I.J. Wireless and Microwave Technologies, **2025, 6, 1-13**
Published Online on December 8, 2025 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2025.06.01

Anomaly Detection in IoT Based Satellite Networks: NidaDeepMix

Nida Canpolat*
Department of Digital Forensics Engineering, Technology Faculty, Firat University, Elazig, Turkey
E-mail: 231144110@firat.edu.tr
ORCID iD: https://orcid.org/0000-0002-5262-1509
*Corresponding Author

Sengul Dogan
Department of Digital Forensics Engineering, Technology Faculty, Firat University, Elazig, Turkey
E-mail: sdogan@firat.edu.tr
ORCID iD: https://orcid.org/0000-0001-9677-5684

Mehmet Karakose
Department of Computer Engineering, Firat University, Elazig, Turkey
E-mail: mkarakose@firat.edu.tr
ORCID iD: https://orcid.org/0000-0002-3276-3788

Turker Tuncer
Department of Digital Forensics Engineering, Technology Faculty, Firat University, Elazig, Turkey
E-mail: turkertuncer@firat.edu.tr
ORCID iD: https://orcid.org/0000-0002-5126-6445

Musa Yenilmez
Department of Computer Engineering, Firat University, Elazig, Turkey
E-mail: myenilmez@firat.edu.tr
ORCID iD: https://orcid.org/0009-0006-1722-3050

Received: 01 November, 2024; Revised: 20 March, 2025; Accepted: 26 August, 2025; Published: 08 December, 2025

Abstract: IOT based satellite networks are one of the modern cyber attack topics. This technology has important application areas such as data collection, monitoring and control without the need for close access. Especially the increasing use of IOT devices and their recent integration with satellite networks have made these devices the target of attacks. The fact that IOT devices have more than one type and require low processing power makes them vulnerable to attacks. The use of IOT devices together with satellite networks increases the complexity of this situation and the size of cyber attacks. This situation has made it necessary to increase the studies on preventing and detecting cyber attacks on IOT based networks. For this purpose, in this article, we propose a new deep learning architecture (NidaDeepMix) that provides high accuracy in order to detect cyber attacks on IOT based satellite networks. The designed layer structure and parameters of the NidaDeepMix architecture are adjusted to effectively cope with complex and difficult situations. The NidaDeepMix architecture has been tested on two separate comprehensive datasets, CSE-CIC-IDS-2018 and BCCC-CIRA-CIC-DoHBrw-2020. As a result of the training, a serious accuracy rate of %99.99 was achieved for the CSE-CIC-IDS-2018 dataset and %99.98 for the BCCC-CIRA-CIC-DoHBrw-2020 dataset. Considering these high accuracy rates, it has been demonstrated that the proposed architecture is quite effective in classifying attacks. These rates obtained on different datasets reveal the generalization success of the model. At the same time the model has also addressed the issue of cyber attacks on IOT based satellite networks with an innovative approach. In this context, a new and effective architecture has been provided to the literature for detecting attacks on IOT based satellite networks. It is envisaged that the proposed method NidaDeepMix will be an important reference model in important issues such as cyber attacks and anomaly detection in the future.

Index Terms: Network Security, Satellite Security, Deep Learning, Cyber Security, Neural Network

1. Introduction

1.1 Background

Today, IOT technology has developed rapidly and has begun to be used in many areas. With this development it has provided convenience and innovation even in daily life. Satellite networks, which are mostly IOT based networks, are one of the important structures that provide innovation and convenience [1-2]. IOT based satellite networks are an indispensable part of communication, data collection and transfer [3-5]. These networks take on important tasks [6-9]. One of these important tasks is communication. Services such as internet are provided with satellite networks. Communication can be provided with this technology with remote or inaccessible regions. On the other hand, services such as location determination and tracking can be provided with some types of satellites. These types of services are generally used in sectors such as transportation, maritime and aviation. Another important task of satellite networks is defense and security [10-11]. They can perform many important tasks such as intelligence acquisition, discovery, military communication, data transfer and early warning with satellite networks [12-14]. In addition emergency management can be provided with satellite networks [15-16]. Disaster management search and rescue operations and emergency aid services can be provided quickly with satellite networks. In this context anomalies in these networks should be detected as early as possible in order to prevent disruption of important tasks such as communication services, defense and security services, navigation services and emergency management services that can be performed with satellite networks.

Attacks on IOT based satellite networks can cause serious difficulties. As a result of the attacks, there may be a service interruption. This negatively affects almost all businesses that communicate with satellite networks. On the other hand, due to attacks on networks, situations such as privacy violations and data security disruptions may be encountered. As a result of the attack commercial, military and sensitive information may fall into the hands of unwanted people. In addition, service interruptions or data privacy resulting from attacks can cause financial losses. When all these difficulties come together, it emphasizes why it is important to ensure security in satellite networks and to detect anomalies in the network.

1.2 Background

Attacks on satellite networks should be detected as early as possible because they seriously endanger data privacy and security, service interruptions and satellite network performance. Due to the scale and heterogeneous structure of the satellite network, anomaly detection systems used today may be weak. Therefore, different and effective solutions should be developed for anomalies in IOT based networks. These methods should have high discrimination features for advanced and complex network models. In this respect there are deficiencies in the literature. These gaps in the literature should be closed regarding satellite network security, which is of great importance both socially and economically. Strong and effective methods should be developed for different data sets. In this study an original and fast model called NidaDeepMix is proposed to cope with all these difficulties. This model is a multi layer deep learning model designed to detect attacks on IOT based satellite networks. The model contains many powerful layers primarily CNN, LSTM, and Attention layers. The combination of these layers allows for better discrimination of complex and difficult attack types. In order to demonstrate the adequacy level of the created model, it was tested on two separate network data sets (CSE-CIC-IDS-2018 and BCCC-CIRA-CIC-DoHBrw-2020). As a result of the test performance metrics were calculated. The low FP (False Positive) and FN (False Negative) rates given by the model proved the robustness of the model. The recommended workflow for detecting anomalies in IOT based satellite networks is as given in Figure 1.

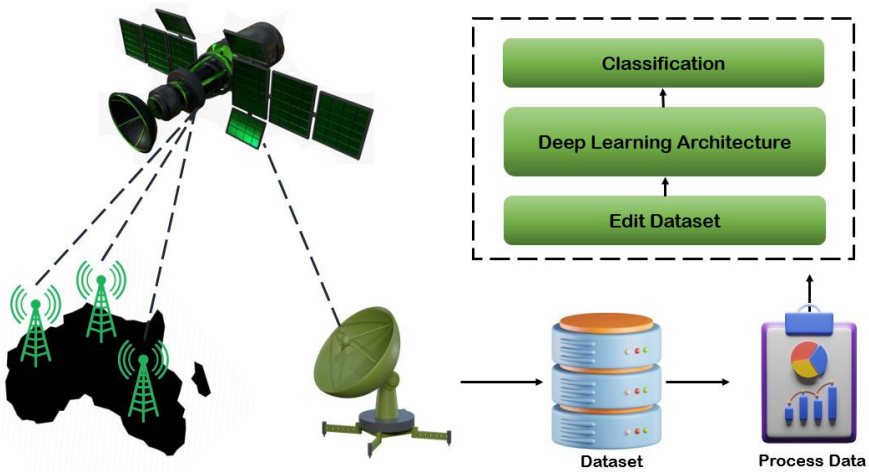

Fig. 1. Recommended detection workflow

1.3 Innovation and Contributions

The contributions and innovations obtained with this study are listed as follows.

- A new multi layer deep learning model (NidaDeepMix) is presented to detect anomalies in IOT based satellite networks.
- The proposed model is designed to provide high performance on different data sets thanks to its different layers.
- The data sets used were tested with both our proposed model and popular deep learning methods, and training times were recorded. As a result of the records it was seen that our model was the fastest model that gave the highest results.
- A different approach was presented to detect anomalies in IOT based satellite networks, which is one of the important problems of today.

2. Literature Review

Studies on detecting anomalies in IoT based devices and IoT based satellite networks have gained interest over the years. Studies in the literature on this subject have aimed to cope with this problem by proposing different methods and models. In 2019, Inayat et al. [17] analyzed learning based methods for cyber attack detection in IoT based systems. This study focused on the process after an attack occurred and considered multiple attack types. In 2022, a federated deep learning type called DFSat was proposed by Moustafa et al. [18]. In this study it was aimed to detect cyber attacks on IoT based satellite networks and the method was tested on two separate datasets and %99.66 accuracy was obtained. In 2022, Koroniotis et al. proposed a forensic framework for smart satellite network security [19]. They used deep learning and machine learning methods while presenting the forensic framework. In 2023, deep neural network architectures such as CNN and LSTM were tested on the CIC-IDS 2017 dataset to detect attacks in IOT systems by Jose et al. [20]. In 2019, a CNN based approach was proposed by Zhang et al. to detect anomalies in the network [21]. The model was tested on the NSL-KDD dataset and an accuracy of %83.31 was obtained. In 2023, Uddin et al. presented a federated learning based distributed approach in the SDN environment to prevent violations in satellite networks [22]. The OpenMined based federated learning method used achieved an accuracy of %79.47. In 2023, a hybrid model was proposed by Gazi et al. to detect attacks on networks [23]. The hybrid architecture was presented under the name HDLNIDS and a convolutional neural network was used to create the model. The architecture was tested on the CICIDS-2018 dataset and an accuracy value of %98.90 was obtained. In 2022, a distributed detection system for detecting DDoS Attacks on satellite internets was presented by Guo et al. [24].

2.1 Literature Gaps

The literature review includes some of the studies conducted to detect anomalies in IOT based devices and IOT based satellite networks. In the light of this literature review, it can be concluded that the number of studies conducted to detect anomalies in IOT based satellite networks is insufficient. Because most of the studies conducted are studies conducted for the security of IOT devices in general. The number of studies conducted directly on IOT based satellite networks is quite limited. In this respect there are deficiencies in the literature both in terms of studies and methods. Since the methods used are generally comparisons of deep learning or machine learning types, the number of studies that create a hybrid model is very few. At the same time, the studies conducted have generally been tested on a single data set. In this context, the number of studies that work with different data sets and generalize the research results is limited. The NidaDeepMix architecture that we proposed in this study has presented a new method to the literature. At the same time the fact that it has been tested on two different comprehensive data sets generalizes the performance of the proposed model. While existing studies have explored individual deep learning models, there is a clear gap for a dedicated, hybrid architecture like NidaDeepMix that is specifically designed and tested for the unique anomaly detection requirements of IoT-based satellite networks.

3. Datasets

While the datasets used in this project capture general network attacks, the threat profiles they contain are representative of threat profiles targeting communication links and data flows in IoT satellite networks. Therefore, two different network datasets were used in this project.

3.1 CSE-CIC-IDS-2018

Two separate datasets were used to test the proposed NidaDeepMix architecture. The first of these is the CSE-CIC-IDS-2018 dataset [25]. The CSE-CIC-IDS-2018 dataset was created as a result of the cooperation between the Communications Security Establishment (CSE) and the Canadian Institute for Cybersecurity (CIC) organizations in order to obtain a realistic cyber defense dataset and is updated every year. Only one data file in the downloaded dataset file was used for this study. The dataset used contains a total of 500.000 data (213.898 normal, 286.102 cyber attacked). In this respect the dataset is a very large dataset to detect cyber attacks on IOT based satellite networks and anomalies in the network.

Some figures and graphs were created to better understand the dataset and its features. In order to examine the feature distribution in the dataset and to perform density analysis, the histogram containing the first 25 features of the dataset is shown in Figure 2. With the histograms shown in Figure 2, information about the data distribution can be obtained and possible outliers can be examined. In addition it helps in how to organize and scale the data before the data preprocessing stage.

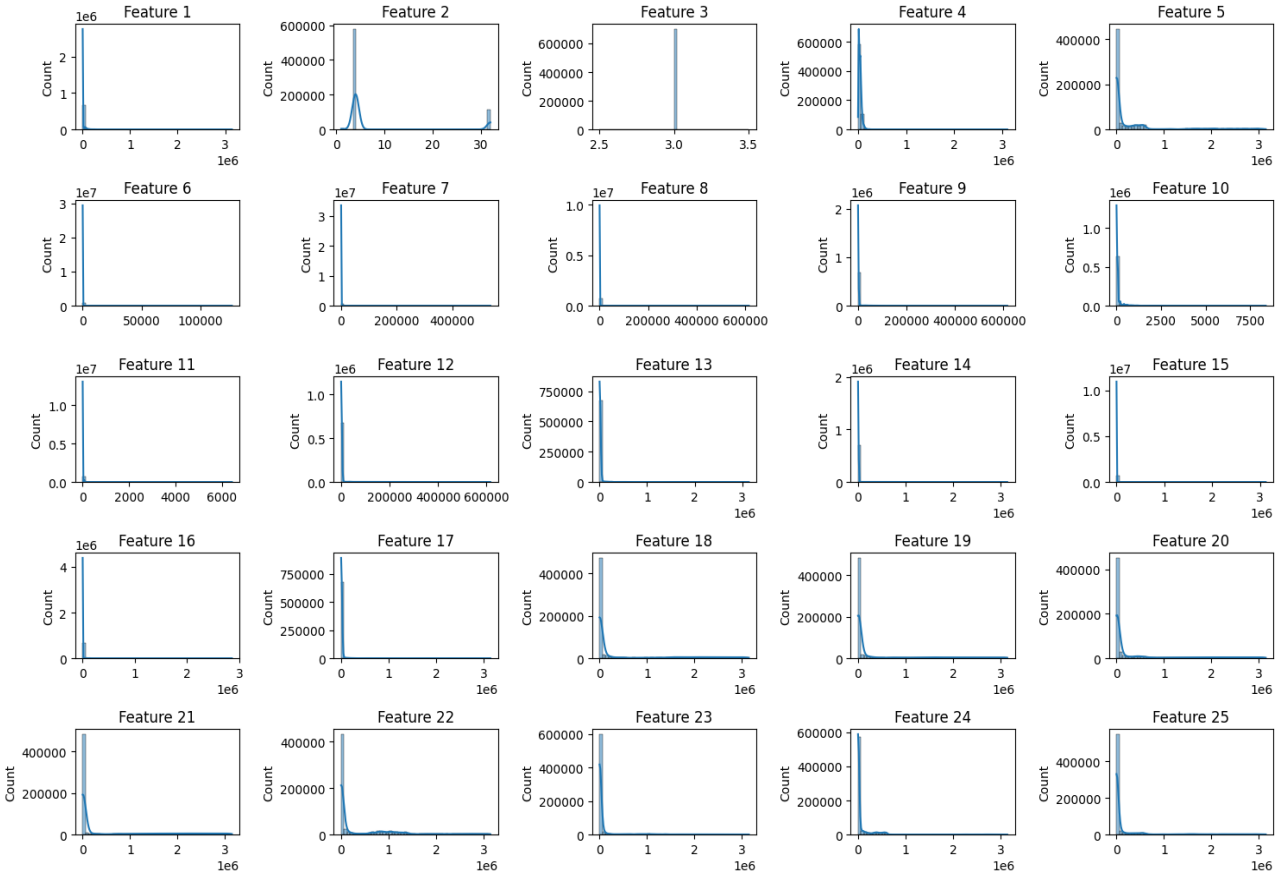

Fig. 2. First 25 features of CSE-CIC-IDS-2018 dataset

To analyze the structure of the CSE-CIC-IDS-2018 dataset, the 2D visualization form can be used with PCA. For this, the data is first converted to a numerical form. Then the features in the dataset are visualized on a two dimensional plane with PCA. In this way, the feature distribution of the data according to the classes is expressed more clearly. This figure plays an explanatory role especially for text based data analysis. The 2D visualization form of the CSE-CIC-IDS-2018 dataset with PCA is as shown in Figure 3.

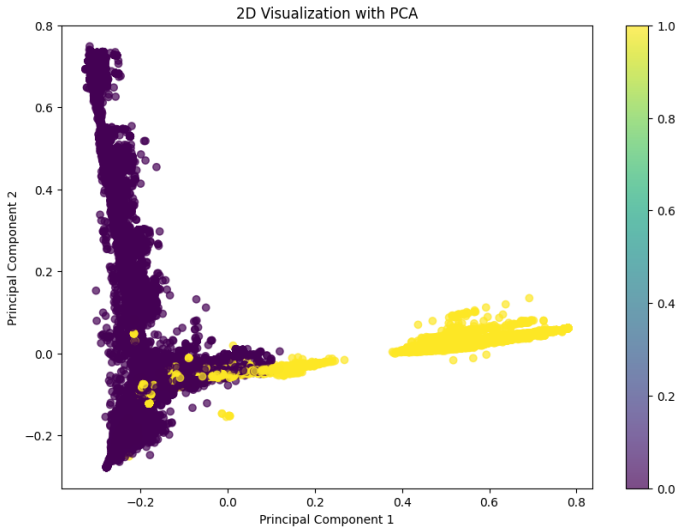

Fig. 3. 2D visualization of CSE-CIC-IDS-2018 dataset with PCA

3.2 BCCC-CIRA-CIC-DOHBRW-2020

Another dataset used to test the proposed NidaDeepMix architecture is the BCCC-CIRA-CIC-DoHBrw-2020 dataset. The BCCC-CIRA-CIC-DoHBrw-2020 dataset is a cybersecurity dataset created by the University of Fredericton New Brunswick. It was created to eliminate the imbalances in the CIRA-CIC-DoHBrw-2020 dataset. The dataset used in this study contains 400.000 data (199.903 normal, 200.097 cyber attacked).

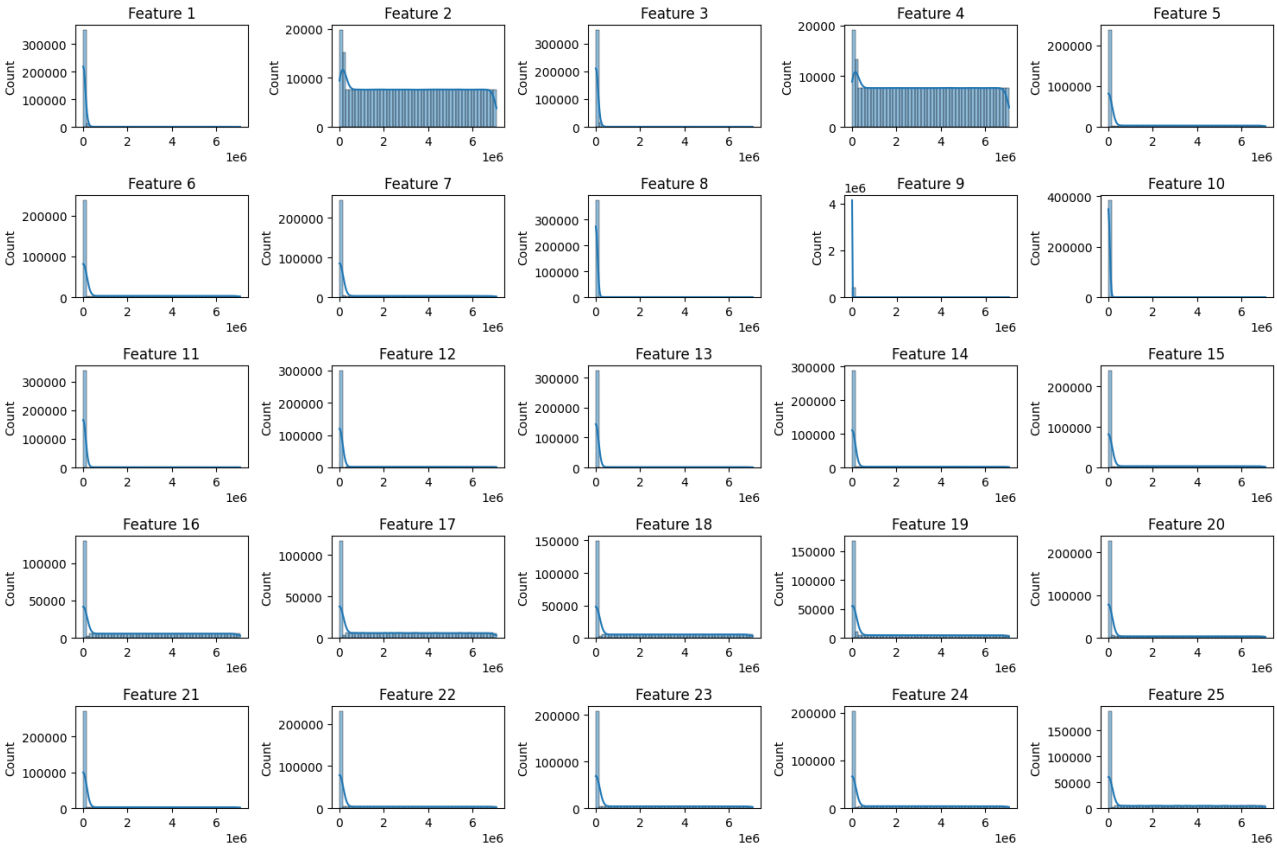

Fig. 4. First 25 features of BCCC-CIRA-CIC-DoHBrw-2020 dataset

Some figures and graphs have been created to better understand the BCCC-CIRA-CIC-DoHBrw-2020 dataset and its features. In order to examine the feature distribution in the dataset and to perform density analysis, the histogram containing the first 25 features of the dataset is shown in Figure 4. With the histograms shown in Figure 4, information about the data distribution can be obtained and possible outlier data can be examined. In addition it helps in how to organize and scale the data before the data preprocessing stage.

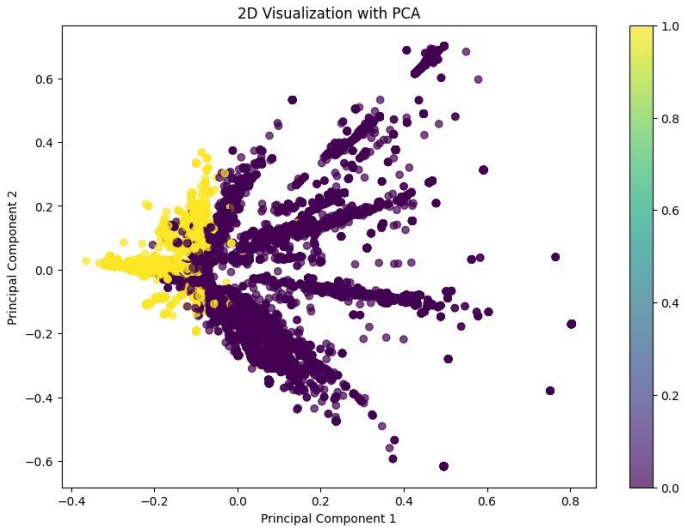

Fig. 5. Visualization of BCCC-CIRA-CIC-DoHBrw-2020 dataset with PCA

To analyze the structure of the BCCC-CIRA-CIC-DoHBrw-2020 dataset, its 2D visualization with PCA can be used. For this the data is first converted to numerical form. Then the features in the dataset are visualized on a two dimensional plane with PCA. In this way the feature distribution of the data according to classes is expressed more clearly. This figure plays an explanatory role, especially for text-based data analysis. The 2D visualization of the CSE-CIC-IDS-2018 dataset with PCA is as shown in Figure 5.

4. Proposed Method

In this study we present an architecture called NidaDeepMix to detect anomalies in IOT based satellite networks (Figure 6). NidaDeepMix is a hybrid deep learning architecture. This model, which is formed by the combination of different layers is a powerful hybrid model that can process both time series data and spatial features with high performance. The versatility and variety of the proposed model is quite effective in identifying the anomalies encountered. At the same time the multi layered structure of the model (Table 1) allows multi dimensional analysis of the data. The use of layers such as CNN, LSTM and Multi Head Attention together has taken the model to an advanced level. In this way the model can learn both short term and long term dependencies with high performance. In addition layers such as Dropout and Batch Normalization were used to increase the generalization ability of the model. In this way, the model can be effective in identifying not only the attack types in the data set it processes, but also the attack types in the data set it processes, but also the attack types that have not been seen before.

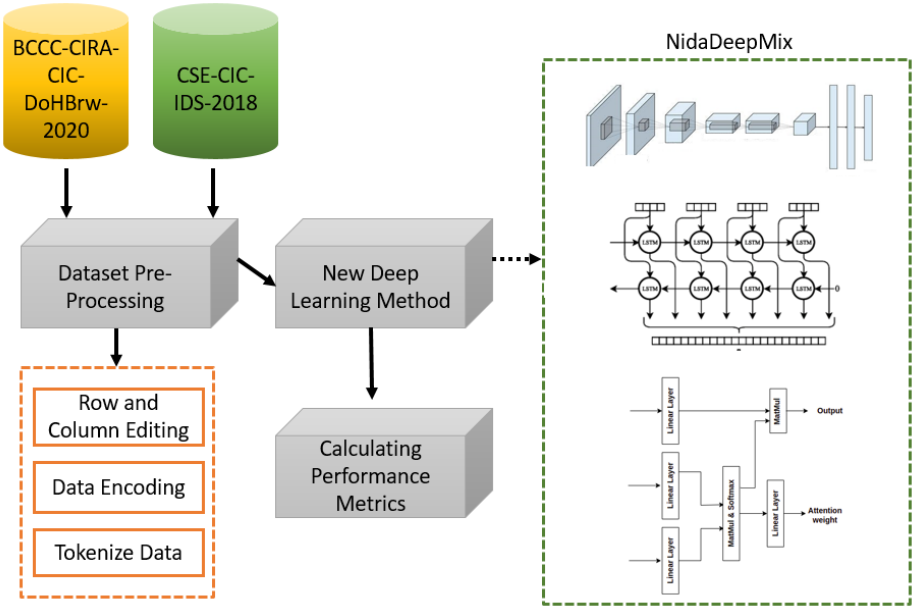

Fig. 6. Proposed Model

The proposed hybrid model generally consists of three steps. These are data preprocessing step, new deep learning step and performance metrics calculation step. The steps are sequential and each step uses the outputs of the previous step.

STEP 1: One of the processes required to detect attacks with higher accuracy in the used datasets is the preprocessing step. In this step, the rows and columns are first arranged in the desired format. To this end, unnecessary rows and columns in both datasets (CSE-CIC-IDS-2018 and BCCC-CIRA-CIC-DoHBrw-2020) are removed. Here, columns such as row numbers and dates are removed. Next, the data is encoded to make the dataset easier to understand and process for the developed architecture. In this step, categorical data is converted to numerical format. Then, to better understand and analyze the dataset in machine language, the data is segmented into tokens. This process transforms the data into meaningful smaller subunits. After these processes, the data becomes more meaningful and usable.

STEP 2: The processed data is passed to the next step. This step is the step where the deep learning process, which is the main part of the proposed architecture is applied. Here the data is processed with a new hybrid model, NidaDeepMix. NidaDeepMix is a model created by combining various deep learning layers. The layer names and parameters used in the model are given in Table 1. In the proposed architecture the data set is added to the model to start processing with the Input layer. The data entered with the Embedding layer is introduced to the model in vector form. This layer allows the semantic relationships of the data to be learned and allows it to be expressed as lower-dimensional but dense vectors. Spatial features are extracted from the data with the 1D Convolutional layer. In the Max Pooling 1D layer, the outputs produced by the 1D Convolutional layer are used and the data with the most distinct features are selected. At the same time the data size is reduced. Here the highest value passing through each filter in the Convolutional layer is selected. Then a second 1D Convolutional layer is added and it is aimed for the model to learn features at a high level. The obtained results were reduced with a Max Pooling 1D layer again. A Bidirectional LSTM layer was added so that the indexes could be processed bidirectionally. The aim of this layer was to learn the dependencies of the data over time. Then a second Bidirectional LSTM layer was added. The features learned from the previous layers were reinforced with this layer. The Multi Head Attention layer was added after this layer, allowing the model to focus on the most important features obtained. The Global Average Pooling layer was added to the model, the average of each feature map was taken and the data was turned into a single vector. In other words while the outputs obtained from the previous layers were reduced, a summary of all the features was obtained. A Dropout layer was added to prevent the created model from memorizing and a Batch Normalization layer was added after it to reduce the complexity of the model and speed up the training time. Finally three consecutive Dense layers were added to the model, providing a fully connected network and the outputs were reduced in each layer. Using three layers in succession in this way made the model more stable and increased the classification performance.

Table 1. Layer parameters

Layers	Input Shape	Output Shape	Activation function
Input Layer	-	None, 59	-
Embedding Layer	None, 59	None, 59,32	-
Conv1D	None, 59,32	None, 55, 64	-
Max pooling 1D	None, 55, 64	None, 27,64	-
Conv1D	None, 27,64	None, 23,128	-
Max Pooling	None, 23,128	None, 11,128	-
Bidirectional	None, 11,128	None, 11,200	-
Bidirectional	None, 11,200	None, 11,200	-
Multi Head Attention	(None, 11,200), (None, 11,200), (None, 11,200)	None, 11,200	-
Global Average Pooling	None, 11,200	None,200	-
Dropout	None,200	None,200	-
Batch Normalization	None,200	None,200	-
Dense	None,200	None,128	ReLu
Dense	None,128	None,64	ReLu
Dense	None,64	None,1	Sigmoid

The 1D CNN layers were chosen to extract local spatial features from sequential traffic data, while the Bidirectional LSTM layers model long term temporal dependencies crucial for detecting multi stage attacks over time. The Multi Head Attention mechanism allows the model to focus on the most critical features across the sequence. Key parameters, such as the number of filters and LSTM units were optimized via grid search to balance high accuracy with computational efficiency, making the model suitable for resource aware deployment.

Each layer of the created neural network model processes the inputs and produces a certain number of features as a result. The number of features obtained from each model is shown in Figure 7.

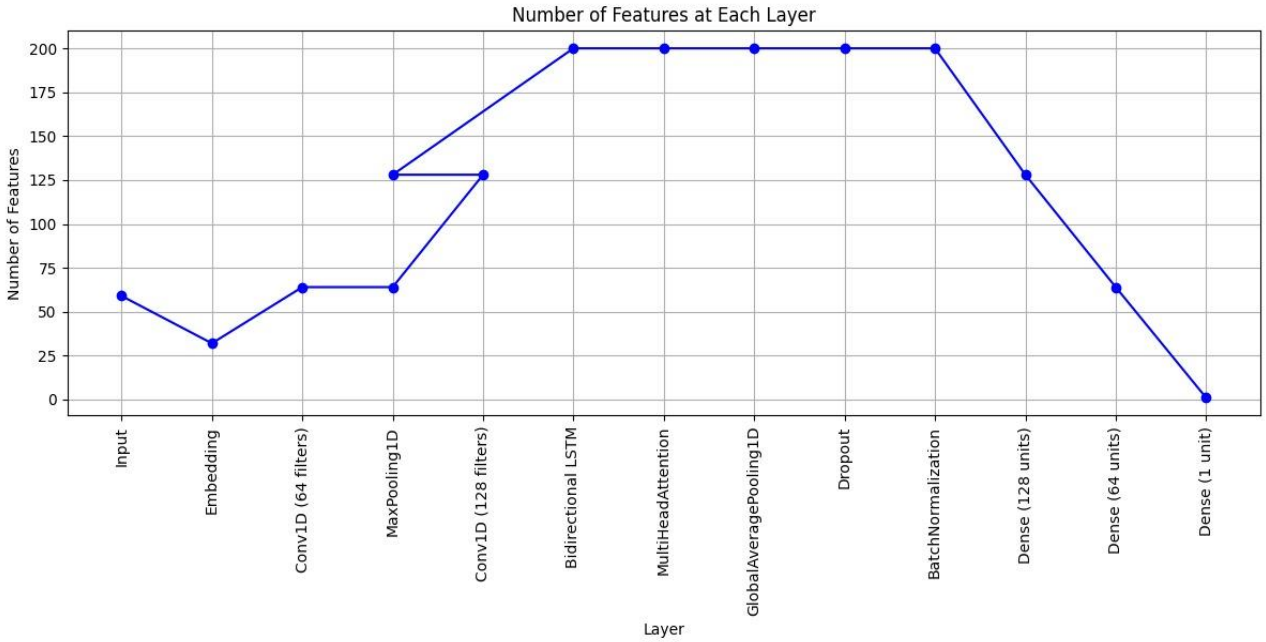

Fig. 7. Number of Features at Each Layer

STEP 3: In the last stage, the model training was completed with the proposed new neural network and the performance metrics were calculated. The experimental results obtained are given in the 'Conclusion' section.

5. Results

After the data is trained, the performance of the created model is calculated with performance metrics. The accuracy and generalization ability of the model can be evaluated with these calculated metrics. In order to calculate some basic performance metrics (Accuracy, Precision, Recall, F1 Score and Geometric Mean), the Confusion Matrix of each data set must first be created. As a result of the training performed with the NidaDeepMix architecture, the Confusion Matrix of the CSE-CIC-IDS-2018 and BCCC-CIRA-CIC-DoHBrw-2020 data sets is shown in Figure 8.

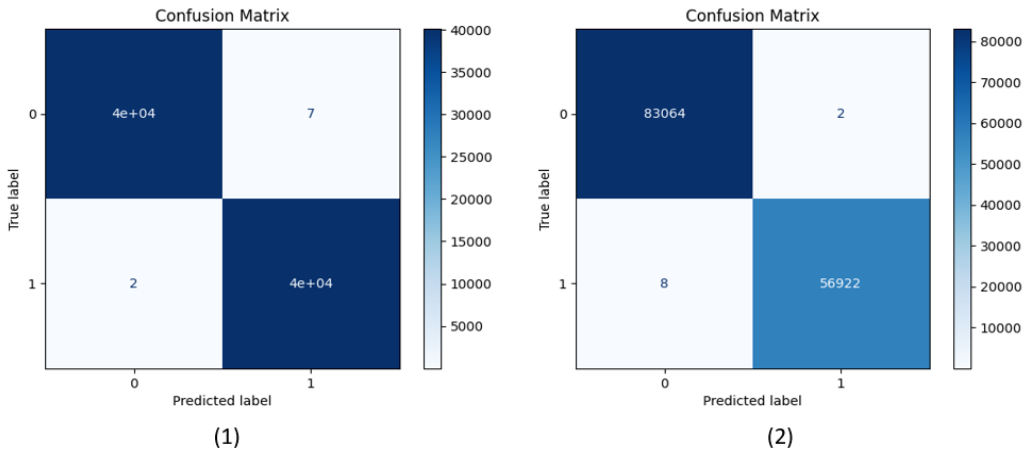

Fig. 8. BCCC-CIRA-CIC-DoHBrw-2020 (1) and CSE-CIC-IDS-2018 (2) Confusion matrix

Some basic performance metrics in Table 2 were calculated using the Confusion matrices given in Figure 8.

The results calculated with the specified performance metric formulas obtained as a result of training the Complexity Matrix and NidaDeepMix architecture are given in Table 2. Table 2 lists the metrics calculated for the two datasets. (Accuracy = (TP+TN)/all (1), Precision = TP/(TP+FP) (2), Recall = TP/(TP+FN) (3) and F1 = 2(Precision x Recall) / (Precision + Recall) (4)).

Table 2. Calculating performance metrics for each dataset

Performance Metrics	BCCC-CIRA-CIC-DoHBrw-2020 Dataset	CSE-CIC-IDS-2018 Dataset
Accuracy	99.98	99.99
Precision	99.98	99.99
Recall	99.99	99.98
F1 Score	99.98	99.99
Geometric Mean	99.98	99.99

An examination of Table 2 reveals the superior performance of our proposed architecture, NidaDeepMix. The high values obtained by our model on two datasets demonstrate its versatility and highlight its importance in detecting anomalies in IoT-based satellite networks. Classification Report Heatmap tables can be used to perform a detailed performance analysis of the proposed model on the datasets. This table evaluates the model not only overall but also by class. This table includes the values of the popular performance metrics Precision, Recall, and F1 Score. Furthermore, the Support value is added to understand whether the examples encountered within the classes have a balanced structure. Table 3 contains the Classification Report Heatmap table for the BCCC-CIRA-CIC-DoHBrw-2020 dataset, while Table 4 contains the Classification Report Heatmap table for the CSE-CIC-IDS-2018 dataset. Exceptionally low values for both False Positive and False Negative rates, as evidenced by nearly perfect Precision and Recall, confirm the high reliability of the model for safety-critical systems where both types of errors carry significant costs.

Table 3. BCCC-CIRA-CIC-DoHBrw-2020 Classification Report Heatmap

	Precision	Recall	F1-Score	Support
Class 0	0.999950	0.999825	0.999887	39895.000000
Class 1	0.999825	0.999950	0.999888	40105.000000
Accuracy	0.999888	0.999888	0.999888	0.999888
Macro avg	0.999888	0.999887	0.999887	80000.000000
Weighted avg	0.999888	0.999888	0.999887	80000.000000

Table 4. CSE-CIC-IDS-2018 2018 Classification Report Heatmap

	Precision	Recall	F1-Score	Support
Class 0	0.999904	0.999976	0.999940	83066.000000
Class 1	0.999965	0.999859	0.999912	56930.000000
Accuracy	0.999929	0.999929	0.999929	0.999929
Macro avg	0.999934	0.999918	0.999926	139996.000000
Weighted avg	0.999929	0.999929	0.999929	139996.000000

When Table 3 and Table 4 are considered, it can be seen that the proposed model is extremely consistent and high quality. For both separate data sets class based Precision, Recall and F1 Score values were obtained above %99.9. These values indicate that the model can perform high quality classification. The low FP and FN values obtained from the model also support this situation. In addition these values prove that the model can be a very suitable method for detecting anomalies in IOT based satellite networks, which is one of the critical security problems of recent times.

Accuracy Loss graphs are needed to analyze the training process and performance of the proposed model. With Accuracy-Loss graphs the learning process of the model, training and validation performance, and whether the model memorizes or not can be observed. Accuracy-Loss graphs of the BCCC-CIRA-CIC-DoHBrw-2020 and CSE-CIC-IDS-2018 datasets are shown in Figure 9.

When the Accuracy-Loss graphs of both the BCCC-CIRA-CIC-DoHBrw-2020 dataset and the CSE-CIC-IDS-2018 dataset are examined, it can be observed that the model has a very high Accuracy value and a low Loss value. This shows that the model works as it should depending on the overshoots. Considering the tables, it can be concluded that the proposed NidaDeepMix architecture can accurately and quickly detect anomalies in IOT-based satellite networks.

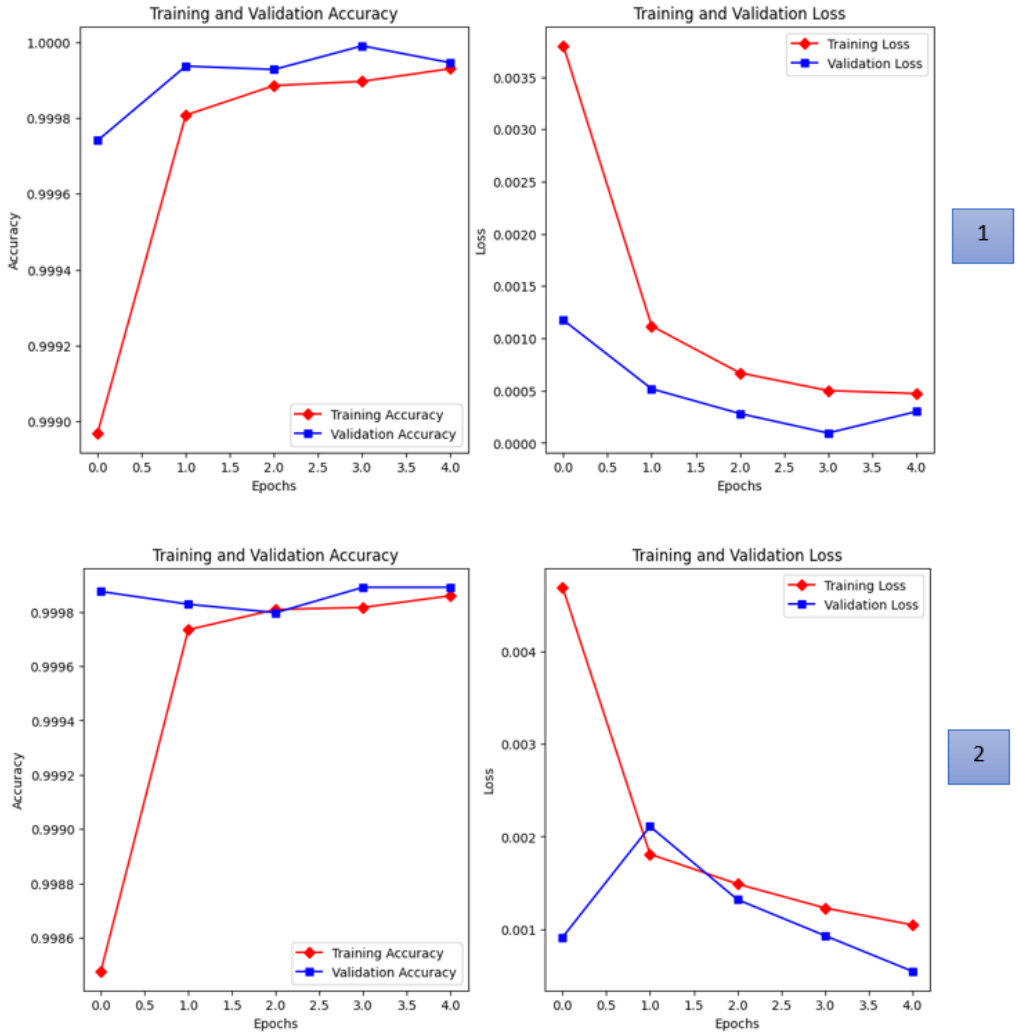

Fig. 9. CSE-CIC-IDS-2018 2018(1) and BCCC-CIRA-CIC-DoHBrw-2020 (2) Accuracy and Loss

6. Discussions

In this study a hybrid deep learning model called NidaDeepMix was developed to detect anomalies in IOT based satellite networks. The model has a strong structure since it is formed by the combination of different layers. Different types of layers have brought the model to a versatile function by coming together and have made it a very suitable method for sensitive and important issues such as negativities occurring in IOT based satellite networks. The created model was tested on two separate data sets. As a result of the tests %99.98 accuracy rate was obtained for the BCCC-CIRA-CIC-DoHBrw-2020 data set and %99.99 accuracy rate was obtained for the CSE-CIC-IDS-2018 data set. Based on the literature review, it is seen that our model has demonstrated superior success.

In order to fully understand the success of the proposed NidaDeepMix model for the detection of anomalies in IOT based satellite networks and to see the difference between it and other architectures, a comparison table was created (Table 5). The table indicates popular deep learning methods and the time (in minutes) they can process each data set.

Table 5. Comparison table

Method	**BCCC-CIRA-CIC-DoHBrw-2020 (%)**	**Approximate Time (Minute)**	**CSE-CIC-IDS-2018 (%)**	**Approximate Time (Minute)**
CNN	98.52	31 m	98.97	40 m
CNN + Attention	99.96	54 m	99.98	60 m
RNN	82.53	13 m	85.44	24 m
LSTM	99.33	67 m	99.87	65 m
GRU	99.89	63 m	99.92	70 m
Our Method	**99.98**	**15 m**	**99.99**	**30 m**

If Table 5 is interpreted, it can be seen that the proposed architecture NidaDeepMix gives the highest Accuracy value for both data sets. At the same time it is seen that our architecture is the fastest architecture after the RNN method. However, if the performance ratio of the RNN method is taken into account, it can be concluded that NidaDeepMix has a noticeable difference in terms of success and speed compared to other models. This superior performance across accuracy, precision, recall and F1 score (as shown in Tables 3 and 4) stems directly from its hybrid architecture. The CNN layers capture local spatial features, the Bidirectional LSTM models long-term temporal dependencies, and the Multi Head Attention mechanism prioritizes the most critical signals. This synergistic design enables more comprehensive feature learning than individual baseline models, which often excel in only one aspect such as CNN in spatial patterns or LSTM in sequence modeling leading to imbalances in precision or recall. Consistently high accuracy combined with the separateness of the test dataset and the use of dropout and batch normalization layers demonstrate that a robust model with low risk of overfitting supports strong generalization ability. The comparison in Table 5 highlights that NidaDeepMix not only achieves the highest accuracy and competitive training times but, crucially its hybrid design provides a more robust overall performance. While baseline models like CNN or LSTM may excel in a single metric our model's integration of spatial and temporal feature extraction, combined with attention mechanisms, ensures consistently high precision and recall a critical balance for minimizing both false alarms and missed detections in security applications.

While the performance demonstrated by the NidaDeepMix architecture is exceptional, it is undeniable that a comprehensive ablation study would provide deeper insights into the contribution of each architectural component. Such a study, which systematically removes or modifies individual layers, would definitively quantify how each element contributes to overall accuracy, precision, and recall. Future research will further validate synergistic design choices and conduct more comprehensive analysis and comparisons to optimize similar hybrid models in the network security field.

6.1 Highligts

The highlights of the study carried out to detect anomalies in IOT satellite networks are as follows:

- A hybrid deep learning model has been proposed for fast and accurate detection of anomalies in IOT based satellite networks. The architecture's efficient design and short training times suggest a favorable scalability and lower computational cost, making it a practical candidate for deployment on ground-based edge servers within the IoT-satellite ecosystem.
- The proposed model has been made versatile by using different layer structures together.
- As a result of the researches, the model has made a noticeable difference to other methods in detecting anomalies in IOT-based satellite networks (with a rate of %99.99 and %99.98).
- While our model gives an excellent accuracy rate, it has performed a very fast training despite being a versatile model (with 15 min. and 30 min.).
- The parameters of the model have been adjusted in a way that can get the highest result from the model and will provide an original model with a high success rate to the literature for detecting anomalies in IOT satellite networks.
- The proposed model has structure suitable for real life scenarios. The model's efficient architecture enables it to be deployed on ground-based gateways or edge servers, which then protect the IoT satellite network, thus mitigating the computational constraints of the end devices themselves.
- The created model is in a form that can be used for different scenarios.

7. Conclusion

In this study NidaDeepMix, a unique and effective deep learning architecture that provides high accuracy for the detection of cyber attacks on IoT based satellite networks, has been proposed. By strategically combining different deep learning layers NidaDeepMix has provided a strong model structure in terms of both high performance and generalizability. Layers such as Convolutional, Bidirectional LSTM, Multi Head Attention were used together in the design of the model allowing the model to learn both spatial and temporal features. As a result of the tests performed on the CSE-CIC-IDS-2018 and BCCC-CIRA-CIC-DoHBrw-2020 datasets %99.99 and % 99.98accuracy were achieved respectively. These high success rates prove that the model performs superiorly not only on a specific dataset but also on datasets with different features. In addition, the short training times of the model reveal the potential to be integrated into real-time applications. In this context the proposed NidaDeepMix model provides a significant contribution to the literature for accurate and rapid detection of cyber attacks in IoT based satellite networks. The success achieved by the model shows that it can be a reference structure in future cyber security studies and anomaly detection applications. As a result, this study offers an innovative and effective approach to increase the security of IoT satellite networks from both technical and practical perspectives.

References

[1] S. K. Routray and H. M. Hussein, "Satellite Based IoT Networks for Emerging Applications," Mar. 2019.

[2] K. Sohraby, D. Minoli, B. Occhiogrosso, and W. Wang, "A Review of Wireless and Satellite-Based M2M/IoT Services in Support of Smart Grids," *Mob. Networks Appl.*, vol. 23, no. 4, pp. 881–895, Aug. 2018, doi: 10.1007/S11036-017-0955-1/TABLES/2.

[3] M. De Sanctis, E. Cianca, G. Araniti, I. Bisio, and R. Prasad, "Satellite communications supporting internet of remote things," *IEEE Internet Things J.*, vol. 3, no. 1, pp. 113–123, Feb. 2016, doi: 10.1109/JIOT.2015.2487046.

[4] B. Soret, I. Leyva-Mayorga, S. Cioni, and P. Popovski, "5G satellite networks for Internet of Things: Offloading and backhauling," *Int. J. Satell. Commun. Netw.*, vol. 39, no. 4, pp. 431–444, Jul. 2021, doi: 10.1002/SAT.1394.

[5] M. Gaikwad, M. Khanapurkar, and S. Untawale, "Recent development of nano-satellite constellation as iot communication platform," *AIP Conf. Proc.*, vol. 2424, no. 1, Mar. 2022, doi: 10.1063/5.0078153/2822190.

[6] F. Chai, Q. Zhang, H. Yao, X. Xin, R. Gao, and M. Guizani, "Joint Multi-Task Offloading and Resource Allocation for Mobile Edge Computing Systems in Satellite IoT," *IEEE Trans. Veh. Technol.*, vol. 72, no. 6, pp. 7783–7795, Jun. 2023, doi: 10.1109/TVT.2023.3238771.

[7] C. Zhou *et al.*, "Delay-aware iot task scheduling in space-air-ground integrated network," *Proc. - IEEE Glob. Commun. Conf. GLOBECOM*, 2019, doi: 10.1109/GLOBECOM38437.2019.9013393.

[8] S. K. Routray, A. Javali, A. Sahoo, K. P. Sharmila, and S. Anand, "Military applications of satellite based IoT," *Proc. 3rd Int. Conf. Smart Syst. Inven. Technol. ICSSIT 2020*, pp. 122–127, Aug. 2020, doi: 10.1109/ICSSIT48917.2020.9214284.

[9] S. K. Routray, R. Tengshe, A. Javali, S. Sarkar, L. Sharma, and A. D. Ghosh, "Satellite Based IoT for MC Applications," Mar. 2019.

[10] P. P. Ray, "Towards an internet of things based architectural framework for defence," *2015 Int. Conf. Control Instrum. Commun. Comput. Technol. ICCICCT 2015*, pp. 411–416, May 2016, doi: 10.1109/ICCICCT.2015.7475314.

[11] C. Han, A. Liu, H. Wang, L. Huo, and X. Liang, "Dynamic Anti-Jamming Coalition for Satellite-Enabled Army IoT: A Distributed Game Approach," *IEEE Internet Things J.*, vol. 7, no. 11, pp. 10932–10944, Nov. 2020, doi: 10.1109/JIOT.2020.2991585.

[12] S. K. Routray, R. Tengshe, A. Javali, S. Sarkar, L. Sharma, and A. D. Ghosh, "Satellite Based IoT for Mission Critical Applications," *2019 Int. Conf. Data Sci. Commun. IconDSC 2019*, Mar. 2019, doi: 10.1109/ICONDSC.2019.8817030.

[13] W. Jiang *et al.*, "Enhanced Communications on Satellite-Based IoT Systems to Support Maritime Transportation Services," *Sensors 2022, Vol. 22, Page 6450*, vol. 22, no. 17, p. 6450, Aug. 2022, doi: 10.3390/S22176450.

[14] I. Lysogor, L. Voskov, A. Rolich, and S. Efremov, "Study of Data Transfer in a Heterogeneous LoRa-Satellite Network for the Internet of Remote Things," *Sensors 2019, Vol. 19, Page 3384*, vol. 19, no. 15, p. 3384, Aug. 2019, doi: 10.3390/S19153384.

[15] R. Damaševičius, N. Bacanin, and S. Misra, "From Sensors to Safety: Internet of Emergency Services (IoES) for Emergency Response and Disaster Management," *J. Sens. Actuator Networks 2023, Vol. 12, Page 41*, vol. 12, no. 3, p. 41, May 2023, doi: 10.3390/JSAN12030041.

[16] U. Zafar, M. A. Shah, A. Wahid, A. Akhunzada, and S. Arif, "Exploring IoT Applications for Disaster Management: Identifying Key Factors and Proposing Future Directions," *EAI/Springer Innov. Commun. Comput.*, pp. 291–309, 2019, doi: 10.1007/978-3-319-99966-1_27.

[17] U. Inayat, M. F. Zia, S. Mahmood, H. M. Khalid, and M. Benbouzid, "Learning-Based Methods for Cyber Attacks Detection in IoT Systems: A Survey on Methods, Analysis, and Future Prospects," *Electron. 2022, Vol. 11, Page 1502*, vol. 11, no. 9, p. 1502, May 2022, doi: 10.3390/ELECTRONICS11091502.

[18] N. Moustafa, I. Khan, … M. H.-I. T., and undefined 2022, "DFSat: Deep Federated Learning for Identifying Cyber Threats in IoT-based Satellite Networks," *ieeexplore.ieee.orgN Moustafa, IA Khan, M Hassanin, D Ormrod, D Pi, I Razzak, J SlayIEEE Trans. Ind. Informatics, 2022•ieeexplore.ieee.org*.

[19] N. Koroniotis, N. Moustafa, and J. Slay, "A new Intelligent Satellite Deep Learning Network Forensic framework for smart satellite networks," *Comput. Electr. Eng.*, vol. 99, p. 107745, Apr. 2022, doi: 10.1016/J.COMPELECENG.2022.107745.

[20] J. Jose and D. V Jose, "Deep learning algorithms for intrusion detection systems in internet of things using CIC-IDS 2017 dataset," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 1, pp. 1134–1141, 2023, doi: 10.11591/ijece.v13i1.pp1134-1141.

[21] X. Zhang, J. Ran, and J. Mi, "An Intrusion Detection System Based on Convolutional Neural Network for Imbalanced Network Traffic," *Proc. IEEE 7th Int. Conf. Comput. Sci. Netw. Technol. ICCSNT 2019*, pp. 456–460, Oct. 2019, doi: 10.1109/ICCSNT47585.2019.8962490.

[22] R. Uddin and S. A. P. Kumar, "SDN-Based Federated Learning Approach for Satellite-IoT Framework to Enhance Data Security and Privacy in Space Communication," *IEEE J. Radio Freq. Identif.*, vol. 7, pp. 424–440, 2023, doi: 10.1109/JRFID.2023.3279329.

[23] E. U. H. Qazi, M. H. Faheem, and T. Zia, "HDLNIDS: Hybrid Deep-Learning-Based Network Intrusion Detection System," *Appl. Sci. 2023, Vol. 13, Page 4921*, vol. 13, no. 8, p. 4921, Apr. 2023, doi: 10.3390/APP13084921.

[24] W. Guo, J. Xu, Y. Pei, L. Yin, C. Jiang, and N. Ge, "A Distributed Collaborative Entrance Defense Framework Against DDoS Attacks on Satellite Internet," *IEEE Internet Things J.*, vol. 9, no. 17, pp. 15497–15510, Sep. 2022, doi: 10.1109/JIOT.2022.3176121.

[25] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," *Int. Conf. Inf. Syst. Secur. Priv.*, vol. 2018-January, pp. 108–116, 2018, doi: 10.5220/0006639801080116.

Authors' Profiles

Nida Canpolat graduated from Digital Forensics Engineering in 2022. She is currently doing her master's degree in Digital Forensics Engineering. Her study topics include machine learning, deep learning, cyber security and artificial intelligence.

Sengul Dogan received the master's degree in bioengineering the Ph.D. degree in electrical and electronics engineering from the Firat University, Elazig, Turkey, in 2007 and 2011, respectively. She is currently a Professor with the Digital Forensics Engineering, Technology Faculty, Firat University. Her main research interests include computer forensics, mobile forensics, image processing, and signal processing. She has been working actively on developing algorithms in machine learning for biomedical data.

Mehmet Karakose (Senior Member, IEEE) received the B.S. degree in electrical engineering, and the M.S. and Ph.D. degrees in computer engineering from Firat University, Elâzığ, Türkiye, in 1998, 2001, and 2005, respectively. From 1999 to 2005, he was a Research Assistant with the Department of Computer Engineering, Firat University. He was an Assistant Professor and an Associate Professor with the Department of Computer Engineering, Firat University, from 2005 to 2014, and from 2014 to 2020, respectively. He is currently a Professor Doctor with the Department of Computer Engineering, Firat University. His research interests include fuzzy systems, intelligent systems, quantum computing, simulation and modeling, fault diagnosis, computer vision, railway inspection systems, and photovoltaic systems.

Turker Tuncer received the master's degree in electronics and computer sciences and the Ph.D. degree in software engineering from Firat University, Elazig, Turkey, in 2011 and 2016, respectively. He is currently an Associate Professor with the Digital Forensics Engineering, Technology Faculty, Firat University. His main research interests include feature engineering, image processing, signal processing, information security, and pattern recognition. He has been working actively on developing algorithms in machine learning applied to visual surveillance and biomedical data.

Musa Yenilmez received the B.S. degree in computer engineering from Firat University, Elâzığ, Türkiye, in 2020. From 2023 to now, he is a Research Assistant with the Department of Computer Engineering, Firat University. His research interests include machine learning, artificial intellegence, image proccessing and federated learning.

How to cite this paper: Nida Canpolat, Sengul Dogan, Mehmet Karakose, Turker Tuncer, Musa Yenilmez, "Anomaly Detection in IoT Based Satellite Networks: NidaDeepMix", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.15, No.6, pp. 1-13, 2025. DOI:10.5815/ijwmt.2025.06.01