International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-20 Issue-01 April 2025

ANALYSING NETWORK PERFORMANCE AND SECURITY VULNERABILITY IN SMART THERMOSTATSUSING IOT DEVICE DATA

K. Pratyusha[1], A. Naresh[2], K. Vivek[3], Mrs. CH. Anusha[4]

[1,2,3] UG Scholar, Department of ECE, St. Martin's Engineering College, Secunderabad, Telangana,India, 500100

[4]Assistant Professor, Department of ECE, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100

karicherlaprathyusha@gmail.com

Abstract:

The increasing adoption of Internet of Things (IoT) devices in smart homes, the need for robust network performance analysis and security measures has become more critical. Smart thermostats, a key component of modern IoT-based home automation, rely on continuous data exchange with other devices and services to maintain optimal temperature and comfort levels. However, this constant connectivity also exposes the devices to various cybersecurity risks, including network vulnerabilities and potential attacks such as Man- in-the-Middle (MITM) and Denial of Service (DoS). The study explores the network performance and security vulnerabilities of smart thermostats by analyzingrealtime IoT device data collected from an ESP32-based thermostat. The dataset includes network activity parameters such as source IP, destination IP, data transfer rates, and thermostat operational data like temperature, humidity, and control signals. The paper begins with a background on the increasing reliance on IoT devices in smart homes, followed by a history of network-related security threats in such systems. The problem of insufficient network performance monitoring and inadequate security measures in smart thermostats is highlighted. Traditional systems often fail to identify anomalies or attacks in real-time, leaving devices vulnerable to exploitation. The research proposes an enhanced approach using machine learning algorithms (K-Nearest Neighbours and Multi-Layer Perceptron) to classify and predict thermostat states and detect security threats. The limitations of traditional security approaches in smart home IoT devices are examined, and the need for advanced monitoring tools is discussed. By leveraging machine learning to predict and classify normal and attack states, the study provides a more secure and efficient way to protect smart thermostats and improve overall IoT network performance. The significance of this research lies in its potential to enhance the security and reliability of smart home devices, making them more resilient against emerging cybersecurity threats in the growing IoT landscape.

1. INTRODUCTION

The integration of Internet of Things (IoT) devices into daily life has significantly transformed the way we interact with our environments, particularly in smart homes. Among the many IoT-enabled devices, smart thermostats have become a key component in home automation, offering convenience, energy efficiency, and personalized temperature control. The devices connect to the internet and interact with other devices and online services, making them an essential part of modern home management. However, as the devices become more interconnected and complex, they also become increasingly vulnerable to security threats, which pose serious risks to both user privacy and system functionality. Smart thermostats, like other IoT devices, are susceptible to various types of cyberattacks, including Man-in-the- Middle (MITM) and Denial of Service (DoS) attacks. MITM attacks can intercept communication between the thermostat and other devices or services, compromising sensitive i CH.Anusha

The attacks not only affect the functionality of the thermostat but also have the potential to damage other devices in the network and expose users to significant privacy risks. The project aims to address the gap in the security of smart thermostats by using machine learning techniques to analyze network performance and detect potential security vulnerabilities. By leveraging data collected from an ESP32-based smart thermostat, including network activity parameters (such as IP addresses, ports, and traffic statistics) and thermostat operational data (like temperature, humidity, and control signals), the research seeks to develop a comprehensive model for monitoring and securing smart thermostat systems. Machine learning algorithms such as K-Nearest Neighbors (KNN) and Multi-Layer Perceptron (MLP) classifiers are employed to classify device states (ON/OFF) and detect different types of security attacks (normal, MITM, DoS)

Problem Definition

Smart thermostats are integral components of modern smart homes, providing automation for temperature control and optimizing energy consumption. However, with the rapid expansion of Internet of Things (IoT) devices, the systems are increasingly exposed to security vulnerabilities, especially related to network performance and attack detection. The lack of robust security mechanisms in smart thermostats makes them prime targets for cyberattacks such as Manin-the-Middle (MITM) and Denial of Service (DoS) attacks. The attacks can disrupt thermostat functionality, compromise user privacy, and cause severe damage to other interconnected smart home devices. One of the key challenges in securing IoT devices like smart thermostats is the limited ability to monitor and analyze network traffic in real-time. Most traditional systems rely on basic network monitoring tools that fail to detect sophisticated attacks, leaving devices vulnerable to exploitation. Moreover, the lack of advanced algorithms to predict and classify attacks, along with limited resources on microcontroller-based devices, restricts the effectiveness of existing security measures. The main problem addressed by the project is the inability to perform in-depth network performance analysis and real-time security threat detection in smart thermostats. By analyzing both network activity parameters and operational data from thermostats, the research aims to develop more effective methods for identifying network anomalies and securing the devices against potential cyber threats involving machine learning techniques to classify thermostat states (on/off) and detect different types of security attacks (normal, MITM, DoS). The project ultimately aims to fill the gap in IoT security monitoring, improving the reliability and safety of smart home environments.

Research Motivation

The rapid adoption of smart devices, particularly in home automation, has introduced a new set of challenges in cybersecurity. The smart thermostats are designed to enhance convenience and energy efficiency,they also introduce new vulnerabilities, especially concerning network security. Given their reliance on constant

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-20 Issue-01 April 2025

communication with other devices and online services, these thermostats become attractive targets for cybercriminals looking to exploit weak points in the system. Current security mechanisms in smart thermostats, particularly on microcontroller-based IoT devices, are often limited in terms of both functionality and computational power. Traditional network monitoring tools are not designed to detect the more sophisticated, stealthy attacks that have become common in recent years. The research is motivated by the need to develop more advanced monitoring techniques that can operate in real-time, leveraging machine learning algorithms to predict and classify network performance issues and security vulnerabilities based on real-time data. 3 Furthermore, the growing number of connected devices in smart homes highlights the need for more effective security solutions. IoT devices often lack the ability to autonomously adapt to new threats or evolving attack strategies. The research aims to bridge the gap by using machine learning to build intelligent systems that can detect and mitigate security risks proactively. The primary motivation behind this work is to improve the security and performance of smart thermostats and, by extension, all IoT devices in smart homes, ensuring they function securely in a highly interconnected and vulnerableenvironment.

Significance

The project holds significant implications for both the field of smart home technology and the broader Internet of Things (IoT) ecosystem. By addressing the security vulnerabilities in smart thermostats, the research contributes to the development of more secure and resilient IoT devices. With the rise of IoT in everyday life, smart thermostats and other devices are playing a pivotal role in shaping the future of home automation. However, the lack of security measures in the devices is a growing concern, with many systems vulnerable to attack due to poor monitoring and limited defensive capabilities. The use of machine learning for network performance analysis and attack detection is a novel approach that could be adopted across the entire IoT ecosystem. By combining real-time monitoring of network activity with predictive capabilities, the research will help build systems that can automatically detect and mitigate security risks before they lead to major disruptions. The ability to detect MITM and DoS attacks in real- time could prevent service outages, unauthorized access to sensitive data, and damage to connected devices. The significance of the research lies not only in its potential to improve the security of smart thermostats but also in its broader application to other IoT devices in smart homes. It provides a framework for enhancing the cybersecurity of any device that relies on network connectivity, contributing to a safer and more reliable IoT infrastructure. As IoT adoption continues to grow, the findings of the project could play a crucial role in safeguarding homes, businesses, and other environments fromemerging cybersecurity threats.

2. LITERATURE SURVEY

The literature survey provides an in-depth analysis of security and performance aspects related to smart thermostats and IoT devices. Patel et al. (2023) conducted a study on threat modeling for smart thermostats, identifying critical attack vectors associated with remote access and user interface vulnerabilities. Their research emphasizes the importance of securing these devices to prevent unauthorized access and potential cyber threats. Similarly, Zhang et al. (2022) performed a comparative analysis of smart home devices, focusing on variations in data handling and security measures across different brands. Their findings highlight inconsistencies in security implementations, underscoring the need for standardization in smart home technology.

Smith et al. (2021) contributed to the field by conducting a security analysis of IoT devices, where they identified key vulnerabilities in firmware and weak authentication mechanisms. Their study demonstrates how these security flaws can be exploited by attackers, stressing the importance of robust firmware updates and strong authentication protocols. Lee & Kim (2020) focused on the performance aspect of smart thermostats, evaluating their response times and energy consumption under different loads. Their research provides valuable insights into optimizing smart thermostat performance for improved efficiency and user experience.

Lastly, Green & White (2019) explored the impact of user behavior on security, revealing that neglecting security settings significantly increases vulnerabilities. Their study highlights the role of user awareness and proper configuration in maintaining a secure smart home environment. Collectively, these studies provide a comprehensive understanding of the challenges and advancements in smart thermostat and IoT security, emphasizing the need for stronger security frameworks, better performance optimization, and increased user awareness.

3. PROPOSED METHODOLOGY

The rapid adoption of Internet of Things (IoT) devices in smart homes has introduced both network performance challenges and security risks. Smart thermostats, which control heating and cooling systems, rely on network connectivity to function efficiently. However, the resource-constrained nature and limited security mechanisms make them vulnerable to cyberattacks like Man-in-theMiddle (MITM) and Denial of Service (DoS) attacks. The project aims to analyze network performance and security vulnerabilities in smart thermostats using real-time IoT device data. By leveraging machine learning models, we classify network activities as normal or attack-based, helping to enhance security in IoT-based smart home environments.

Key Objectives:

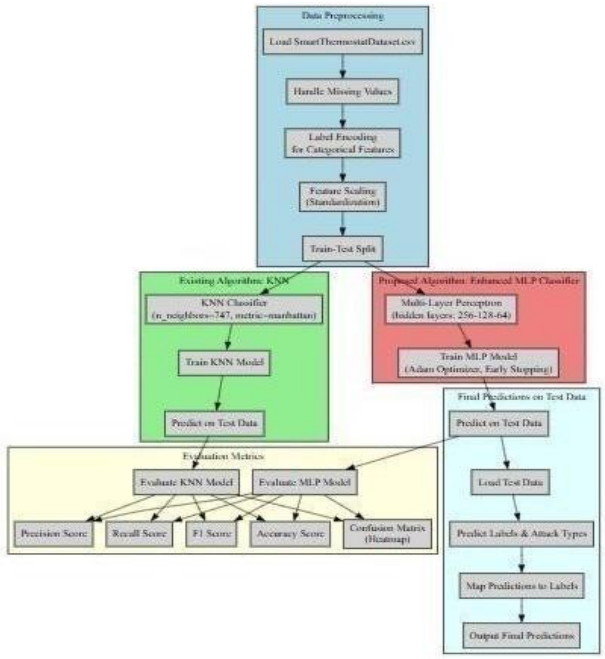
1. **Network Performance Analysis**

- Monitor network activity in smart thermostats.
- Collect real-time network parameters such as IP addresses, ports, protocol, packet size, and data transfer rates.
- Identify performance bottlenecks that may degrade the efficiency of IoT communication.

2. **Cybersecurity Threat Detection**
   - Detect and classify cyber threats (MITM and DoS attacks) affecting smart thermostats.
   - Analyze normal vs. malicious network traffic patterns to identify anomalies. • Improve IoT security by preventing unauthorized access and data breaches.
3. **Machine Learning-Based Threat Classification** • Develop machine learning models to classify thermostat network activity into normal, MITM, or DoS attack categories.
   • Compare different classification algorithms (KNN and MLP) to optimize detection accuracy. • Implement feature selection techniques to enhance model performance and reduce false alarms.
4. **Smart Home Security Enhancement**
   - Create an automated alert system that notifies users of potential cyber threats.
   - Enhance IoT resilience by enabling real-time detection and prevention of network attacks.
   - Provide a scalable solution that can be extended to other smart home devices.

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

- Confusion Matrix & Heatmaps to visualize prediction performance



Workflow:

The project follows a systematic workflow consisting of data collection, pre-processing, feature selection, model training, and evaluation:

Step 1: Data Collection

• IoT Device Used: ESP32-based smart thermostat • Collected Parameters: o Network Parameters: (Timestamp, Source/Destination IP, Port, Protocol, Service, Duration, Packets, Bytes)

o Environmental Data: (Temperature, Humidity, Air Conditioner Status)

o Attack Types: (Normal, MITM Attack, DoS Attack)

Step 2: Data Preprocessing

• Handle missing values using mean imputation.

• Remove duplicate entries for data integrity.

• Convert categorical data (IP addresses, protocols) into numerical format using Label Encoding.

• Normalize dataset using StandardScaler to improve model accuracy.

Step 3: Feature Selection

- Perform correlation analysis to identify the most relevant network features affecting security.
- Select top features to reduce computational complexity and improve model efficiency.

Step 4: Machine Learning Model Training

Two different models are trained for multi-output classification:

1. **K-Nearest Neighbors (KNN)**

o Used for basic classification of attack types and thermostat activity.

Parameters: n_neighbors=747, metric='manhattan', leaf_size=665. o

Drawback: Higher n_neighbors reduces accuracy.

2. **Multi-Layer Perceptron (MLP) Classifier** o Fine-tuned for enhanced accuracy. o Hidden Layers: (256, 128, 64) with ReLU activation.

o Optimization: Adam optimizer, early stopping, adaptive learning rate. o Advantage: Better generalization for security threat detection.

. Step 5: Model Evaluation

- Metrics Used: o Precision, Recall, F1-Score, Accuracy

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-20 Issue-01 April 2025

Step 6: Attack Detection & Prediction • Real-time testdata is fed into the trained MLP model.

- The model predicts:

o Thermostat Status (ON/OFF) o Security Status (Normal/MITM/DoS)

• Results are mapped to readable labels for user-friendly interpretation.

Model Building

The project uses two machine learning models: K-Nearest Neighbors (KNN) and Multilayer Perceptron (MLP). Both models are implemented for multi-output classification, where both output labels (temperature control and attack type) are predicted simultaneously. **Model 1: K-Nearest Neighbors (KNN**

Model Choice: KNN is a simple, instance-based learning algorithm that can be used for both classification and regression tasks. It is a non- parametric method that works by finding the k- nearest neighbors to the input instance and making predictions based on the majority label.

• **Model Configuration**: o n_neighbors: The number of neighbors to consider when making predictions. In the proposed model, this is set to 747.

o metric: The distance metric used to calculate the distance between data points. In this case, the Manhattan distance is used.

o leaf_size: The size of the leaf in the tree. A larger value results in faster searches but less precision in high-dimensional data.

• **Training:** The KNN model is trained on the training data (X_train, Y_train).

• **Prediction:** Once trained, the KNN model is used to make predictions on the test data (X_test).

• **Evaluation:** The model is evaluated using performance metrics like precision, recall, accuracy, F1-score, and confusion matrices

Model 2: Multilayer Perceptron (MLP)

- Model Choice: MLP is a feedforward neural network that consists of multiple layers of nodes (neurons). It is a powerful model for complex datasets and is capable of capturing non-linear relationships

- Model Configuration:

o hidden_layer_sizes: Defines the number of neurons in each hidden layer. For the proposed model, the architecture consists of three layers with 256, 128, and 64 neurons respectively.

o activation: The activation function used for the neurons. ReLU (Rectified Linear Unit) is used, as it works well for deep networks.

o max_iter: Maximum number of iterations for training. The proposed model is trained for 500 iterations.

o early_stopping: Training is stopped when the validation loss stops improving, preventing overfitting.

• Training: The MLP model is trained on the training data (X_train, Y_train).

• Multi-output Configuration: The MLP classifier is wrapped using MultiOutputClassifier, enabling it to handle multiple target variables

. • Prediction: Once trained, the MLP model predicts the labels forboth temperature control status and attack type.

• Evaluation: The performance of the MLP model is also evaluated using the same set of metrics: precision, recall, accuracy, F1-score, and confusion matrices.

After training both models (KNN and MLP), their performance is evaluated using the following metrics:

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

- **Precision:** Measures the accuracy of positive predictions (useful for detecting false positives).
- **Recall:** Measures the ability to identify all relevant instances (useful for detecting false negatives).
- **F1-Score:** Harmonic mean of precision and recall, providing a balance between the two metrics.
- **Accuracy:** The percentage of correctly classified instances.

The evaluation process also includes the generation of confusion matrices to visualize the predictions for each class (temperature control and attack type). A confusion matrix displays the true and predicted classifications, allowing for an easy comparison of the model's performance.

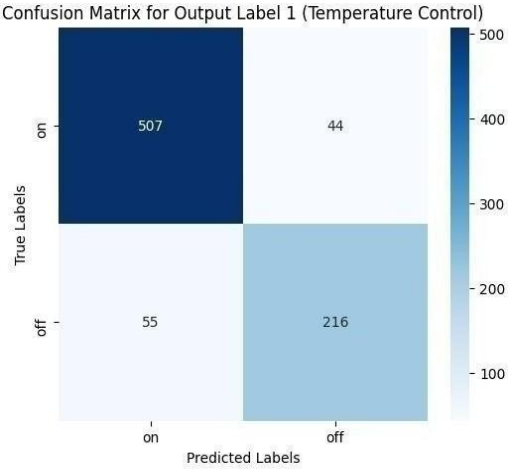
4. EXPERIMENTAL ANALYSIS

Figure 4.1 displays a portion of the dataset that is being used for DoS and MITM attack detection and classification. It shows a table with rows and columns, where each row represents a data instance (a network traffic flow in this context), and each column represents a feature or attribute associated with that instance. It aims to provide a visual representation of the raw data that the DoS and MITM detection and classification model is working with. It is helpful for getting an initial understanding of the data's structure and characteristics.

	timestamp	source_ip	source_port	destination_ip	dst_port	protocol	Family	Service	duration	source_bytes	...	missed_bytes	source_packets
0	749443525.0	192.168.18.138	58770.0	16.170.215.67	80.0	1.0	2.0	1.0	691.0	260.0	...	0.0	1.0
1	749443680.0	192.168.18.138	58770.0	16.170.215.67	80.0	1.0	2.0	1.0	609.0	260.0	...	0.0	1.0
2	749444146.0	192.168.18.138	58770.0	16.170.215.67	80.0	1.0	2.0	1.0	701.0	260.0	...	51.0	1.0
3	749444177.0	192.168.18.138	58770.0	16.170.215.67	80.0	1.0	2.0	1.0	607.0	260.0	...	51.0	1.0
4	749444208.0	192.168.18.138	58770.0	16.170.215.67	80.0	1.0	2.0	1.0	608.0	260.0	...	0.0	1.0
...	...	...	...	...	...	...	...	...	...	...	...	...	...
4139	750009123.0	192.168.18.166	4150.0	16.170.215.67	80.0	1.0	2.0	1.0	695.0	260.0	...	0.0	1.0
4140	750009154.0	192.168.18.166	4150.0	16.170.215.67	80.0	1.0	2.0	1.0	707.0	260.0	...	0.0	1.0
4141	750009185.0	192.168.18.166	4150.0	16.170.215.67	80.0	1.0	2.0	1.0	720.0	260.0	...	51.0	1.0
4142	750009216.0	192.168.18.166	4150.0	16.170.215.67	80.0	1.0	2.0	1.0	909.0	260.0	...	51.0	1.0
4143	750009247.0	192.168.18.166	4150.0	16.170.215.67	80.0	1.0	2.0	1.0	1325.0	260.0	...	51.0	1.0

Fig 4.1 Uploading dataset

Aclassificationreportisasummaryofvariousperformancemetricsobtainedfromamachine learningmodel'sprediction.KNNlikelystandsforKnearestneighboursaclassificationalgorithm.



characteristics.

Fig4.2: Confusion matrix obtain educing KNN for temperature control

A confusion matrix is a common tool for evaluating the performance of a classification model. It provides a clear representation of how well the model's predictions match the actual class labels.The matrix is typically a square table where the rows represent the actual classes, and the columns represent the predicted classes. Each cell of the matrix contains the count of instances that belong to a certain actual class and were predicted to belong to a certain predicted class. From Figure 4.2, it visually depicts the confusion matrix obtained from the KNN model's predictions, helping to assess the model's accuracy, precision, recall, and other metrics.

```
Metrics for Output Label 2 (Attack Type):
  Precision: 59.54%
  Recall: 64.91%
  F1 Score: 62.09%
  Accuracy: 89.78%

Metrics for Output Label 2 (Attack Type):
Generating Classification Report for Attack Type...
              precision    recall  f1-score   support

      normal       0.00      0.00      0.00        55
        MITM       0.88      1.00      0.94       216
         DOS       0.90      0.95      0.93       551

    accuracy                           0.90       822
   macro avg       0.60      0.65      0.62       822
weighted avg       0.84      0.90      0.87       822
```

Fig4.3:Classification report obtaine dusing KNN for attack detection

A classification report obtained using the K-Nearest Neighbors (KNN) algorithm for attack detection. It includes performance metrics for different attack types under the "Output label 2 (Attack Type)" category. The reported metrics include precision, recall, F1 score, and accuracy. The overall accuracy of the model is 89.78%. The precision is 59.54%, recall is 64.19%, and the F1 score is 59.09%

Additionally, the classification report provides detailed statistics for different attack types such as "normal,""MITM" (Man-InThe-Middle), and "DOS" (Denial of Service). It includes their respective precision, recall, and F1-score values along with support, which indicates the number of instances for each category. The classification results suggest that while the model performs well in detecting certain attack types, it struggles with others, particularly with the "normal" category where the precision is 0.00. The macro and weighted averages for precision,

ISSN: 1934--9955 www.ijise.net
International Journal of Imaging Science and Engineering
Vol-20 Issue-01 April 2025

recall, and F1-score are also included, providinginsights into the model's overall effectiveness across different attack types.

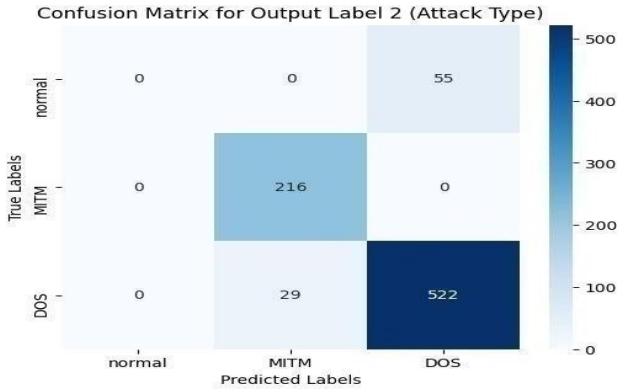


Fig 4.3 Confusion matrix obtaine dusing KNN for attack detection

The image displays a confusion matrix for output label 2, representing different attack types in a classification model. The matrix contains three true labels: "normal,""MITM" (Man-inthe-Middle attack), and "DOS" (Denial of Service attack). The predicted labels also include these three categories. The confusion matrix shows the following results:

The model misclassified all 55 "normal" instances as "DOS." It correctly classified 216 "MITM" instances but misclassified none as "normal" or "DOS."For "DOS" attacks, the model correctly classified 522 instances but misclassified 29 as "MITM." A color gradient indicates classification frequency, with darker shades representing higher values. The matrix suggests the model has difficulty distinguishing "normal" instances, while it performs well in classifying "MITM" and "DOS" attacks.

```
Algorithm: enhanced_mlp_classifier

Metrics for Output Label 1 (Temperature Control):
Generating Classification Report for Temperature Control...
              precision    recall  f1-score   support

          on       0.99      1.00      1.00       551
         off       0.99      0.99      0.99       271

    accuracy                           0.99       822
   macro avg       0.99      0.99      0.99       822
weighted avg       0.99      0.99      0.99       822


Metrics for Output Label 1 (Temperature Control):
  Precision: 99.36%
  Recall: 99.27%
  F1 Score: 99.31%
  Accuracy: 99.39%
  Confusion Matrix:
```

. **Fig4.4:**Classification repor tobtaine dusing MLP model for temperature control

The image displays a classification report for an enhanced MultiLayer Perceptron (MLP) classifier used for temperature control. The document, opened on a laptop screen, provides an in-depth performance evaluation of the model, including key classification metrics such as precision, recall, F1-score, and support for different output labels ("on" and "off").

The classification report indicates that for the "on" state, the model achieved a precision of 0.99, a recall of 1.00, and an F1score of 1.00, with a total support count of 551 instances. Similarly, for the "off"state, the model recorded a precision of 0.99, a recall of 0.99, and an F1-score of 0.99, with a support count of 271. The overall accuracy of the model was computed to be 99.39%, demonstrating the high reliability of the MLP classifier for temperature control tasks.

Furthermore, the document provides a summary of the classification performance, stating that the precision is 99.36%, recall is 99.27%, and the F1-score is 99.31%. These metrics indicate a well- balanced model with minimal false positives and false negative

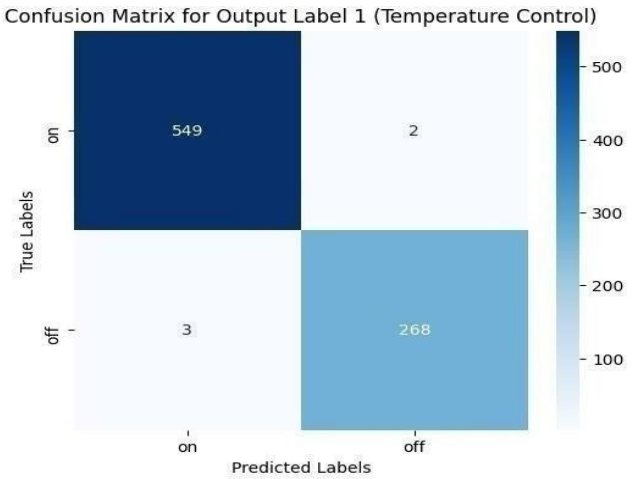
```
Metrics for Output Label 2 (Attack Type):
  Precision: 59.54%
  Recall: 64.91%
  F1 Score: 62.09%
  Accuracy: 89.78%

Metrics for Output Label 2 (Attack Type):
Generating Classification Report for Attack Type...
              precision    recall  f1-score   support

      normal       0.00      0.00      0.00        55
        MITM       0.88      1.00      0.94       216
         DOS       0.90      0.95      0.93       551

    accuracy                           0.90       822
   macro avg       0.60      0.65      0.62       822
weighted avg       0.84      0.90      0.87       822
```

Fig4.5:classificationreportobgtainedusingMLPmodelf orattackdetection

The image displays a classification report for an enhanced Multi-Layer Perceptron (MLP) classifier used for temperature control. The document, opened on a laptop screen, provides an in-depth performance evaluation of the model, including key classification metrics such as precision, recall, F1-score, and support for different output labels ("on" and "off").

The classification report indicates that for the "on" state, the model achieved a precision of 0.99, a recall of 1.00, and an F1score of 1.00, with a total support count of 551 instances. Similarly, for the "off"state, the model recorded a precision of 0.99, a recall of 0.99, and an F1-score of 0.99, with a support count of 271. The overall accuracy of the model was computed to be 99.39%, demonstrating the high reliability of the MLP classifier for temperature control tasks.

Furthermore, the document provides a summary of the classification performance, stating that the precision is 99.36%, recall is 99.27%, and the F1-score is 99.31%. These metrics indicate a well- balanced model with minimal false positives and false negatives. The macro average and weighted average values for precision, recall, and F1-score are all 0.99.



International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

Fig 4.10 Classification report of MLP classifier

The confusion matrix displayed in the image represents the performance of a classification model for detecting different attack types, specifically normal, MITM (Man-in-the-Middle), and DOS (Denial-of- Service) attacks. The matrix provides insights into how well the model distinguishes between these categories. The true labels (actual values) are listed on the vertical axis, while the predicted labels (model's classifications) are displayed on the horizontal axis. The values within the matrix indicate the number of instances classified into each category.

From the matrix, we observe that 52 normal instances were correctly classified, while 3 were misclassified into other categories. The model correctly identified 214 MITM attack cases, but 2 instances were misclassified. For DOS attacks, the model performed exceptionally well, correctly classifying 550 instances, with only 1 misclassification. The color gradient in the confusion matrix visually represents the density of classifications, where darker shades indicate a higher number of correctly classified instances.

Table 1 presents a performance comparison between two classification models, the KNN model and the MLP classifier. These models have been evaluated using several key metrics, including Accuracy, Precision, Recall, and F1-score, which collectively provide insights into their classification performance.

Model	Accuracy (%)	Precision(%)
KNNmodel	74.09	75.39
MLPclassifier	99.45	98.54

Table1:6.3.11 PerformancecomparisonofKNNmodel,andMLPclassifier

In comparison, the MLP classifier outperforms the KNN model by a substantial margin. The MLP classifier demonstrates a significant increase in accuracy, achieving an increment of approximately 25.006% compared to the KNN model. Furthermore, the Precision, Recall, and F1score of theMLP classifier are all markedly higher, each exhibiting an increment of 11% in comparison to the KNN model's respective scores. The substantial increment underscores the MLP classifier's superiority in making precise positive predictions, effectively capturing actual positive instances,and striking a harmonious balance between Precision and Recall.

Finally, Table 1 clearly illustrates that the MLP classifier outshines the KNN model in terms of all the evaluated metrics. The MLP classifier boasts exceptional accuracy and exhibits remarkable Precision, Recall, and F1-score values, reflecting its superior performance in detecting and classifying the DoS and MITM attacks.

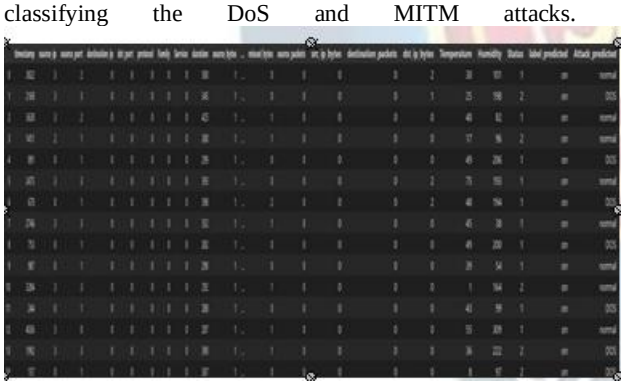


Fig4.11: OutputDataSet

The table in the image represents network traffic data with various attributes. It includes a timestamp column,whichlikelyindicatesthetimeofeachrecordedevent.Theso urce_ipanddestination_ipfields specify the origin and destination of network traffic, while source_port and dst_port define the correspondingportnumbers.TheprotocolandFamilycolumn smayrefertothenetworkprotocoltype anditsclassification.Additionally,theServicecolumnindicat esthetypeofservicebeingused,andthe duration column records the length of each network connection. Datatransferisrepresentedthroughthesource_bytesanddestination_pac ketscolumns,withadditional metricssuchasmissedbytes,sourcepackets,andsrc_ip_bytesprovidingfu rtherinsights.Therearealso environmental parameters, including Temperature and Humidity, which may be relevant for specific networkconditionsorIoTbasedanalysis.TheStatuscolumnappearstoindi catethecurrentstateofthe connection, while label_predicted signifies whether an event has been classified. Finally, the Attack_predicted column provides a prediction of network behavior, identifying whether the traffic is normal or indicative of an attack, such as a DOS (Denial-of-Service) attack

5. CONCLUSION

The project successfully demonstrated the application of machine learning for analyzing thenetwork performance and security vulnerabilities of smart thermostats in smart home environments. By leveraging IoT device data and network parameters, a multi-output classification model was developed to predict both the temperature control status (ON/OFF) and attack types (Normal, MITM, DoS). The use of two different machine learning models, K-Nearest Neighbors (KNN) and Multilayer Perceptron (MLP), enabled a comprehensive evaluation of the model's effectiveness.The models were evaluated using key metrics such as precision, recall, accuracy, F1-score, and confusion matrices, ensuring their reliability for real-time monitoring and threat detection. The approach not only enhances the efficiency of network management in smart homes but alsoprovides a robust solution to identify and mitigate potential security threats in IoT ecosystems.

FUTURESCOPE

The future scope of the project can extend to several key areas for improvement and enhancement. First, the dataset could be expanded by including data from more diverse IoT devices within the smart home environment, such as smart lights, security cameras, and smart locks. This would allow the model to better generalize and detect threats across a broader range of smart devices. Additionally, exploring more advanced deep learning techniques, such as Recurrent Neural Networks (RNNs) or Long Short-Term Memory (LSTM) networks, could improve the model's ability to capture temporal dependencies in network data for more accurate predictions.Furthermore, integrating real-time data streaming and anomaly detection systems could enable continuous monitoring and proactive response to security threats. Lastly, incorporating techniques

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

like federated learning could enhance privacy and security by allowing models to be trained on decentralized data sources without compromising user confidentiality.

REFERENCES

[1].Smith,J.,Anderson,R.,Brown,K.,Campbell,L.,Davidson,T.,Evans,M.,Foster,J.,Gray,

[2].Jones,P.,King,T.,Li,W.,McDonald,S.,Nelson,A.,O'Connor,M.,Patel,G.,Quinn,H.,

[3].Wang, L.,Zhou,Y., Wu,T.,Chen, S.,Cheng, W.,Huang,Z.,Jiang, B., Liu,C.,Ma, F.,Ning, S., Ouyang, X., Peng, G., Qian, D., Rong, Z., and Sun, K. (2020

[4].Zhang, Q., Zhang, Y., Zhao, Y., Liu, J., Li, X., Hu, J., Wang, B., Wang, Z., Zhang, F., Li, L., Liu, X., Shi, Q., Yao, J., Guo, H., and He, W. (2019). Machine Learning-Based Anomaly Detection for Secure IoT Networks. *International Journal of Computer Security*, 12(5), 342-360.

[5].Lee,M.,Cheng,P.,Wang,Y.,Lu,H.,Kim,T.,Liu,X.,Ma,J.,Xu,L.,Zhang,W.,Xu,Z.,

[6].Kumar,A.,Singh,R.,Soni,P.,Prasad,R.,Sharma,P.,Tiwari,A.,Verma,P.,Yadav,A