International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.1 (2025) pp. 792-810
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Exploring Artificial Intelligence and Data Science-Based Security and its Scope in IoT Use Cases

Amjan Shaik[1]*, Bhuvan Unhelkar[2], Prasun Chakrabarti[3]

[1]PDF Scholar, University of South Florida, USA & Dean R&D Cell, St.Peters Engineering College, Maisammaguda, Telangana, INDIA,
* **Corresponding Author Email:** amjansrs@gmail.com - **ORCID:** 0000-0002-5247-785X

[2]Department of Information Systems and Decision Sciences, Muma College of Business, University of South Florida, Sarasota, USA,
Email: bunhelkar@usf.edu - **ORCID:** 0000-0002-5247-785Y

[3]Department of CSE, Director - Directorate of Research and Publications & Dean International Affairs, Sir Padampat Singhania University, Udaipur, Rajasthan, INDIA,
Email: drprasun.cse@gmail.com - **ORCID:** 0000-0002-5247-785Z

Article Info:

DOI: 10.22399/ijcesen.869
Received : 03 December 2024
Accepted : 06 February 2025

Keywords :

Internet of Things (IoT) security,
Intrusion detection systems (IDS),
Multi-Layer Perceptron (MLP),
Deep Learning Framework,
Cybersecurity.

Abstract:

The fast growth of IO networks has resulted in a security crisis besides the development of decentralized-based innovations, and such decentralized bases or technologies also made challenges in terms of speed, performance, and scalability. Traditional machine learning-based intrusion detection systems (IDS) are unable to manage the intricate and non-linear correlations seen in massive amounts of IoT data. They produce relatively low detection rates, especially in multi-class classification, where many attack types must be addressed. Overcoming these hurdles calls for frameworks: innovative enough to accommodate the challenge whilst using the wealth of data produced by IoT devices. Abstract In this paper, we introduce a unique MLP-based deep learning architecture for intrusion detection in IoT settings. This framework includes a preprocessing pipeline that optimally normalizes and applies one-hot-encoding to the data to prepare it optimally for classification. We tested the algorithms on the UNSW-NB15 dataset, commonly used for IDS. Mere quantitative results show that MLP surpasses classical models like Logistic Regression, SVM, and Random Forests, giving a precision of 97.53%, recall of 97.23%, and accuracy of 97.73% on the multi-class classification task. This framework is undoubtedly scalable and provides a sufficient security mechanism for the whole IoT ecosystem; hence, it can be used in various actual use cases. This performance shows that it could solve the new threats developing in IoT environments.

1. Introduction

The explosive expansion of IoT devices has transformed sectors with the capability to gather data in real-time and facilitate automation connect consistently. But this growth also finally brings significant issues, especially around data security, processing speed, and scalability. Due to its inherent nature of producing millions of new types of data with a high complexity structure, IoT networks will have to encounter a higher degree of human skills needed to set high cyber threats like intrusion, attack, data losses, and data breaches. However, conventional Intrusion Detection Systems (IDS) have several drawbacks, including poor scalability, dependence on traditional machine learning models, and challenges in multi-class classification, which limit their capability to address these issues. The corresponding literature emphasizes that IoT ecosystems desperately require more sophisticated methods to protect their domains. Ahmed et al. As [1] noted, although the combination of IoT and big data has great potential, it is also a double-edged sword plagued by data inefficiency and security issues. Kumar et al. 2] studied technical transformations (IoT + big data) but called for reliable frameworks for risk management. Similarly, Tanwar et al. However, secure data analytics architectures based on ML and DL have been proposed in [2-11]. However, the accuracy and

scalability of such mechanisms in a dynamic IoT environment are still not adequately addressed. Such results highlight the need for new approaches to counter the growing requirements for IoT security.

To overcome these difficulties, this study intends to provide a DL-based intrusion detection framework based on Multi-Layer Perceptron (MLP) for IoT networks. The main focus is creating a highly scalable, efficient, and accurate method that can deal with various attack scenarios in the IoT scenario. The novelties of the research comprise an optimized preprocessing pipeline, reliable feature engineering techniques, and the MLP incorporation to improve the classification performance. The proposed framework outperforms the conventional approaches in capturing intricate and non-linear data interactions.

Contributions to Research are Substantial We provide a detailed comparison of classical and contemporary ML models, like Logistic Regression SVM and Random Forests, to establish benchmarking capabilities. Second, the study presents a comprehensive preprocessing pipeline that entails normalization and one-hot encoding to harmonize the compatibility with the MLP structure. Third, the UNSW-NB15 dataset, widely used for intrusion detection, is used to confirm the practicability of the framework.

The structure of the paper is as follows: A thorough literature review is included in Section II for IoT security techniques, and it highlights the gaps and opportunities in existing IoT security solutions. In Section 3, we present the suggested method, which is based on MLP, about evaluation metrics, model creation, and data processing. Section 4 presents the experimental results in detail and compares the performance of the suggested framework with the most advanced models. The discussion and the limitations of the study are presented in Section 5. Results are discussed about the importance of the findings, and possible limitations of the study are pointed out. Lastly, Section 6 ends the paper with future research directions (i.e., scalability, adaptability, and real-time deployment in IoT systems).

Related Work

The literature explores the integration of IoT, AI, and big data analytics, addressing security, efficiency, and emerging challenges in IoT applications. Ahmed et al. [1], the surge in IoT devices aligns with significant data growth, posing difficulties in data efficiency, processing, analytics, and security. Opportunities emerge from their convergence, which is explored in this paper. Kumar et al. [2] explored IoT and big data's transformative impact on biomedical and healthcare technologies, focusing on advanced medical imaging and telemedicine applications. Adi et al. [3] addressed challenges in IoT applications, focusing on data processing limitations and proposing an adaptive learning framework. Tien et al. [4] use the concept of service goods to combine physical goods with a service layer, enhanced by IoT, RTDM, and AI technologies' integration. Yaqoob et al. [5] Industrial IoT (IIoT) generates big data, but processing faces challenges due to IoT resource constraints. This study explores BDA's role in intelligent IIoT systems, presenting frameworks, case studies, opportunities, and challenges. Ghosh et al. [7] IoT Evolution, AI Impact, Future Prospects, Ethical Concerns, Human Control, Smart Revolution, Technological Advancements, and Work Changes. Driss et al. [8] Surveyed IoT and DL for smart cities. Integrating IoT in urban life enhances services like healthcare and surveillance. Challenges discussed. Sarker et al. [9] AI rapidly advances in mobile data science, enhancing app intelligence. The paper surveys AI techniques and models for diverse applications. Gupta et al. [10] AI and BDA enhance supply chain resilience. A systematic review reveals their application, the improvements in phases, and the benefits. Challenges highlighted. Tanwar et al. [11] explored ML and DL for secure data analytics, proposing an architecture and taxonomy, addressing challenges, and comparing existing proposals. Iqbal et al. [12] emphasized Big Data's role in innovative city development, discussing its economic impact, challenges, and applications with Computational Intelligence. Rahman et al. [13] Global population growth demands a shift to smart agriculture. IoT and data analytics address challenges, enhance efficiency, and boost productivity. Paun et al. [14] AI and ML reshape education, enhancing personalized learning. A study explores students' knowledge, attitudes, and challenges in adopting AI in HEIs. Fortino et al. [15] Edge computing enhances IoT networks, offering low latency, privacy, and efficient AI applications. The review explores AI-edge convergence, applications, challenges, and future directions.

Alazab et al. [16], the smart city employs ICT for sustainable development, emphasizing privacy and security. Holistic Big Data Integrated AI Modelling addresses these concerns, improving data management in innovative city applications. Lu et al. [17] explored IoT-enabled edge computing, focusing on security considerations, challenges, and opportunities. Case studies on smart parking and CDN are reviewed. Sahoo et al. [18] reviewed big data's applicability in manufacturing, exploring trends and suggesting future research areas. The analysis includes contributors, institutions, and

conceptual evolution. Gill et al. [19] delved into cloud computing's role, emphasizing emerging paradigms like Blockchain, IoT, and AI and assessing their influence and challenges. Janssen et al. [20] explored why AIoT initiatives in smart cities fail to scale, emphasizing strategic, data, and organizational factors. Rejeb et al. [21] reviewed IoT applications in healthcare, emphasizing key topics like AI, blockchain, and 5G. It outlines future research areas and potential challenges for IoT-based healthcare implementation. Bhatia et al. [22] addressed challenges in accessing large IoT data, providing solutions for heterogeneity, security, and real-time processing. Experimental analysis favors fog over cloud. Future trends emphasize security in fog data analytics. Supriya et al. [23] AI and machine learning enhance diagnostics, treatment, and outbreak predictions in healthcare. Big data analysis and wearable devices aid disease prevention. Challenges and equity concerns persist. Dutta et al. [24] Data analytics is crucial across fields, especially in healthcare. Big data and IoT integration enhance real-time medical monitoring. Hong et al. [25] Blockchain technology emphasizes data security yet faces challenges. Integrating machine learning enhances resilience against attacks in various applications, showing promising advancements. Sharma et al. [26] conducted a bibliometric study on big data analytics and machine learning, identifying dominant clusters and emerging research areas. Anderl et al. [27] explored the impact of AI-based cyber-attacks on Industry 4.0, emphasizing evolving threats and strategies, and urging ongoing research for defense development. Wamba et al. [28] explored the impact of digital technologies, online consumer reviews, and big data analytics on consumer goods companies. Wamba et al. [29] introduced a framework for understanding the adoption and impact of the Internet of Things (IoT) at various levels. Shah et al. [30] emphasized the potential of Big Data Analytics (BDA) and the Internet of Things (IoT) in disaster management. Dixit et al. [31], integrating IoT, big data, and AI revolutionizes agri-food systems, enhancing efficiency, traceability, and quality. Embracing these innovations is crucial for modern agriculture's success. Bag, Surajit et al (2020) studied a work entitled role of institutional pressures and resources in the adoption of big data analytics powered artificial intelligence, sustainable manufacturing practices and circular economy capabilities [32]. Zaidan et al. [33] surveyed intelligent processes for IoT-based smart homes, classifying articles into knowledge engineering, detection, analytical, and control processes. Identified issues inform future research recommendations. Raza et al. [34] highlight the challenges and opportunities of fog computing in handling massive IoT data analytics. It explores applications and potential research directions. Yoon et al. [35] reviewed the security challenges of deploying blockchain in smart cities and explored the convergence of blockchain and AI technologies. Singh et al. [36] addressed the need for efficient big data forensics in IoT environments using Google's Map Reduce framework and machine learning models. Winter et al. [37] the Internet is expanding beyond devices, connecting everyday objects. Technical advancements promise benefits, but concerns about surveillance and privacy persist. Varela et al. [38], Advanced in artificial intelligence and data science, spanning theoretical models to diverse applications, are transforming society, economy, and healthcare. Sahu et al. [39] explored innovative technologies, like AI, Blockchain, and IoT, for pan-Canadian health and environment surveillance, addressing challenges and proposing an architecture. Vankatesan et al. [40] enhanced banking infrastructure, enabling real-time data for customer interactions, analytics, and decision-making, addressing growing demands and expectations in digital banking. Bantahar et al. [41] explored the impact of BDA-AI technologies on environmental performance in the supply chain, emphasizing green digital learning's moderating role. Sarker et al. [42] provided an extensive overview of AI-based modeling, exploring various techniques and applications in diverse fields. Saeed et al. [43] discussed the growing demand for 6G wireless communication systems to address limitations in 5G networks, emphasizing key technologies and research directions. Yi et al. [44] AI emerges as a pivotal force in finance, transforming risk control, marketing, and operations. The paper highlights global AI applications, risks, and ethical considerations in the financial sector. Paul et al. [45] The Internet of Things generates vast data analyzed through complex networks, forming human dynamics. Smart Buddy integrates IoT, social networks, and big data for real-time behavior analysis in smart cities. Fuller et al. [46] AI enhances innovation by providing data-driven insights, models, and visualizations, supporting innovation managers in various aspects, as detailed in four case studies. Sheta et al. [47], the Internet of Things (IoT), with billions of connected devices, generates vast amounts of data. Machine learning in smart cities is explored, emphasizing algorithm taxonomy and application specifics. Sofi et al. [48] Modern agriculture, driven by precise data and IoT technologies, leverages machine learning for increased production quality and quantity. [49] Reviewed diverse aspects of network big data, including data types, storage, privacy, security, and applications, highlighting challenges and predicting

future trends. Datta et al. [50] explored big data analytics' potential in energy industry process safety and risk management, offering insights for informed decision-making and safer operations. The review highlights challenges in existing IoT systems, such as data inefficiency, scalability, and evolving threats. This research proposes a robust MLP-based framework to address these issues, leveraging advanced preprocessing, feature engineering, and model training techniques to enhance intrusion detection and security in IoT environments.

2. Material and Methods

2.1 Proposed Framework

The process of implementing the security enhancement for IoT use cases shown in Figure 1 includes several sequential and dependent steps to guarantee the correctness and reliability of the classification performance. Data Importing and Cleaning: The working environment imports the UNSW-NB15 dataset in this phase. To prevent bias in the data and compromise its integrity, mean imputation is used to fill in any missing values. This step is essential since it guarantees the dataset is clean and prepared for additional processing. After this, Data Preprocessing and Feature Engineering are performed to make data ready for modeling. With one-hot, categorical variables get converted to numerical values, allowing machine learning models to understand non-numeric data. We are scaling the numerical features using Min-Max so that all of the variables can have the same range which helps the model to converge faster during training and increases the accuracy of building a model as well. Next, we split the dataset into features (X) and labels (Y) and then perform a 70:30 train-test split in order to make sure that our models are trained on unseen data. In the Model Training Phase, different ML algorithms are implemented on the training dataset. Such as Logistic Regression, Linear SVM, KNN, Decision Tree (DT), Random Forest, and the proposed Multi-Layer Perceptron (MLP) framework. They are trained in isolation, and hyperparameters optimized are similar. This multi-layer perceptron (MLP)-based framework contains deep learning capabilities to learn complex patterns and identify non-linear relationships within the dataset. These features make MLPs a good candidate for the multi-class classification problems within this work. Finally, the Phase Model evaluation uses evaluation metrics to evaluate all models. They cover a wide range of the assessment for binary and also for multi-class classification metrics. So here, cross-validation techniques, such as k-fold validation, are implemented to assure robustness, and ensemble learning techniques, such as the voting classifier, are applied to combine predictions and improve overall performance. The Results Visualization phase (Figure 1) shows graphical representations of the model performance. The developed MLP framework outperforms all models where the performance metrics are displayed as a bar chart and its visualization plot. It includes correlation analysis and confusion matrices, so that if the predictions contain any bias or inconsistent behaviour, they can be picked as insights, thereby leading to potential actions for better tuning. This ensures that these models can later be reused for deployment or future analysis without retraining, saving time and computational costs. The detailed framework, summarized in Figure 1, presents a combination of deep learning and machine learning methods, as an efficient and comprehensive approach to mitigate the security issues in IoT applications. Notations used in this paper are provided in Table 1.

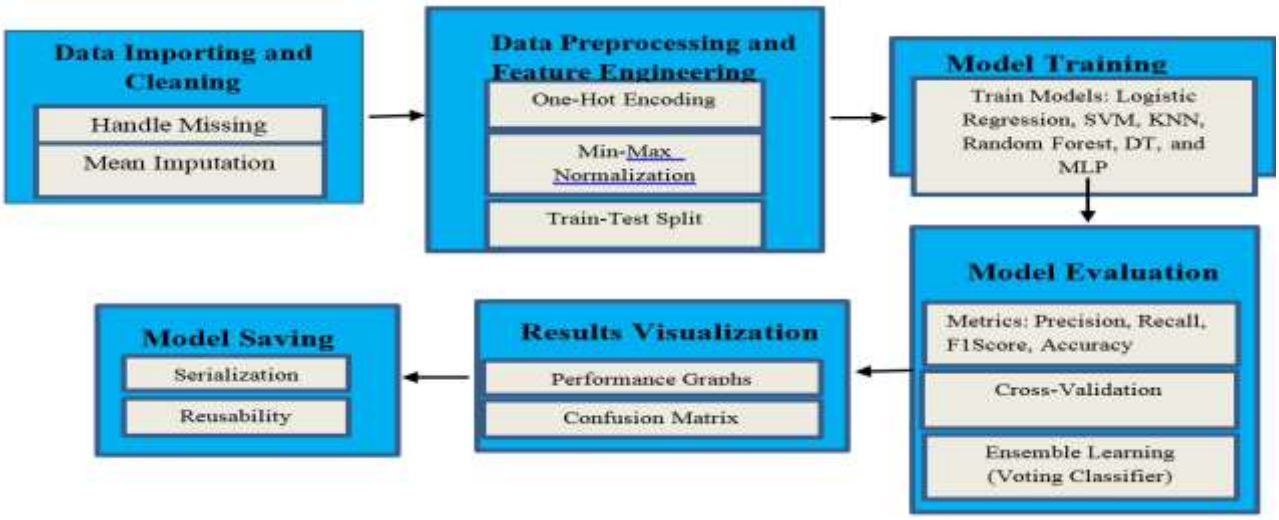

Figure 1. *Methodology for AI and Data Science-Based Security in IoT Use Cases*

Table 1. *Notations Used in the Methodology*

Notation	Description
x_{new}	Mean-imputed value of a feature in the dataset
n	Number of observations
x_i	Individual data points or feature value
x’	The normalized value of a feature
min(x)	Minimum value of the feature x
max(x)	Maximum value of the feature x
X	Feature matrix
Y	Label vector
X_{train}	Training feature matrix
X_{test}	Testing feature matrix
y_{train}	Training label vector
y_{test}	Testing label vector
$\beta_0, \beta_1, \ldots . \beta_n$	Coefficients in the logistic regression model
e	Based of the natural logarithm
W	Weight vector in the SVM model
b	Bias term in the SVM model
y_i	Actual label for observation i
d(x_i, x_j)	Euclidean distance between points x_i and x_j
P_j	Proportion of class j in a dataset
Gini(D)	Gini impurity for dataset DD
H(D)	Entropy of dataset DD
$\sigma(x)$	Sigmoid activation function applied to input xx
$train\_test\_split$	Function to split the dataset into training and testing subsets
k	Number of neighbors in KNN or folds in k-fold cross-validation
Voting Classifier	Ensemble method combining predictions from multiple models

Mathematical Model

The proposed methodology employs a mathematical framework for the Classification of multiple classes using the UNSW-NB15 dataset, focusing on building a robust and efficient machine-learning pipeline. The process begins with data importing and preprocessing, where missing values in the dataset are handled through mean imputation, calculated as $x_{new} = \frac{\sum_{i=1}^{n} x_i}{n}$, ensuring that the dataset is complete and ready for further analysis. The categorical variables are encoded using one-hot encoding, creating k binary variables for a categorical feature with k categories, represented as:

$$x_i = \begin{cases} 1 & if\ x = category_i \\ 0 & otherwise. \end{cases} \quad (1)$$

Normalization is applied to numerical features using Min-Max Scaling, transforming each feature xx to a range [0, 1] as:

$$x' = \frac{x - \min(x)}{\max(x) - \min x)} \quad (2)$$

Subsets of the dataset are then separated for testing and training, usually in a 70:30 ratio, using

$$X_{train}, X_{test}, y_{train}, y_{test} = train_{test}{}_{split(X,Y,test_{size}=0.3,random_{state}=100)} \quad (3)$$

The next phase involves model training, where several ML models, The proposed Multi-Layer Perceptron (MLP), Decision Trees (DT), Random Forests, K-Nearest Neighbors (KNN), Support Vector Machines (SVM), and Logistic Regression are used. The logistic function is used to model a class's likelihood in logistic regression:

$$P(Y=1|X) = \frac{1}{1+e^{-(\beta_0+\beta_1 X_1+\beta_2 X_2+\cdots\ldots+\beta_n X_n)}} \quad (4)$$

For SVM, Maximizing the margin between classes is the aim of optimization, expressed as:

$$maximize\ \frac{2}{\|W\|} \qquad subject\ to\ y_i(W.x_i + b) \geq 1 \quad (5)$$

KNN uses the Euclidean distance to calculate the distance between points and uses the majority vote of its kk nearest neighbors to classify a data point:

$$d(x_i, x_j) = \sqrt{\sum_{k-1}^{n}(x_{ik}, x_{jk})^2} \quad (6)$$

Decision Trees and Random Forests employ metrics like Gini Impurity and Entropy for splitting nodes. Gini Impurity is calculated as:

$$Gini(D) = 1 - \sum_{j-1}^{c} P_j^2 \quad (7)$$

while Entropy is given by:

$$H(D)=-\sum_{j-1}^{c} P_j \log_2 (P_j) \quad (8)$$

The MLP framework, using a deep learning architecture, applies activation functions to add non-linearity, like the Sigmoid function:

$$\sigma(x) = \frac{1}{1+e^{-x}} \quad (9)$$

Cross-validation techniques, such as k-fold validation, are applied to ensure robustness, while ensemble learning, using a voting classifier, aggregates predictions from multiple models to improve accuracy.

The trained MLP model is saved using serialization for future use, ensuring computational efficiency. Integrating preprocessing, model training, and robust pipeline design, this mathematical framework provides a scalable and efficient approach for addressing security challenges in IoT use cases.

Algorithm 1. *MLP-Based Framework for Intrusion Detection in IoT Networks*

Algorithm: MLP- IoT Network Intrusion Detection Framework Based on
Input: UNSW-NB15 dataset D
Output: Results of intrusion detection and performance metrics P

1. Begin
2. D'←DataPreprocessing(D) //encoding and normalization
3. (T1, T2, T3)←SplitData(D')
4. Configure MLP model m
5. Optimize model parameters
6. m'←TrainModel(m, T1)
7. Persist m'
8. Load m'
9. R←IntrusionDetection(m', T2)
10. P←Evaluation(T3, R)
11. Print R
12. Print P
13. End

Proposed Algorithm

The algorithm we propose develops a multi-layer perceptron (MLP)- IoT network using a framework based on intrusion detection in a systematic method with the model. Conceptually, it addresses vital challenges in handling complex non-linear patterns in IoT traffic to ensure efficient data preprocessing, robust training of the model, and holistic evaluation. A scalable and secure algorithm that detects different categories of attacks by combining the above ML classifiers is a good solution for real-world IoT applications.

This paper shows an automated algorithm describing a sequential approach towards establishing an MLP based model for identifying penetrations over an IoT based network. Beginning with the data ingestion and pre-processing stage, where the IMF data set is imported, and NaN values have been filled using mean imputed. Such a preprocessing step guarantee that the dataset is comprehensive and free from discrepancies, which is essential for reliable model training and testing. Now the next phase comes which is data preprocessing, it is common to do since you will want to do a little shaping to the dataset to do classification. The categorical features will be encoded one-hot to help the model understand the non-numeric values. At the same time, Min-Max normalization is used to scale numerical features so that all features are on the same scale. This will increase the model's convergence during training. Next the data is separated into features and labels and split into a train-test set with a 70:30 ratio so that model can be evaluated on unseen data.

During model training, the MLP architecture is defined with an input layer that matches the size of the input feature, ReLU-activated hidden layers, and an output layer with softmax activation for classification into many classes. In this training phase, we apply the Adam optimizer and quantify prediction error using the cross-entropy loss function to fine-tune all model parameters. One hot encodes the target classes and provides a simple method by which the MLP can learn to elaborate complex high-order non-linear relationships in data and be effective in the multi-class classification task.

After training, test data is used to evaluate the model. This model's performance is evaluated by computing key metrics like accuracy, recall, precision, and f1 score. The visualization techniques include some graphs and a performance comparison with classic machine learning models, which facilitates comprehension of the model's efficacy and emphasizes its superiority. Finally, the trained MLP model is serialized using techniques like pickle to be saved and this will help to reuse the same trained MLP model Whenever needed without retraining it. This is an important step, especially when deploying the model in a real IoT environment where resources are limited. This algorithm is the use of advanced preprocessing, modeling, and evaluation techniques all to overcome the issues of IoT networks for intrusion detection.

Dataset Details

The UID, which is to this day one of the most complete benchmark datasets for the evaluation of intrusion detection systems, was released by the Cyber Range Lab of the Australian Centre for Cyber Security (ACCS) as the UNSW-NB15 dataset [51]. IXIA Perfect Storm is a tool it generates The dataset

includes about 2.5 million recordings of network traffic. It covers nine types of malicious activities (e.g., DoS, Backdoors, Exploits) as well as normal traffic. The dataset includes 49 features, which are categorical, numerical, and timestamp data, and a label that types attack. The shape of the data allows us to perform a lot of feature engineering and machine learning on it.

3. Results and Discussions

To assess our proposed framework which is based on Multi-Layer Perceptron (MLP), the paper employs the UNSW-NB15 dataset that contains network traffic samples in ten different classes of which the nine foremost classes are attacks and one is normal traffic, that can be used in intrusion detection applications [30]. We contrast the MLP's performance with that of cutting-edge linear regression, decision trees, random forests, K-Nearest Neighbors (KNN), support vector machines (SVM) (Cortes & Vapnik, 1995), logistic regression (Bishop, 2007), and random forests (Breiman, 2001). The experiments were performed in a Python environment using the Tensor Flow library and Scikit-learn library on a system with the following specifications; Intel i7, 16Gb RAM, and NVIDIA GPU to support deep learning computations. Figure 2 illustrates the distribution of normal and abnormal labels. The majority of the pie, representing 75.99%, is labeled as "normal,"while the remaining 24.01% is labeled as "abnormal." This indicates that the data being analyzed has a significant proportion of normal instances and a smaller proportion of abnormal ones

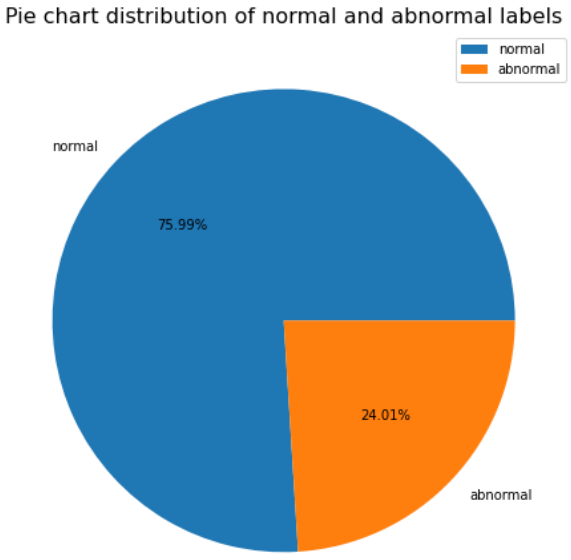

Figure 2. *Pie Plot For Normal And Abnormal (Binary Class)*

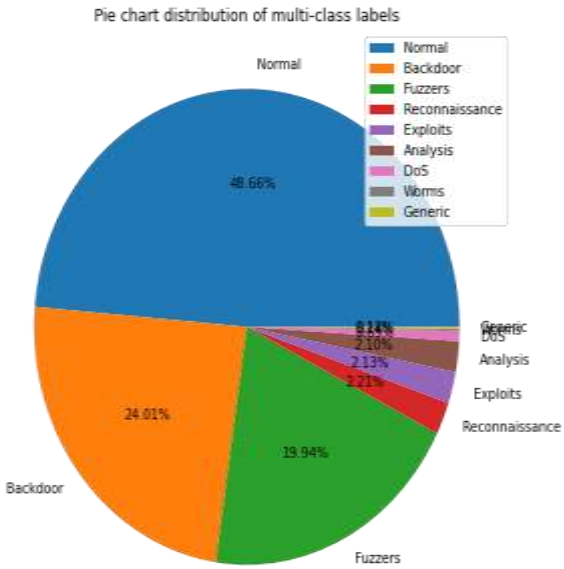

Figure 3. *Data Distribution Dynamics (Multi-Class)*

. Figure 3 illustrates the distribution of multiple class labels. The most significant proportion, 48.66%, is labeled as "Normal," followed by "Backdoor" at 24.01% and "Fuzzers" at 19.94%. Smaller proportions are attributed to "Reconnaissance" (2.21%), "Exploits" (2.13%), "Analysis" (2.10%), "DoS" (0.33%), "Worms" (0.13%), and "Generic" (0.13%).

This indicates that the data being analyzed contains many instances classified as "Normal," with a more balanced representation of the other classes. Figure 4 visually represents the relationships between features and the goal variable in a binary classification problem. White signifies no or weak correlations, blue denotes negative correlations, and red denotes positive correlations. Analyzing these patterns allows you to identify important features for model building and selection.

Figure 5 matrix graphically depicts the connections between the target variable and features in a multi-class classification issue. Positive correlations are shown in red, negative correlations in blue, and no or minimal correlations in white. These trends may be examined to identify important feature selection and model-building factors. Figure 6 shows a linkage between Real versus Theoretical values of a binary class classification model. Data points on the x-axis and values on the y-axis. where the blue line represents the expected and the red line represents the actual. The model's accuracy in predicting each data point's true class may be assessed using this graphic. Figure 7 shows the expected result vs. actual compare diff for binary class classification type. Data points are plotted on the x-axis, while the y-axis shows values. Actual Values: The red line Predicted Values: The blue line With the help of the

visualization, we can evaluate how accurately the model predicts the class for each data point.

The difference displayed between the expected and the actual is the binary class classification type, and is displayed in Figure 8. The x-axis depicts data points and the y-axis provides values. Actual values are represented by the red line, while the blue line corresponds to predicted values. Using this visualization, one can evaluate how well the model is predicting the class for each data point. The figure 9 is the difference between expected values and the real values related to the binary class classification type. Then instead of the x-axis, which is the data points, the y-axis, which is the value.

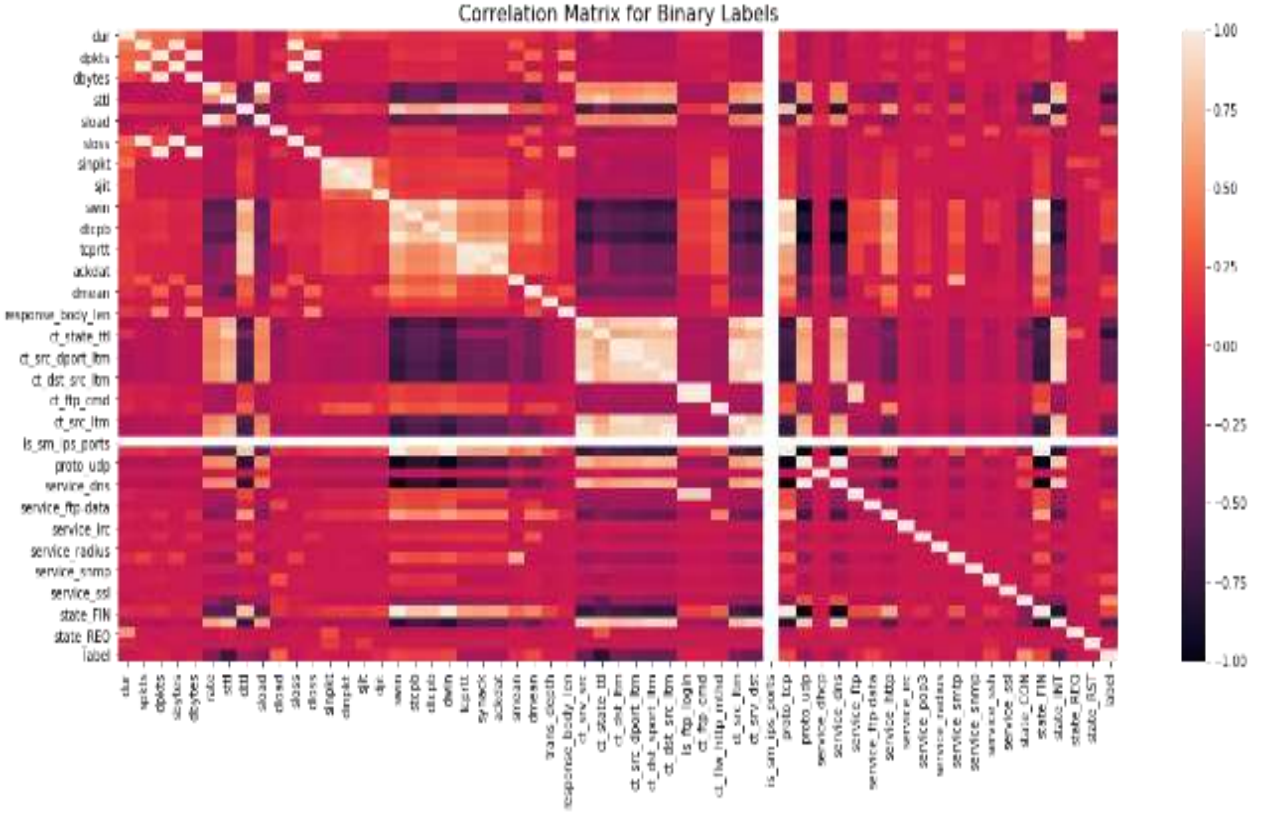

Figure 4. *Matrix of Correlation for Binary Labels*

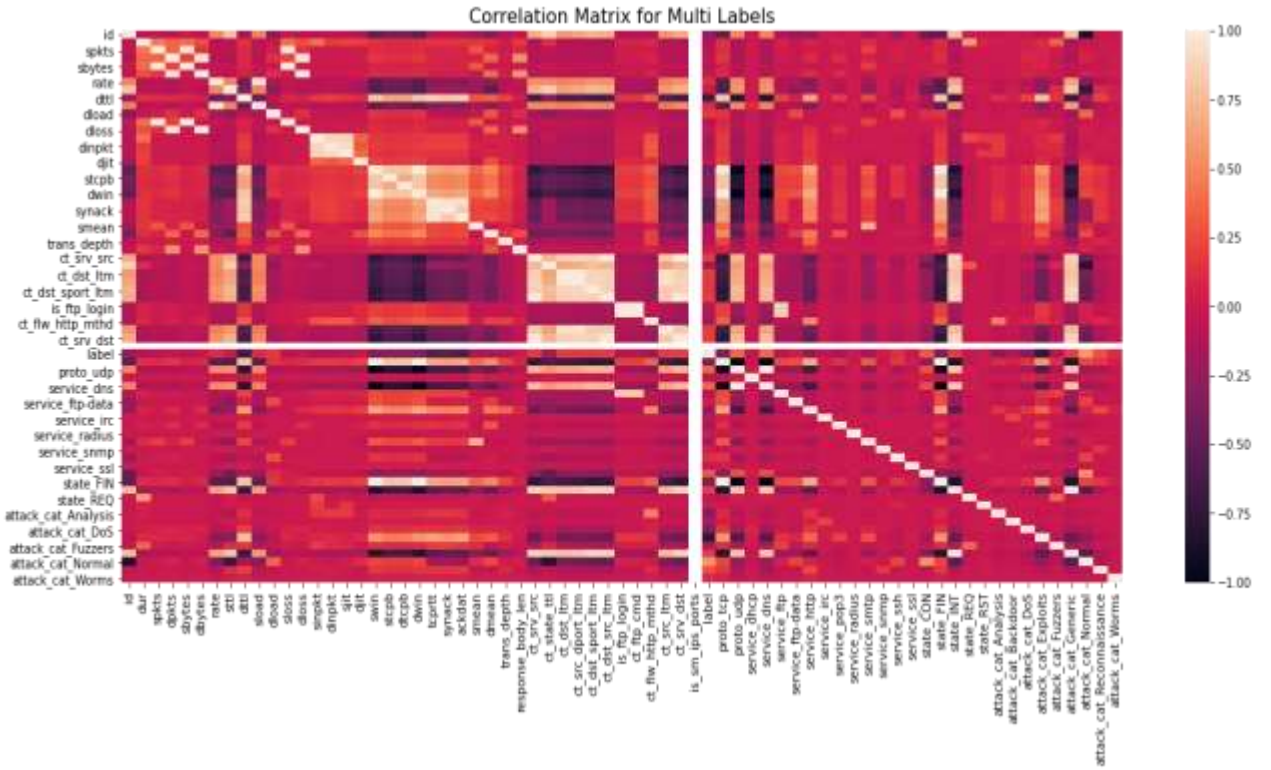

Figure 5. *Matrix of Correlation for Binary Labels*

The red line is the actual value, Blue line is the predicted value. On this visualization, one might evaluate how accurately For every data point, the model can predict the class. Real vs expected comparison for a binary class classification model figure 10 The x-axis shows new data points, while the y-axis shows the matching values. The blue line shows the expected values and the red line the facts.This graphic can be used to evaluate how well each data point is predicted to belong to the correct class. As we can see in figure 11, a binary class classification model used to predict the values will differ from the actual ones. real data points on the x-axis and Y values on the y-axis. The red line indicates the actual values, while the blue line indicates the expected values. Using the graphic we can evaluate the capacity of the model in predicting the appropriate class for each data point. The true vs the predicted values for a binary class classification model, look on the Figure 12. On the y-axis we have the values, and on the x-axis we have the data points. The blue line shows the predicted values while the red line shows the data (the facts). Using the plot, one can evaluate how accurately the model predicted the class to which each point belongs.

Multi-class classification losses with gaps between real and estimated values (Figure 13) Values data points in the x-axis and displayed on the y-axis. Blue line indicates expected values and red line shows facts. With the help of this plot, one can evaluate how accurately the model classifies each data point. Figure 14 compares expected and actual values for a classification model with multiple classes. The x-axis contains data points and the y-axis provides values. The actual values shown in red line and predicted values shown in blue line. With the help of visualization one can evaluate how the model able to inform the class of each data points.In Figure 15, we collect the actual and expected values for a multi-class classification model. The y-axis represents values, and the x-axis represents data points. In contrast, the blue and red lines represent predicted and observed values, respectively. By displaying each data point's class prediction visually, one can judge the performance of the model.A multi-class classification model contrasts the actual and expected results (Figure 16). Values appear on the y-axis, while datapoints are displayed on the x-axis. The blue line represents anticipated values, whereas the red line represents actual values. This graphic can be used to verify if the model is predicting one of the classes for each dot. We decode the predictions into the labels using the following code. (Top: Multi-class (3-class) classification model; Below: Actual vs. Expected distribution of Multi-class classification model; and we run the code to compare the actual vs. expected values (Figure 17). Values are on the y-axis, while data points are on the x-axis. Whereas the blue line displays the expected values, the red line displays the actual values. It is possible to verify whether the model correctly predicted the class for every data point in the figure.

Figure 18 illustrates how a multi-class classification model handles both expected and actual results. Values are represented on the y-axis, and data points are represented on the x-axis. The red line displays the actual data, and the blue line displays the predictions. You may use the following graphic to understand the model performance for every data point prediction class. Multi-Class Classification MODEL (Actual vs Expected) Figure 19 The values are on the y-axis, while the data points are on the x-axis. Expected numbers are shown as the blue line, and actual values are shown in red. The figure might be used to measure how accurately the model classifies each data point correctly Figure 20 is binary classification results demonstrate how well different machine learning models perform in protecting IoT use cases based on measures including accuracy, precision, recall, and F1-score. The proposed Multi-Layer Perceptron (MLP) framework consistently outperforms other models across all metrics. It can accurately identify attack events with few false positives, as evidenced by its greatest precision of 97.23%. Similarly, the recall value for MLP is 97.16%, demonstrating how well it detects most assault events with few false negatives. At 97.19%, MLP's F1-score—a harmonic mean of precision and recall—highlights its well-rounded performance.In terms of accuracy, the MLP framework demonstrates its superiority by achieving 97.56%, reflecting its overall effectiveness in classifying network traffic accurately. Comparatively, Random Forest and Decision Trees also deliver competitive results, with Random Forest scoring slightly below MLP in most metrics. Other models, including Logistic Regression, Linear SVM, and K-Nearest Neighbors (KNN), show reasonable performance but fall short of the MLP framework’s precision and robustness.

Linear Regression, while functional, achieves lower scores, emphasizing its limitations in handling the complex patterns present in the dataset. These results emphasize the significance of the MLP framework in addressing security challenges in IoT environments. Its ability to process non-linear relationships and capture intricate patterns in the data highlights its effectiveness in intrusion detection.

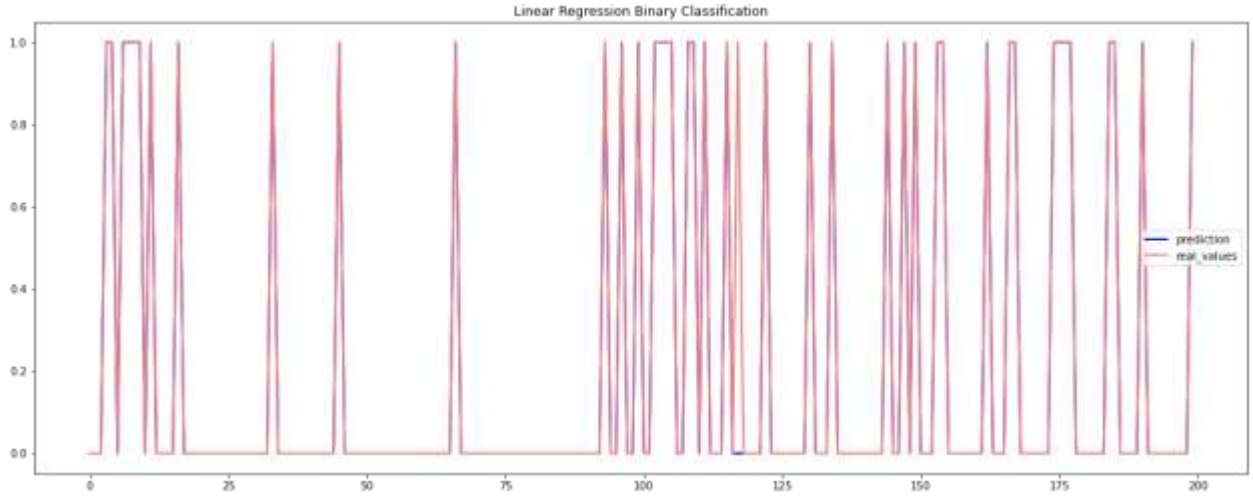

Figure 6. *Linear regression Plot Between Real and Predicted Data*

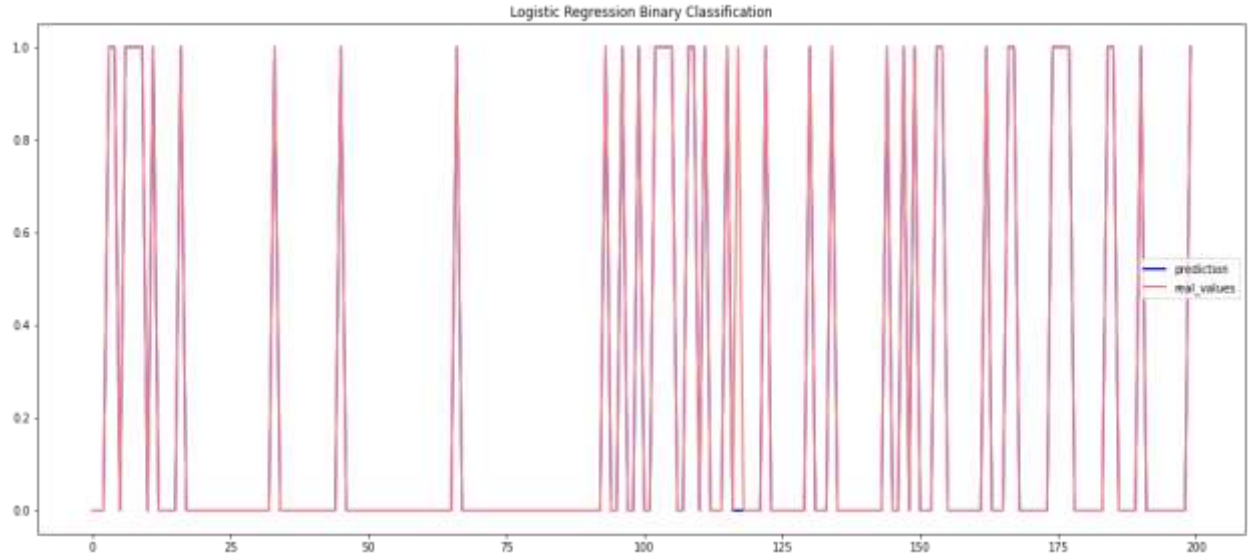

Figure 7. *Logistic Regression Plot Between Real and Predicted Data*

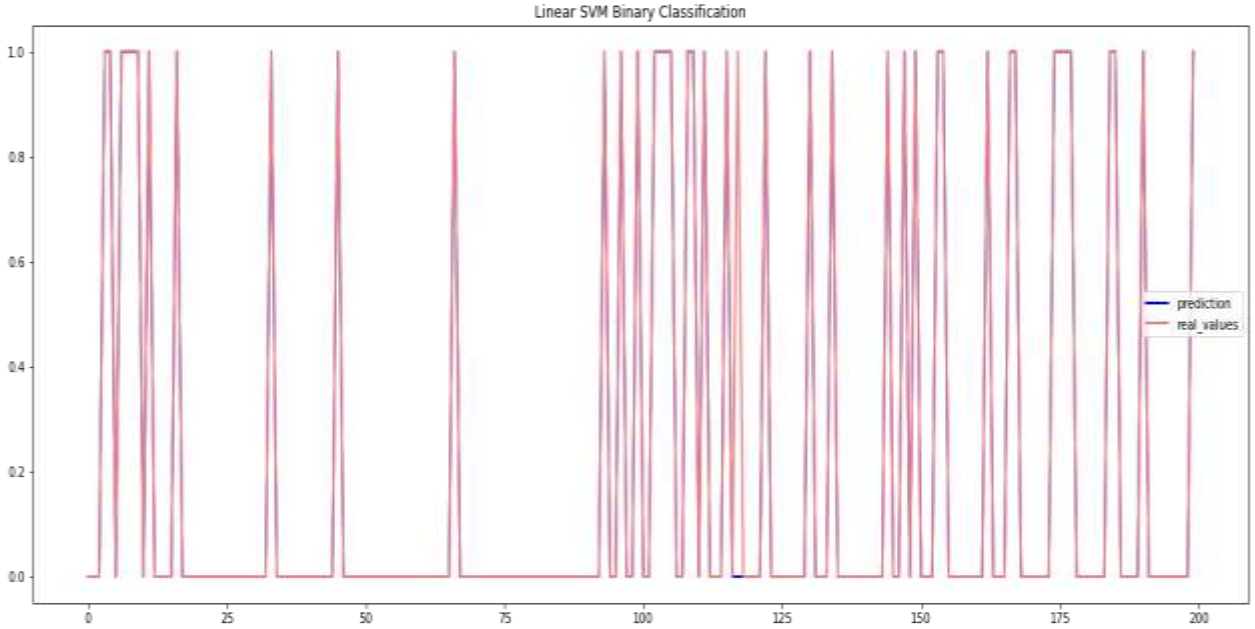

Figure 8. *Linear SVM Plot Between Real and Predicted Data*

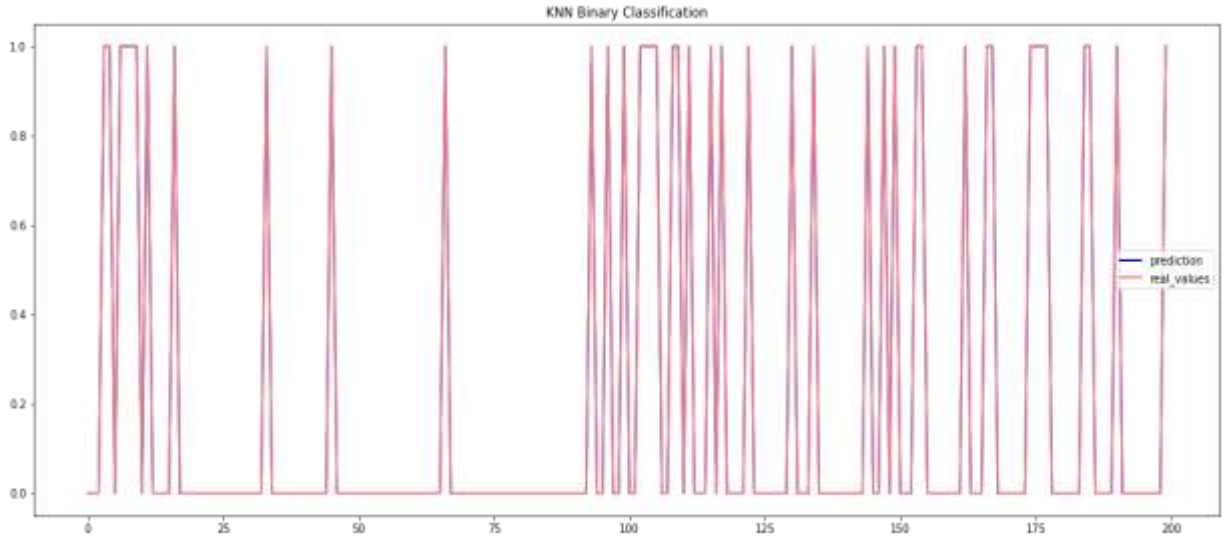

Figure 9. *KNN Plot Between Real and Predicted Data*

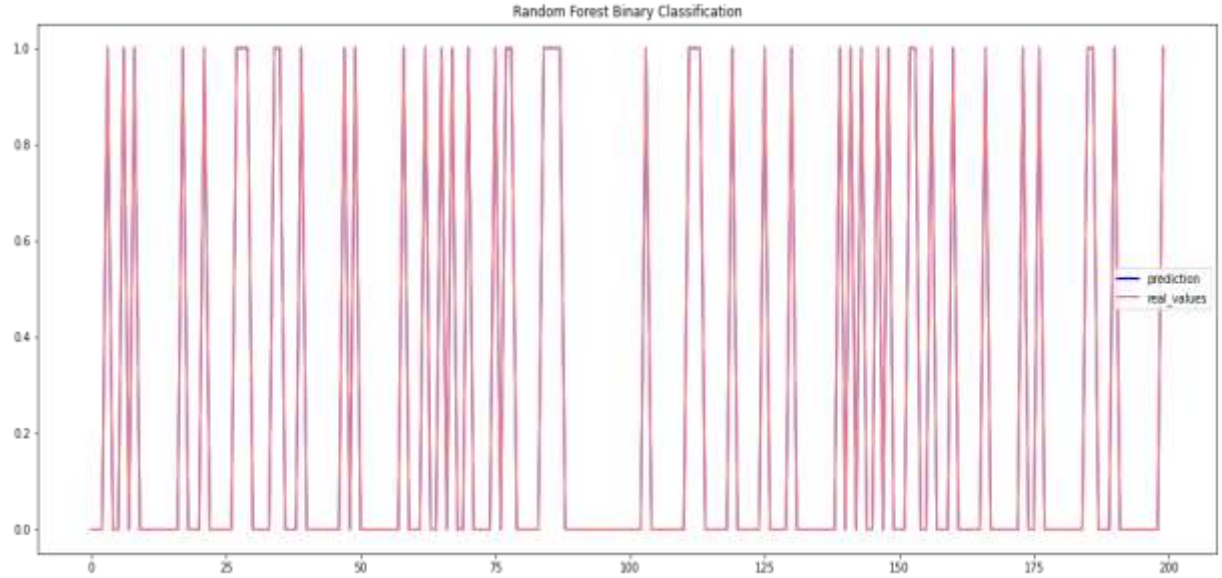

Figure 10. *Random Forest Plotting Actual Data Against Predicted Data*

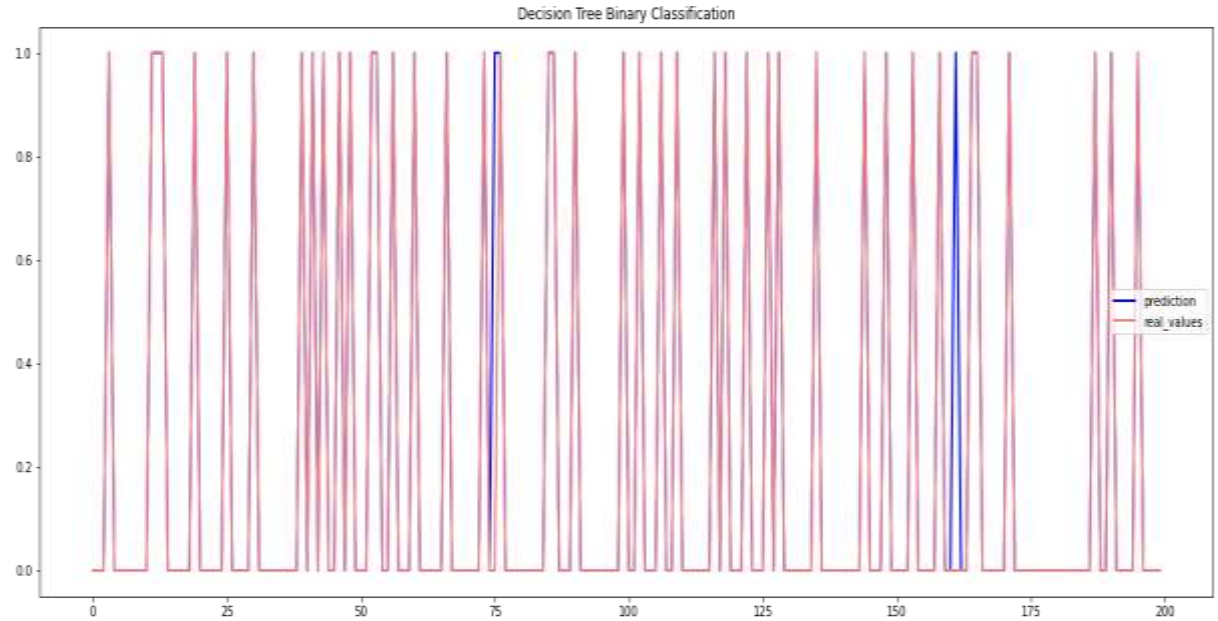

Figure 11. *Real and Predicted Data in a DT Plot*

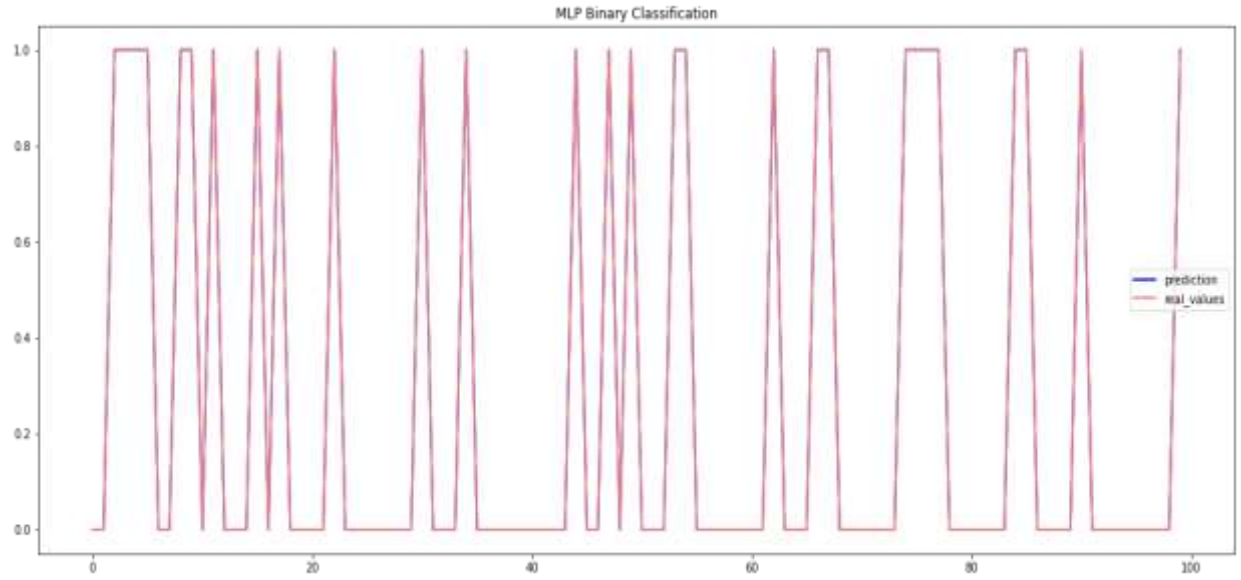

Figure 12. *MLP Plot Between Real and Predicted Data*

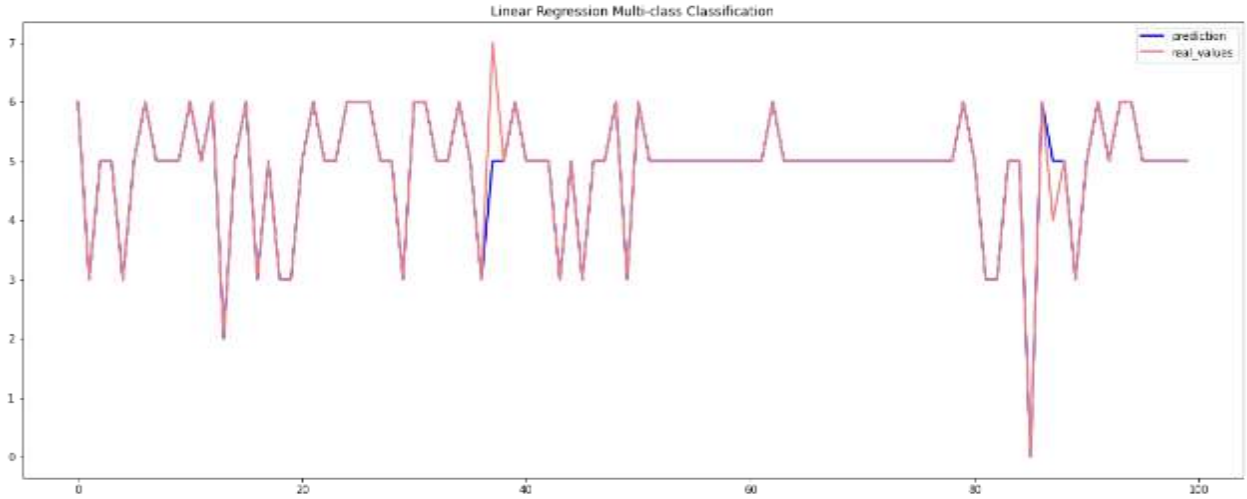

Figure 13. *Plotting Real and Predicted Data using Linear Regression for Multi-Class Classification*

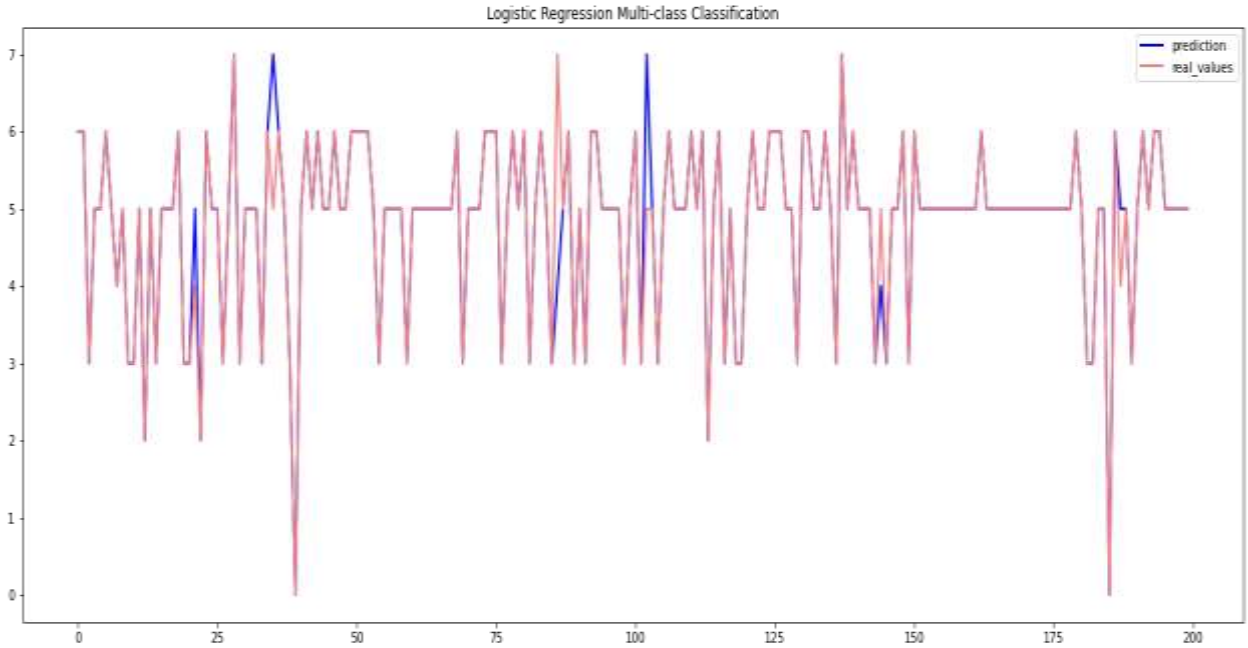

Figure 14. *Plotting Real and Predicted Data Using Logistic Regression for Multi-Class Classification*

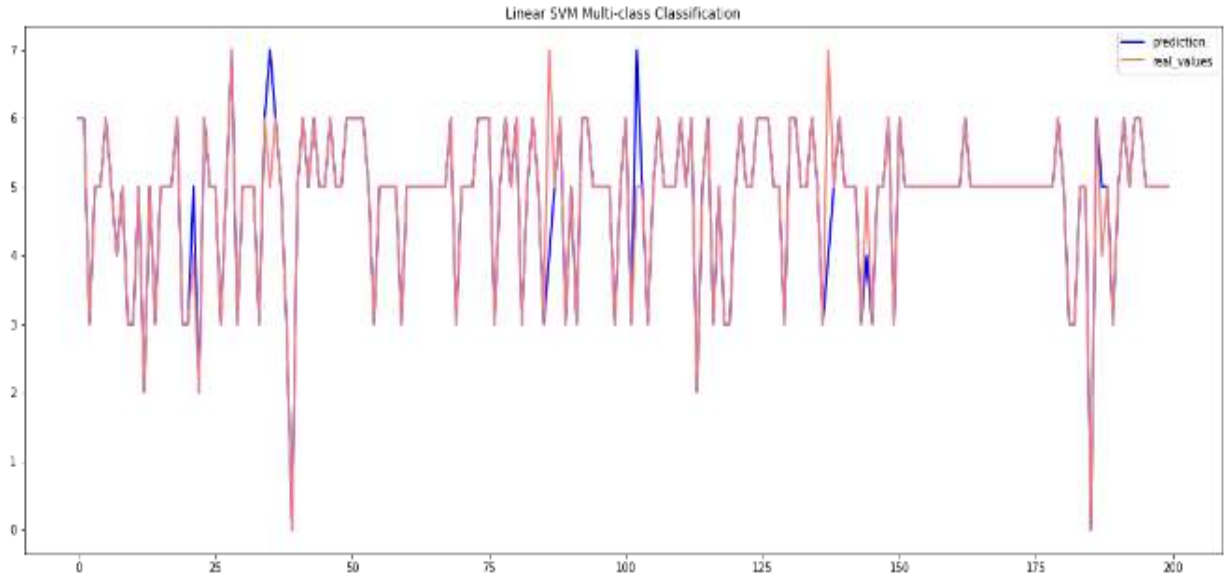

Figure 15. *Plotting Real and Predicted Data Using Linear SVM for Multi-Class Classification*

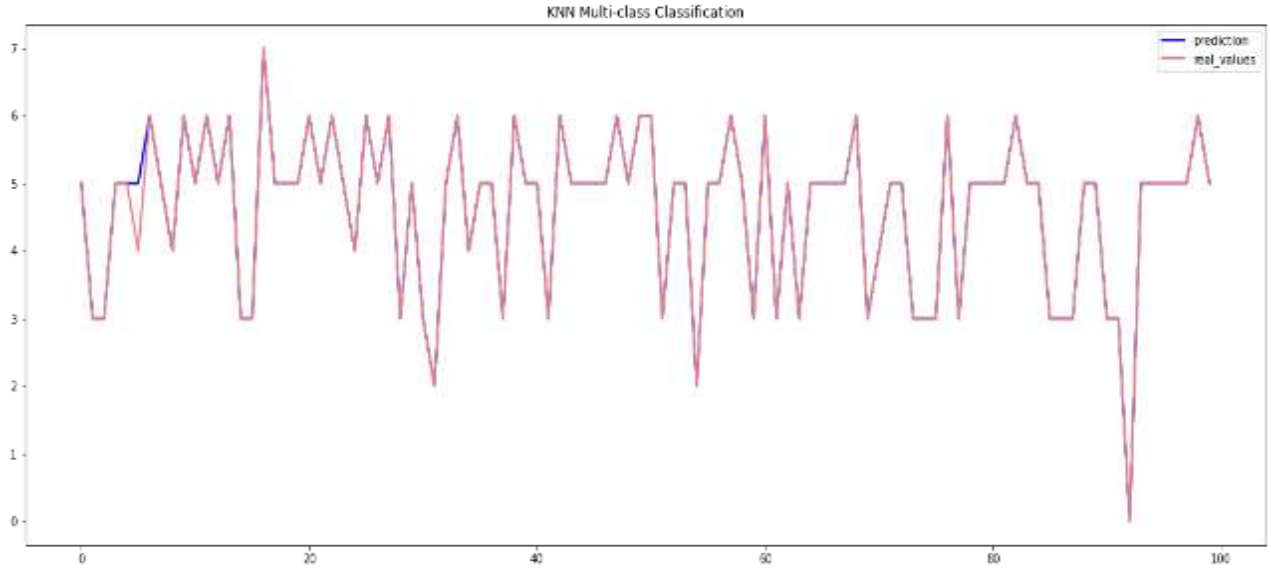

Figure 16. *KNN Plot for Multi-Class Classification Between Actual and Predicted Data*

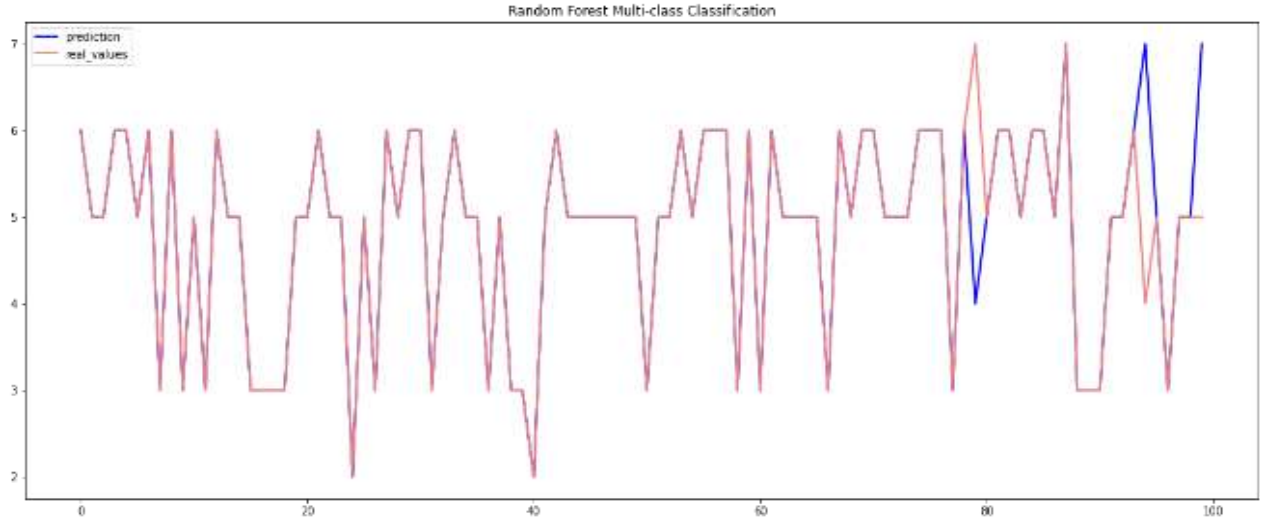

Figure 17. *RF Plot for Multi-Class Classification Between Actual and Predicted Data*

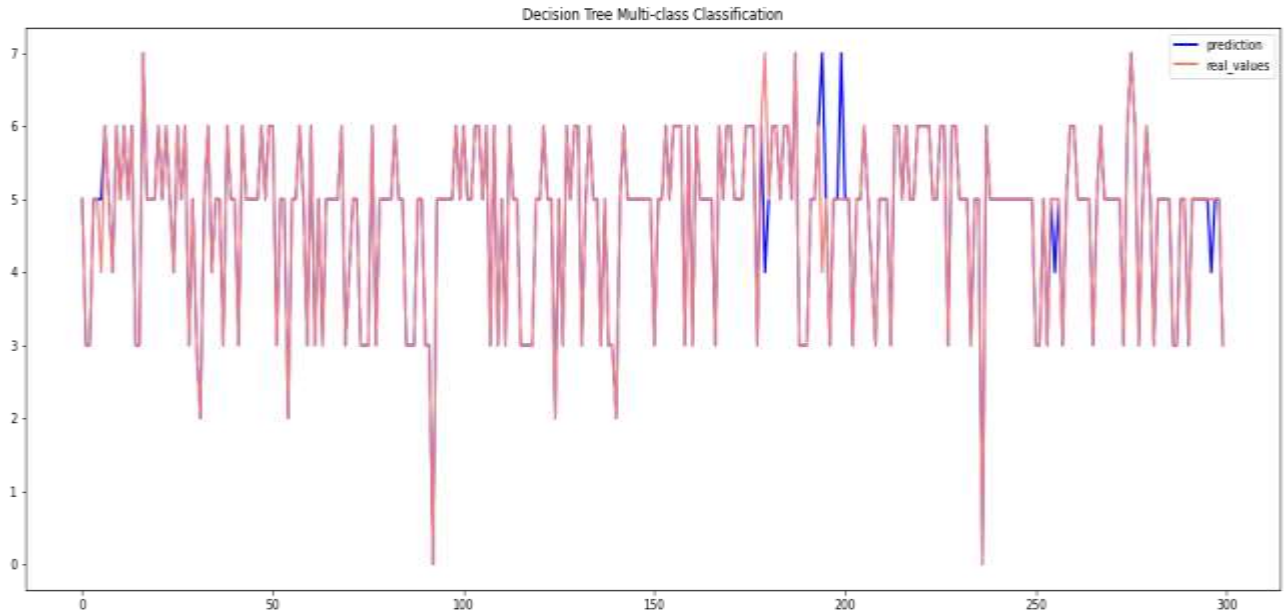

Figure 18. *DT Plot for Multi-Class Classification Between Actual and Predicted Data*

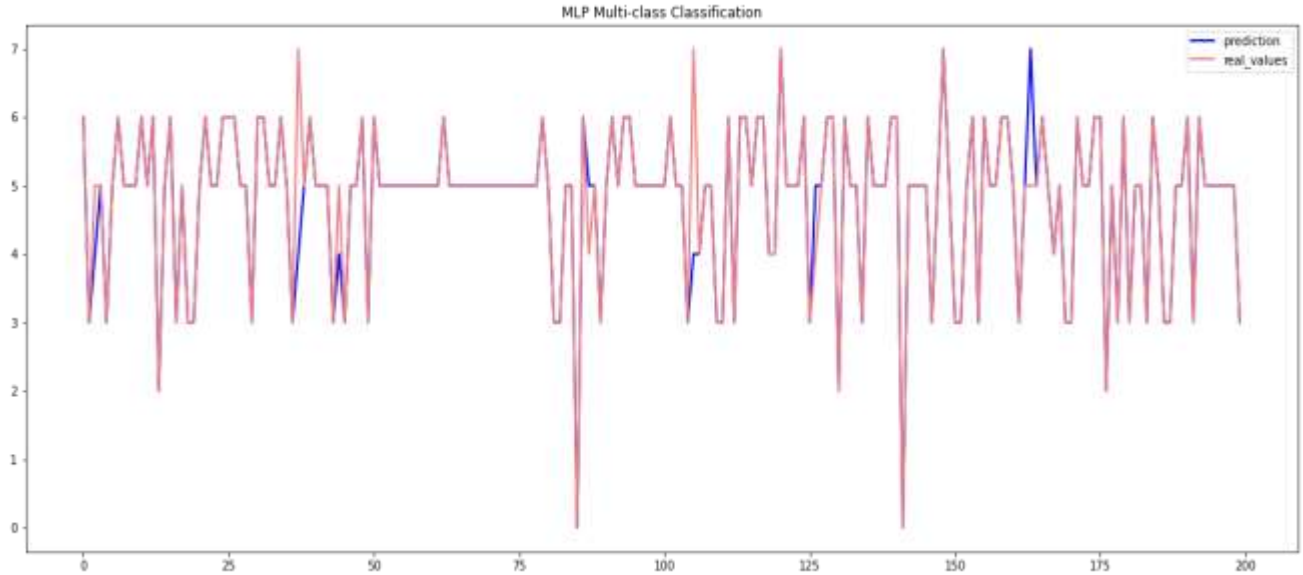

Figure 19. *MLP Plot for Multi-Class Classification Between Actual and Predicted Data*

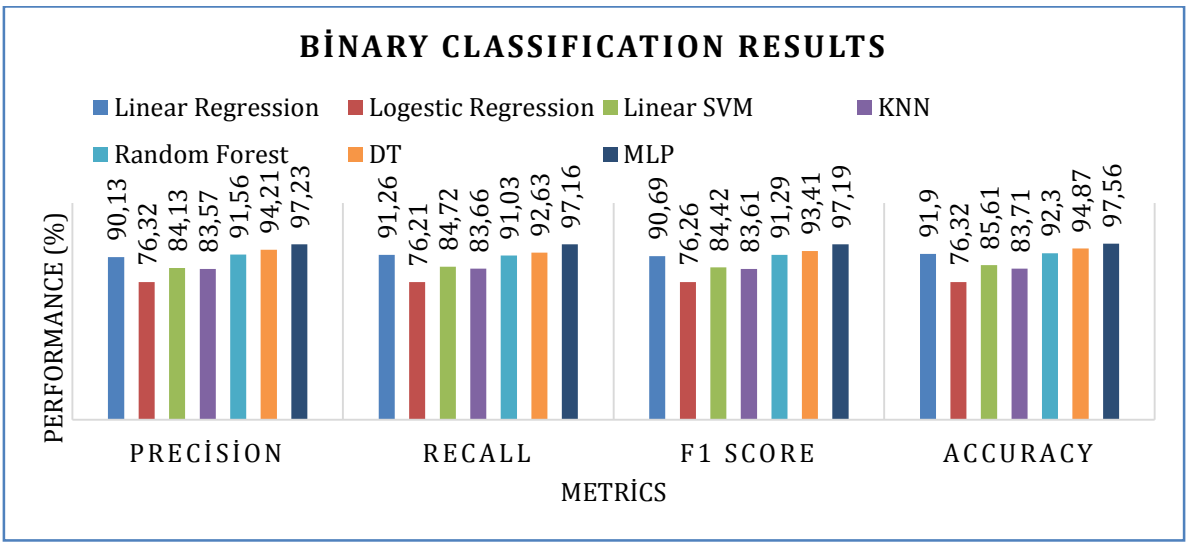

Figure 20. *Binary Classification Performance of the Models in Securing IoT Use Cases*

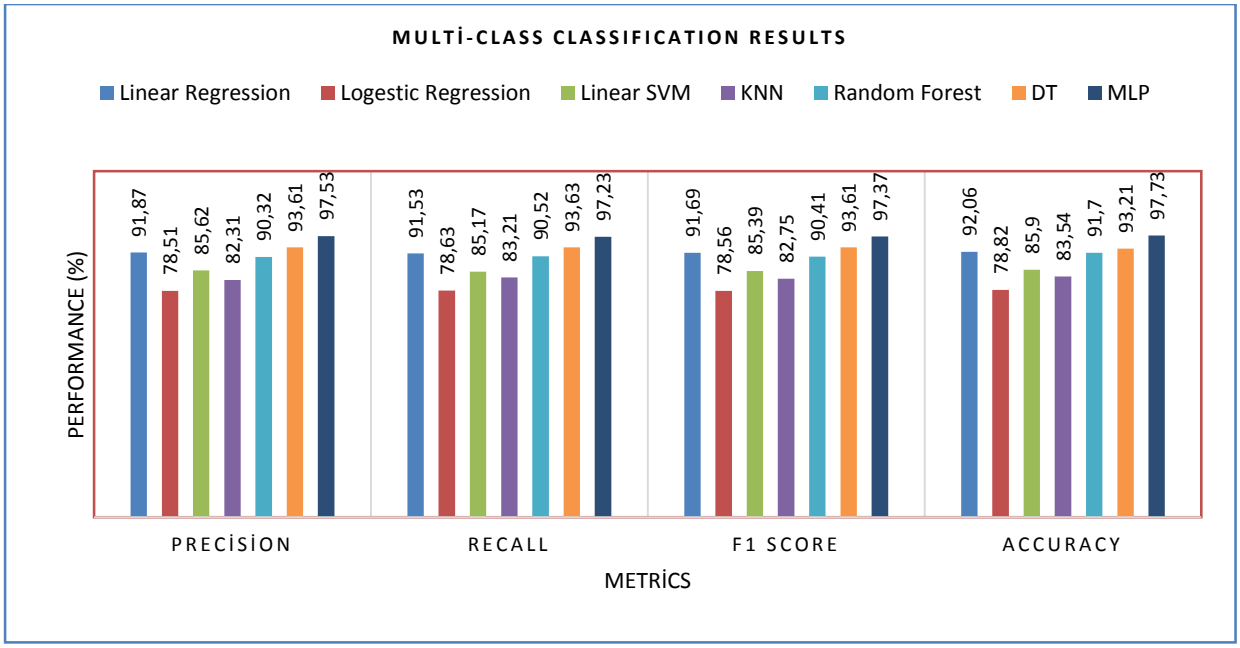

Figure 21. *Multi-Class Classification Performance of the Models in Securing IoT Use Cases*

The consistent performance across multiple metrics further validates its reliability for real-world applications, making it suitable for IoT-based security solutions.

Figure 21 is the outcome of the multi-class classification highlight the comparative performance of various machine learning models applied to the UNSW-NB15 dataset for securing IoT use cases. The proposed Multi-Layer Perceptron (MLP) framework demonstrates superior performance across all evaluated metrics, making it the most effective model in handling complex multi-class classification tasks. The precision achieved by the MLP is 97.53%, reflecting its high capability to correctly identify true positive instances with minimal false positives. Similarly, its recall value of 97.23% underscores the framework's ability to capture the majority of relevant instances, minimizing false negatives. The F1-score for the MLP framework, calculated at 97.37%, highlights its balanced performance by harmonizing precision and recall. This metric validates the MLP's consistency and robustness in multi-class scenarios. Furthermore, the model achieves the highest accuracy of 97.73%, demonstrating its capability to correctly classify network traffic events across all classes. In comparison, In terms of precision, recall, and F1-score measures, Random Forest and Decision Tree models exhibit strong performance. closely trailing the MLP framework. However, these models fail to match the MLP in handling the intricate patterns within the dataset.

Again, other models do an average of the job (Moderate performance) with Logistic Regression getting a fairly low score because it tries to model non-linear relationships in a linear way. The extremely low performance of Linear Regression over all metrics illustrates its unsuitability for this kind of multi-class classification problem. In addition, these results further confirm The efficacy of the suggested MLP framework, especially in the case of IoT security applications where multi-class classification is crucial for identifying different attack types. MLP clearly outperforms Random Forest over several metrics, and this demonstrates MLP's capacity to learn and process non-linear relationships, making it a suitable candidate to manage complexity around network security datasets. Hence, it emerges as the best solution to mitigate the problems related to the intrusion detection in IoT scenarios.

Discussions

Although the boom of IoT devices has brought about an era of great change, it has also laid bare some of the most fundamental weaknesses in the foundations of network security. However, most of the conventional IDS have been inefficient in classifying the multi-dimensional nature of the attacks in real-time because of the complexity and high dimensionality of the data produced by IoT devices. Because traditional machine learning models use statistical analysis, they cannot identify intricate patterns leading to multiple forms of attacks, which gives an inadequate detection rate. We review of the contemporary techniques to expose the shortcomings including: (1) limited scalability, (2) multi-class classification inadequacy, (3) lack of a generic frameworks that can adapt to dynamic attack scenarios. These challenges call for new deep learning methods to improve the IDS detection and

classification capabilities. To address these gaps, we propose a new methodology that uses a deep learning (MLP-based) framework. In addition to the binary classification tasks, the MLP treats nonlinear relationships and utilizes high-dimensional features, making it appropriate for multi-class classification models, unlike other traditional models. The methodology presents novel features such as a very well-structured pre-processing pipeline, normalization of the entire feature set, and advanced ensemble learning techniques for comparative analysis. In addition, cross-validation will make sure that our evaluation is robust, and data visualization will help us understand the model performances.

The outcomes indicate the effectiveness of the proposed MLP framework with maximal accuracy, precision, recall, and F1-score for both binary and multi-class classification scenarios. This suggests that the MLP not only overcomes the limitation of the traditional models but also offers a scalable solution which can deal with the complexity of IoT network traffic. Closing these gaps in the state-of-the-art provides a foundation for deploying more robust IDS in real-world IoT settings. This research has important implications, not only providing a simple technique to improve the security of IoT but also establishing a benchmark for future intrusion detection research. Finally, Section 4.1 presents the limitations of the current study and possible avenues for further investigation and improvement. IoT has been used and applied in different fields [52-59].

Limitations of the Study

This study, however, has limitations. To begin with, the MLP framework suggested in this study depends on extremely costly training, limiting its usability among low-resource IoT areas. Second, the UNSW-NB15 dataset contains a large variety of attack butcannot cover all trending attacks, leading to the limitations of the model's generalizability in newly emerged covert channels [45]. Finally, the method is mainly based on offline analysis and is not evaluated under real-time performance in a dynamic IoT environment. The above limitations will be addressed in our future work to enable large-scale implementation of the proposed framework, enabling it to adapt to new threats, and apply within real-time settings.

4. Conclusions

To overcome the drawbacks of the intrusion detection systems dedicated to IoT environments, this research presented a framework based on deep learning with a Multi-Layer Perceptron (MLP). The framework provides a 4G version, which outperforms existing methods in problems involving both binary and multi-class classification, owing to automated preprocessing pipelines, resilient feature normalization and scalable model training. These results suggest that the complexity of IoT network traffic is solvable with high MLP accuracy, precision, recall, and F1-score when used with the UNSW-NB15 dataset. Compared to traditional machine learning models, the results also emphasize how effectively the proposed method overcomes the gaps present in the state-of-the-art approaches. The study recognizes some limitations, such as the high computational complexity of MLP, the limited set of records assuming they cover all emerging threats, and the inability to check in real-time. These limitations can be tackled in future work by improving the efficiency of the proposed framework to fit the resource constraints of IoT devices, by enabling online learning for the detection of threats in real time, and by using datasets that evolve to imitate the appearance of new attack vectors. This research has important implications in the area of IoT security and presenting an efficient solution for cyber threat detection and classification. Scalability, real-time adaptability, and generalizability will be future improvement directions to ensure broad applicability for secure IoT ecosystems against advanced cyber weapons.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Ahmed, Ejaz; Yaqoob, Ibrar; Hashem, Ibrahim Abaker Targio; Khan, Imran; Ahmed, Abdelmuttlib Ibrahim Abdalla; Imran, Muhammad and Vasilakos, Athanasios V. (2017). The role of big data analytics in

the Internet of Things. *Computer Networks*. doi:10.1016/j.comnet.2017.06.013

[2] Banerjee, Amit. (2020). Emerging trends in IoT and big data analytics for biomedical and health care technologies. *Handbook of Data Science Approaches for Biomedical Engineering.* 121–152. doi:10.1016/B978-0-12-818318-2.00005-2

[3] Adi, Erwin; Anwar, Adnan; Baig, Zubair; Zeadally, Sherali. (2020). Machine learning and data analytics for the IoT. *Neural Computing and Applications*. pp.14A3RE. doi:10.1007/s00521-020-04874-y

[4] Tien, James M. (2017). Internet of Things, Real-Time Decision Making, and Artificial Intelligence. *Annals of Data Science*. 4(2):149–178. doi:10.1007/s40745-017-0112-5

[5] Ur Rehman, Muhammad Habib; Yaqoob, Ibrar; Salah, Khaled; Imran, Muhammad; Jayaraman, Prem Prakash; Perera, Charith. (2019). The role of big data analytics in industrial Internet of Things. *Future Generation Computer Systems*. 1-40. doi:10.1016/j.future.2019.04.020

[6] Ahmed, Ejaz; Yaqoob, Ibrar; Hashem, Ibrahim Abaker Targio; Khan, Imran; Ahmed, Abdelmuttlib Ibrahim Abdalla; Imran, Muhammad; Vasilakos, Athanasios V. (2017). The role of big data analytics in Internet of Things. *Computer Networks*. 1-22. 12doi:10.1016/j.comnet.2017.06.013

[7] Ghosh, Ashish; Chakraborty, Debasrita; Law, Anwesha. (2018). Artificial Intelligence in Internet of Things. *CAAI Transactions on Intelligence Technology*. 1-11. doi:10.1049/trit.2018.1008

[8] Atitallah, Safa Ben; Driss, Maha; Boulila, Wadii; Ghaczala, Henda Ben. (2020). Leveraging Deep Learning and IoT big data analytics to support the smart cities development: Review and future directions. *Computer Science Review*. 38:1–29. doi:10.1016/j.cosrev.2020.100303

[9] Sarker, Iqbal H.; Hoque, Mohammed Moshiul; Uddin, Md. Kafil; Alsanoosy, Tawfeeq. (2020). Mobile Data Science and Intelligent Apps: Concepts, AI-Based Modeling and Research Directions. *Mobile Networks and Applications*. 1–19. doi:10.1007/s11036-020-01650-z

[10] Efpraxia D. Zamani, Conn Smyth, Samrat Gupta, Denis Dennehy. (2023). Artificial intelligence and big data analytics for supply chain resilience: a systematic literature review. *Annals of Operations Research*. 327:605–632. https://doi.org/10.1007/s10479-022-04983-y

[11] Gupta, Rajesh; Tanwar, Sudeep; Tyagi, Sudhanshu; Kumar, Neeraj. (2020). Machine Learning Models for Secure Data Analytics: A taxonomy and threat model. *Computer Communications*. 1–36. doi:10.1016/j.comcom.2020.02.008

[12] Iqbal, Rahat; Doctor, Faiyaz; More, Brian; Mahmud, Shahid; Yousuf, Usman. (2018). Big data analytics: Computational intelligence techniques and application areas. *Technological Forecasting and Social Change*. 1–13. doi:10.1016/j.techfore.2018.03.024

[13] Elijah, Olakunle; Rahman, Tharek Abdul; Orikumhi, Igbafe; Leow, Chee Yen; Hindia, MHD Nour. (2018). An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges. *IEEE Internet of Things Journal*. 1–17. doi:10.1109/JIOT.2018.2844296

[14] Valentin Kuleto, Milena Ili´c, Mihail Dumangiu, Marko Rankovi´c, O. (2021). Exploring Opportunities and Challenges of Artificial Intelligence and Machine Learning in Higher Education Institutions. *MDPI*. 13(18):1-16. https://doi.org/10.3390/su131810424

[15] Amira Bourechak, Ouarda Zedadra, Mohamed Nadjib Kouahla and Antonio Guer. (2023). At the Confluence of Artificial Intelligence and Edge Computing in IoT-Based Applications: A Review and New Perspectives. *MDPI*. 1-49.

[16] Jie Chen; L. Ramanathan; Mamoun Alazab. (2021). Holistic big data integrated artificial intelligent modeling to improve privacy and security in data management of smart cities. *Microprocessors and Microsystems.* 1–17. doi:10.1016/j.micpro.2020.103722

[17] Alrowaily, Mohammed; Lu, Zhuo. (2018). Secure Edge Computing in IoT Systems: Review and Case Studies. *IEEE*. 440–444. doi:10.1109/SEC.2018.00060

[18] Saumyaranjan Sahoo. (2021). Big data analytics in manufacturing: a bibliometric analysis of research in the field of business management. *International Journal of Production Research*. 1–30. doi:10.1080/00207543.2021.1919333

[19] Gill, Sukhpal Singh; Tuli, Shreshth; Xu, Minxian; Singh, Inderpreet; Singh, Karan Vijay; Lindsay, Dominic; Tuli, Shikhar; Smirnova, Daria; Singh, Manmeet; Jain, Udit; Pervaiz, Haris; Sehgal, Bhanu; Kaila, Sukhwinder Singh; Mishra, Sanjay; Aslanpour, Mohammad Sadegh; Mehta, Harshit; Stankovski, Vlado; Garraghan, Peter. (2019). Transformative Effects of IoT, Blockchain and Artificial Intelligence on Cloud Computing: Evolution, Vision, Trends and Open Challenges. *Internet of Things*. 1–33. doi:10.1016/j.iot.2019.100118

[20] Berk Kaan Kuguoglu, Haiko van der Voort and Marijn Janssen. (2021). The Giant Leap for Smart Cities: Scaling Up Smart City Artificial Intelligence of Things (AIoT) Initiatives. *MDPI*. 13(21):1-16. https://doi.org/10.3390/su132112295

[21] Abderahman Rejeb, Karim Rejeb, Horst Treiblmaier, Andrea Appolloni. (2023). The Internet of Things (IoT) in healthcare: Taking stock and moving forward. *Internet of Things.* 22:1-23. https://doi.org/10.1016/j.iot.2023.100721

[22] Jitendra Bhatia, Kiran Italiya, Kuldeepsinh Jadeja, Malaram Kumhar. (2023). An Overview of Fog Data Analytics for IoT Applications. *MDPI*. 23(1):1-31. https://doi.org/10.3390/s23010199

[23] Supriya M. and Vijay Kumar Chattu. (2021). A Review of Artificial Intelligence, Big Data, and Blockchain Technology Applications in Medicine and Global Health. *MDPI*. 5(3):1-20. https://doi.org/10.3390/bdcc5030041

[24] Mishra, Sushruta (2020). Analysis of the role and scope of big data analytics with IoT in health care domain. *Handbook of Data Science Approaches for Biomedical Engineering*. 1–23. doi:10.1016/B978-0-12-818318-2.00001-5

[25] Tanwar, Sudeep; Bhatia, Qasim; Patel, Pruthvi; Kumari, Aparna; Singh, Pradeep Kumar; Hong, Wei-Chiang. (2020). Machine Learning Adoption in Blockchain-Based Smart Applications: The Challenges, and a Way Forward. *IEEE Access*. 8:474–488. doi:10.1109/access.2019.2961372

[26] Zhang, J. Z., Srivastava, P. R., Sharma, D., and Eachempati, P. (2021). Big data analytics and machine learning: A retrospective overview and bibliometric analysis. *Expert Systems with Applications*. 184:115561. doi:10.1016/j.eswa.2021.115561

[27] Antonio João Gonçalves de Azambuja, Christian Plesker, Klaus Schützer. (2023). Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. *MDPI*. 12(8):1-18. https://doi.org/10.3390/electronics12081920

[28] Mariani, Marcello M.; Fosso Wamba, Samuel (2020). Exploring how consumer goods companies innovate in the digital age: The role of big data analytics companies. *Journal of Business Research*. 121:338–352. doi:10.1016/j.jbusres.2020.09.012

[29] Frederick J. Riggins and Samuel Fosso Wamba. (2015). Research Directions on the Adoption, Usage, and Impact of the Internet of Things through the Use of Big Data Analytics. *Hawaii International Conference on System Sciences*. 1-10. DOI: 10.1109/HICSS.2015.186

[30] Shah, Syed Attique; Seker, Dursun Zafer; Hameed, Sufian; Draheim, Dirk. (2019). The Rising Role of Big Data Analytics and IoT in Disaster Management: Recent Advances, Taxonomy and Prospects. *IEEE Access*. 1–1. doi:10.1109/ACCESS.2019.2913340

[31] Misra, N. N.; Dixit, Yash; Al-Mallahi, Ahmad; Bhullar, Manreet Singh; Upadhyay, Rohit; Martynenko, Alex. (2020). IoT, big data and artificial intelligence in agriculture and food industry. *IEEE Internet of Things Journal*. 1–19. doi:10.1109/JIOT.2020.2998584

[32] Bag, Surajit; Pretorius, Jan Ham Christiaan; Gupta, Shivam; Dwivedi, Yogesh K. (2020). Role of institutional pressures and resources in the adoption of big data analytics powered artificial intelligence, sustainable manufacturing practices and circular economy capabilities. *Technological Forecasting and Social Change*. 1–14. doi:10.1016/j.techfore.2020.120420

[33] Zaidan, A. A.; Zaidan, B. B. (2018). A review on intelligent process for smart home applications based on IoT: coherent taxonomy, motivation, open challenges, and recommendations. *Artificial Intelligence Review*. 1–24. doi:10.1007/s10462-018-9648-9

[34] Anawar, Muhammad Rizwan; Wang, Shangguang; Azam Zia, Muhammad; Jadoon, Ahmer Khan; Akram, Umair; Raza, Salman. (2018). Fog Computing: An Overview of Big IoT Data Analytics. *Wireless Communications and Mobile Computing*. 1–22. doi:10.1155/2018/7157192

[35] Singh, Saurabh; Sharma, Pradip Kumar; Yoon, Byungun; Shojafar, Mohammad; Cho, Gi Hwan; Ra, In-Ho. (2020). Convergence of Blockchain and Artificial Intelligence in IoT Network for the Sustainable Smart City. *Sustainable Cities and Society*. 1–23. doi:10.1016/j.scs.2020.102364

[36] Chhabra, Gurpal Singh; Singh, Varinder Pal; Singh, Maninder. (2018). Cyber forensics framework for big data analytics in IoT environment using machine learning. *Multimedia Tools and Applications*. 1–20. doi:10.1007/s11042-018-6338-1

[37] Winter, Jenifer; Ono, Ryota. (2015). The Future Internet Algorithmic Discrimination: Big Data Analytics and the Future of the Internet. 10.1007/978-3-319-22994-2 (Chapter 8):125–140. doi:10.1007/978-3-319-22994-2_8

[38] Juan M. Górriz, et. al. (2020). Artificial intelligence within the interplay between natural and artificial Computation: advances in data science, trends and applications. Neurocomputing. 410:237-270. doi:10.1016/j.neucom.2020.05.078

[39] M. Bublitz, Frederico; Oetomo, Arlene; S. Sahu, Kirti; Kuang, Amethyst; X. Fadrique, Laura; E. Velmovitsky, Pedro; M. Nobrega, Raphael; P. Morita, Plinio. (2019). Disruptive Technologies for Environment and Health Research: An Overview of Artificial Intelligence, Blockchain, and Internet of Things. *International Journal of Environmental Research and Public Health*. 16(20):1–24. doi:10.3390/ijerph16203847

[40] Ramalingam, Hariharan; Venkatesan, V.Prasanna. (2019). Conceptual analysis of Internet of Things use cases in Banking domain. *Conference: TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON)*. 34–2039. doi:10.1109/TENCON.2019.8929473

[41] Smail Benzidia;Naouel Makaoui;Omar Bentahar; (2021). The impact of big data analytics and artificial intelligence on green supply chain process integration and hospital environmental performance. *Technological Forecasting and Social Change*. 1–13. doi:10.1016/j.techfore.2020.120557

[42] Iqbal H. Sarker. (2022). AI-Based Modeling: Techniques, Applications and Research Issues Towards Automation, Intelligent and Smart Systems. *SN Computer Science*. 3(158):1-20. https://doi.org/10.1007/s42979-022-01043-x

[43] Zakria Qadira, Khoa N. Lea , Nasir Saeedb , Hafiz Suliman Munawar. (2023). Towards 6G Internet of Things: Recent advances, use cases, and open challenges. *ICT Express*. 9(2):296-312. DOI:10.1016/j.icte.2022.06.006

[44] Yuxin Li, Jizheng Yi1, Huanyu Chen1 and Duanxiang Peng. (2021). Theory and application of artificial intelligence in financial industry. *Data Science in Finance and Economics*.1(2):96-116. DOI:10.3934/DSFE.2021006

[45] Paul, Anand; Ahmad, Awais; Rathore, M. Mazhar; Jabbar, Sohail. (2016). Smartbuddy: defining human behaviors using big data analytics in social internet of things. *IEEE Wireless Communications*. 23(5):68–74. doi:10.1109/MWC.2016.7721744

[46] Kakatkar, Chinmay; Bilgram, Volker; Füller, Johann (2019). Innovation analytics: Leveraging artificial intelligence in the innovation process. *Business Horizons*. 1–11. doi:10.1016/j.bushor.2019.10.006

[47] Mahdavinejad, Mohammad Saeid; Rezvan, Mohammadreza; Barekatain, Mohammadamin;

Adibi, Peyman; Barnaghi, Payam; Sheth, Amit P. (2017). Machine learning for Internet of Things data analysis: A survey. *Digital Communications and Networks*. 1–57. doi:10.1016/j.dcan.2017.10.002

[48] Ravesa Akhter;Shabir Ahmad Sofi. (2021). Precision agriculture using IoT data analytics and machine learning. *Journal of King Saud University - Computer and Information Sciences*. 1–39. doi:10.1016/j.jksuci.2021.05.013

[49] lv, zhihan; Song, Houbing; Basanta-Val, Pablo; Steed, Anthony; Jo, Minho (2017). Next-Generation Big Data Analytics: State of the Art, Challenges, and Future Research Topics. *IEEE Transactions on Industrial Informatics*. 1–9. doi:10.1109/TII.2017.2650204

[50] Goel, Pankaj; Datta, Aniruddha; Mannan, M. Sam (2017). Application of big data analytics in process safety and risk management. *2017 IEEE International Conference on Big Data (Big Data)*. 1143–1152. doi:10.1109/BigData.2017.8258040

[51]Moustafa, M., & Slay, J. (2015). UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15). *Harvard Dataverse*. https://doi.org/10.7910/DVN/OGDUHB

[52]D, jayasutha. (2024). Remote Monitoring and Early Detection of Labor Progress Using IoT-Enabled Smart Health Systems for Rural Healthcare Accessibility. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.672

[53]Ponugoti Kalpana, L. Smitha, Dasari Madhavi, Shaik Abdul Nabi, G. Kalpana, & Kodati , S. (2024). A Smart Irrigation System Using the IoT and Advanced Machine Learning Model: A Systematic Literature Review. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.526

[54]J. Anandraj. (2024). Transforming Education with Industry 6.0: A Human-Centric Approach . *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.732

[55]N. Vidhya, & C. Meenakshi. (2025). Blockchain-Enabled Secure Data Aggregation Routing (BSDAR) Protocol for IoT-Integrated Next-Generation Sensor Networks for Enhanced Security. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.722

[56]Alkhatib, A., Albdor , L., Fayyad, S., & Ali, H. (2024). Blockchain-Enhanced Multi-Factor Authentication for Securing IoT Children's Toys: Securing IoT Children's Toys. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.417

[57]P. Jagdish Kumar, & S. Neduncheliyan. (2024). A novel optimized deep learning based intrusion detection framework for an IoT networks. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.597

[58]Vutukuru, S. R., & Srinivasa Chakravarthi Lade. (2025). CoralMatrix: A Scalable and Robust Secure Framework for Enhancing IoT Cybersecurity. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.825

[59]Iqbal, A., Shaima Qureshi, & Mohammad Ahsan Chishti. (2025). Bringing Context into IoT: Vision and Research Challenges. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.760