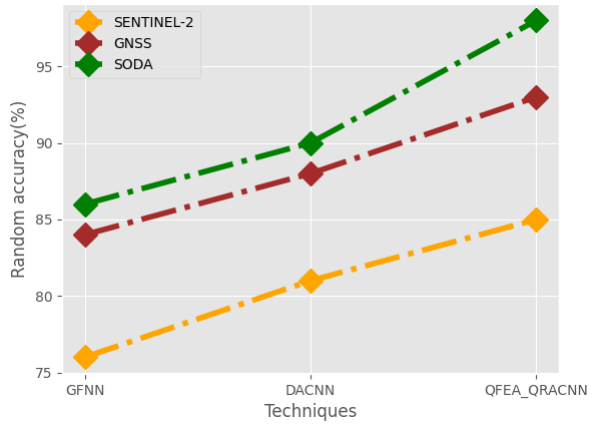
(a) DATA INTEGRITY



(b) LATENCY

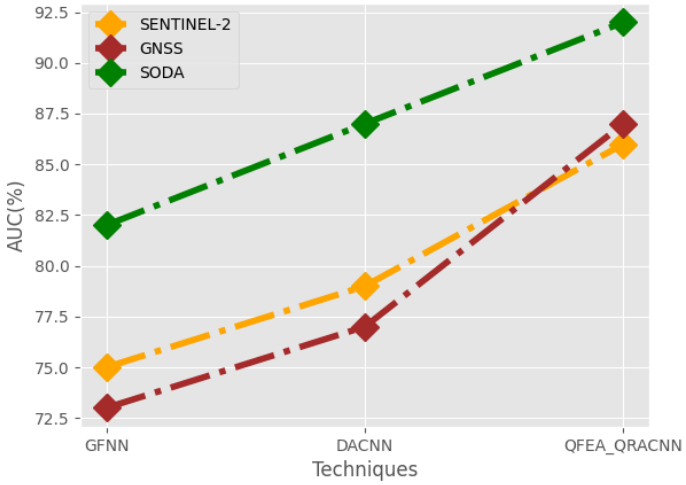


(c)QOS



(d) Random accuracy

DOI: https://doi.org/10.54216/JCIM.170106
Received: February 09, 2025 Revised: May 23, 2025 Accepted: July 01, 2025



(e) AUC

Figure 2. Comparative analysis for SENTINEL-2 dataset in terms of (a) Data integrity, (b) LATENCY, (c) QOS, (d) random accuracy, (e) AUC

Figure-2 (a)- (e) shows comparative analysis for SENTINEL-2 dataset. Proposed technique Data integrity of 86%, LATENCY 84%, QOS 83%, random accuracy 85%, AUC 86%; GFNN attained Data integrity of 77%, LATENCY of 74%, QOS of 72%, random accuracy of 76%, AUC of 75%, DACNN attained Data integrity of 82%, LATENCY of 78%, QOS of 75%, random accuracy of 81%, AUC of 79%. For GNSS dataset. The proposed technique attained Data integrity of 89%, LATENCY of 91%, QOSof 84%, random accuracy of 93%, AUC of 87%; GFNN attained Data integrity of 78%, LATENCY of 79%, QOSof 74%, random accuracy of 84%, AUC of 73%, DACNN attained Data integrity of 83%, LATENCY of 85%, QOSof 78%, random accuracy of 88%, AUC of 77%. Proposed technique Data integrity 93%, LATENCY 95%, QOS of 96%, random accuracy of 98%, AUC of 92%; GFNN attained Data integrity of 80%, LATENCY of 84%, QOS of 87%, random accuracy of 86%, AUC of 82%, DACNN attained Data integrity of 85%, LATENCY of 91%, QOS of 90%, random accuracy of 90%, AUC of 87% for SODA dataset.

7. Conclusion

New Safety Analysis on Satellite Data with Machine Learning for the Modelling of Remote Sensing Network Security is the main objective of this work. A contemporary network domain is given in this paper, along with an intrusion detection approach that employs input from both ground and satellite networks. As such, the data security has been evaluated using quantile regression adversarial convolutional-neural-networks, while the remote sensing network security evaluation has utilized quantum federated encryption algorithm. This paper also provides a dependable and extensive deep learning based intrusion detection system for both satellite and terrestrial network environments. In order to combat attacks in the contemporary network environment, there is a greater need than ever for an intuitive cybersecurity solution due to rise in network intrusion attacks. The results show high levels of efficiency for both the plain and encrypted data. Our model was the best by a small margin, even though all of the models did well overall in the classification of satellite photos. A few possible extensions might be considered for future study, even if our proposed PHE encryption method is efficient and accurate in classifying data and sensitive information in satellite photographs is maintained.

References

[1] A. T. Azar, E. Shehab, A. M. Mattar, I. A. Hameed, and S. A. Elsaid, "Deep learning based hybrid intrusion detection systems to protect satellite networks," *Journal of Network and Systems Management*, vol. 31, no. 4, pp. 82, 2023.

[2] R. Uddin and S. A. Kumar, "SDN-based federated learning approach for satellite-IoT framework to enhance data security and privacy in space communication," *IEEE Journal of Radio Frequency Identification*, vol. 7, pp. 424-440, 2023.

DOI: https://doi.org/10.54216/JCIM.170106
Received: February 09, 2025 Revised: May 23, 2025 Accepted: July 01, 2025

[3] J. J. Sousa, J. Lin, Q. Wang, G. Liu, J. Fan, S. Bai, and L. P. Reis, "Using machine learning and satellite data from multiple sources to analyze mining, water management, and preservation of cultural heritage," *Geo-spatial Information Science*, vol. 27, no. 3, pp. 552-571, 2024.

[4] S. Salim, N. Moustafa, M. Hassanian, D. Ormod, and J. Slay, "Deep federated learning-based threat detection model for extreme satellite communications," *IEEE Internet of Things Journal*, 2023.

[5] A. Bhattacharyya, S. M. Nambiar, R. Ojha, A. Gyaneshwar, U. Chadha, and K. Srinivasan, "Machine Learning and Deep Learning powered satellite communications: Enabling technologies, applications, open challenges, and future research directions," *International Journal of Satellite Communications and Networking*, vol. 41, no. 6, pp. 539-588, 2023.

[6] R. Kumar and S. Arnon, "Improving physical layer security of ground stations against geo satellite spoofing attacks," in *International Symposium on Cyber Security, Cryptology, and Machine Learning*, Cham, Switzerland, Jun. 2023, pp. 458-470.

[7] F. Bao, K. Huang, and S. Wu, "The retrieval of aerosol optical properties based on a random forest machine learning approach: Exploration of geostationary satellite images," *Remote Sensing of Environment*, vol. 286, p. 113426, 2023.

[8] R. Fu, X. Ren, Y. Li, Y. Wu, H. Sun, and M. A. Al-Absi, "Machine-learning-based UAV-assisted agricultural information security architecture and intrusion detection," *IEEE Internet of Things Journal*, vol. 10, no. 21, pp. 18589-18598, 2023.

[9] R. Manoharan, "Improving Security and Performance in Chaotic Optical Communication via Real-Time Pilot Signal Processing Techniques," *IETE Journal of Research*, pp. 1-9, 2025.

[10] M. Rajesh, S. Ramachandran, K. Vengatesan, S. S. Dhanabalan, and S. K. Nataraj, "Federated Learning for Personalized Recommendation in Securing Power Traces in Smart Grid Systems," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 88-95, Feb. 2024, doi: 10.1109/TCE.2024.3368087.

[11] A. Goel, A. K. Goel, and A. Kumar, "The role of artificial neural network and machine learning in utilizing spatial information," *Spatial Information Research*, vol. 31, no. 3, pp. 275-285, 2023.

[12] W. Jiang, H. Han, Y. Zhang, and J. Mu, "Federated split learning for sequential data in satellite–terrestrial integrated networks," *Information Fusion*, vol. 103, p. 102141, 2024.

[13] O. Hall, F. Dompae, I. Wahab, and F. M. Dzanku, "A review of machine learning and satellite imagery for poverty prediction: Implications for development research and applications," *Journal of International Development*, vol. 35, no. 7, pp. 1753-1768, 2023.

[14] A. Sebastianelli, F. Serva, A. Ceschini, Q. Paletta, M. Panella, and B. Le Saux, "Machine learning forecast of surface solar irradiance from meteo satellite data," *Remote Sensing of Environment*, vol. 315, p. 114431, 2024.

DOI: https://doi.org/10.54216/JCIM.170106
Received: February 09, 2025 Revised: May 23, 2025 Accepted: July 01, 2025