Emerging Trends in Digital Transformation

Volume-1, Issue-2, July 2025 ISSN:**3107-4308** *Paper ID:* ***ETDT-V1-I2-24***

EFFICIENT DETECTION OF IOT BOTNET ATTACKS USING A HYBRID ML MODEL

KHUTEJA NAZLEE, M.Tech, Dept of CSE,
Mrs. Y. SUSHEELA, Associate Professor, Department of CSE,
Vaageswari College of Engineering (Autonomous), Karimnagar, Telangana.

ABSTRACT: In response to the growing Internet of Things (IoT) environment, numerous new security hazards have emerged. This article provides a practical approach to identifying botnet intrusions on the Internet of Things. The methodology implements a hybrid machine learning framework. The complexity of botnet-based attacks increases as the number of devices implicated increases. Device vulnerabilities can be exploited to conduct directed denial of service (DDoS) attacks and other forms of harm. Traditional detection systems are incapable of accommodating the dynamic nature of these threats as a result of their dependence on immutable models or rules that are managed by a single algorithm.

In order to circumvent these challenges, the proposed methodology integrates both supervised and unsupervised machine learning methodologies. It employs clustering techniques to identify anomalies and decision tree features to facilitate processes. Publicly available datasets, such as Bot-IoT and CICIDS, are employed to train and validate models. The hybrid model surpasses individual classifiers in terms of precision, recall, and F1-scores.

Index Terms: *Internet of Things (IoT), Botnet Detection, Machine Learning (ML), Hybrid Model, Anomaly Detection, Intrusion Detection System (IDS), Network Security, Cybersecurity, Supervised Learning, Unsupervised Learning, DDoS Attack, Traffic Classification.*

1. INTRODUCTION

The proliferation of the Internet of Things (IoT) has enabled the development of numerous items, including smart residential devices and critical infrastructure components. This development has resulted in a greater number of alternatives available to cybercriminals. Fraudsters frequently target IoT devices due to their inadequate security protocols and processing capabilities. The development and distribution of botnets, which are networks of infected devices that are under the control of perpetrators, is a prevalent and severe issue in this region. These botnets are instrumental in the planning of malicious activities, such as data intrusions, Distributed Denial-of-Service (DDoS) attacks, and network disruptions.

Traditional cybersecurity strategies are confronted with novel threats from botnet attacks on the Internet of Things. These attacks can rapidly alter their behavior to imitate lawful traffic patterns in order to evade detection by traditional rule-based or signature-based systems. The already challenging task of developing security standards is further complicated by the vast array of Internet of Things (IoT) devices and locations. Static models or isolated machine learning algorithms are not always as effective in the long term due to their inability to adapt to new, unanticipated attack vectors. As a result, there is a pressing need for sophisticated, scalable detection technologies that can detect botnet activity in real time across a variety of IoT environments.

There is considerable interest in the utilization of machine learning (ML) techniques to identify botnet assaults on IoT networks. Algorithms that have been trained with machine learning are capable of identifying intricate patterns in network traffic and even the smallest anomalies, both of which may indicate hostile activity. Supervisory learning methodologies, including decision trees and support vector machines, have demonstrated considerable proficiency in classification tasks when provided with labeled data. Clustering and anomaly detection are examples of unsupervised learning techniques that can be used to identify new or emergent hazards, even in the absence of labeled data. The complex and ever-changing IoT circumstances present unique challenges for each machine learning technique when implemented independently.

In this study, we examine a hybrid ML model that can circumvent these constraints by combining the adaptive capabilities of unsupervised learning with the predictive capabilities of supervised learning. The proposed model aims to enhance the efficiency and robustness of botnet attack detection on the Internet of Things by integrating the two methodologies. The hybrid framework validates hazardous behaviors by employing trained supervised

DOI : *https://doi.org/10.5281/zenodo.16811125*

models for pattern classification and clustering to identify anomalies in unlabeled data. This two-stage method enhances detection efficacy by reducing false positives and improving generalizability to new attack scenarios. The model's performance is compared to that of more conventional detection methods using enormous IoT botnet datasets.

The hybrid design that has been proposed is not only technically effective but also meets the practical requirements of modern IoT ecosystems due to its scalability, low latency, and compatibility with existing network infrastructures. The model's emphasis on real-time, cost-effective traffic analysis enables delayed responses to potential hazards. Future research will focus on intelligent cybersecurity solutions that are data-centric, adaptable, and based on machine learning. This is accomplished by employing a groundbreaking botnet detection technique that enhances the security of the Internet of Things.

2. LITERATURE REVIEW

Sharma, P., & Rao, M. (2020). This investigation employs neural network models to integrate client behavior data in order to forecast short-term demand. The authors create a model that integrates behavioral variables, such as utilization patterns and preferences, into the prediction mechanism. This is necessary because traditional forecasting methods frequently fail to account for the unique consumption behaviors of individuals. Load forecasting is enhanced by the utilization of artificial neural networks (ANNs) to identify nonlinear consumer behavior-energy consumption correlations. This investigation demonstrates that consumer behavior enhances short-term load forecasting models, a critical component of energy management and power system planning.

Zhang, X., Wang, J., & Li, Y. (2020). This investigation proposes the utilization of hybrid machine learning to detect botnet incursions on smart home IoT networks. The model identifies detrimental actions that conventional security measures fail to detect by combining machine learning techniques. The hybrid method is capable of detecting botnet attacks by analyzing network traffic patterns and device behaviors. Intelligent and adaptable security solutions are essential in the rapidly evolving field of smart home technologies, where IoT devices have introduced new threats. The proposed approach enhances cybersecurity by precisely and efficiently detecting botnet activity in smart residences.

Ahmed, M., Mahmood, A. N., & Hu, J. (2020). This article examines a diverse array of network anomaly detection technologies in order to guarantee cybersecurity. In their article, the authors discuss the advantages and disadvantages of statistical methods, machine learning algorithms, and hybrid models. Anomaly detection is a challenging task due to the evolving structure of network data and the complexity of contemporary cyber threats. It also encompasses the accessibility of datasets, real-time detection, and feature selection. This paper is beneficial for researchers and practitioners who are developing anomaly detection systems that are more effective. This is due to its comprehensive analysis of previous methodologies.

Gupta, R., & Kumar, A. (2021). The authors introduce a hybrid deep learning model that integrates LSTM and CNN networks to identify botnet activity in IoT contexts. The long short-term memory (LSTM) component captures temporal correlations, while the convolutional neural network (CNN) component obtains spatial information from network traffic data. This enables the model to assess intricate botnet activity patterns. This combination enhances detection by enhancing data interpretation. This research demonstrates that hybrid strategies are the most effective method of safeguarding IoT networks from botnet attacks.

Khan, S., & Lee, Y. (2021). This investigation introduces an ensemble learning system for the purpose of identifying IoT botnet attacks. The ensemble technique enhances resilience and accuracy by utilizing numerous machine learning classifiers to capitalize on the distinctive characteristics of each model. A comparison is made between the bagging and boosting ensemble approaches for the purpose of detecting botnets in this study. In the defense of IoT systems, ensemble models outperform individual classifiers. The authors underscore the importance of collaborative learning in order to address the intricate and constantly evolving cyber threats associated with the Internet of Things (IoT).

Li, H., Zhang, K., & Li, Q. (2021). In this investigation, feature selection methodologies and deep learning models are implemented to identify botnet activity in IoT networks. The most critical features of network traffic data are identified during the feature selection process. The functionality of the model is enhanced by reducing its dimensionality. A deep learning model is trained to classify traffic as either good or evil based on the specified attributes. The hybrid technique underscores the significance of feature selection in IoT cybersecurity solutions by enhancing detection efficiency and accuracy.

DOI : *https://doi.org/10.5281/zenodo.16811125*

Singh, G., & Kaur, P. (2022). The authors assert that a hybrid machine learning system is capable of identifying IoT botnet attacks. The framework employs a diverse array of machine learning techniques to detect suspect botnet patterns in network data. The model employs both supervised and unsupervised learning to mitigate cyber risks and address the fluidity of IoT networks. The hybrid design is scalable and efficient for IoT network security, as demonstrated by the research, with low false-positive rates and high detection accuracy.

Chen, L., Wang, J., & Zhao, Q. (2022). The hybrid detection method described in this paper, which employs autoencoders and random forest classifiers, simplifies the process of detecting IoT botnet intrusions. Normal network data structure is captured by the autoencoder component through unsupervised learning for outlier detection. After identification, the random forest classifier infers anomaly damage. This divided procedure enhances false positives and detection. The research demonstrates that the development of dependable IoT cybersecurity solutions is feasible through the application of deep learning and ensemble methods.

Patel, S., & Joshi, P. (2022). These authors propose a hybrid detection method that employs SVM and neural networks to identify IoT botnet activities. The neural network component identifies intricate nonlinear relationships, while the support vector machine (SVM) component manages high-dimensional data and establishes optimal decision boundaries. The model's generalizability and detection accuracy are significantly enhanced by the integration of these two methods. This investigation demonstrates the efficacy of hybrid strategies in safeguarding IoT networks from sophisticated botnet attacks.

Zhang, Y., Wu, Q., & Xie, L. (2023). This study introduces a hybrid deep learning model that employs attention processes to identify botnet incursions in IoT networks. The spatial and temporal information from network traffic data is extracted by the model using CNNs and LSTM networks. The accuracy of model detection is enhanced by the attention mechanism, which prioritizes the most critical input data. The research demonstrates that the proposed technique can safeguard IoT systems by detecting botnet activities.

Wang, S., & Liu, Y. (2023). The authors introduce a hybrid model that employs gradient boosting and CNN to identify IoT botnet attacks. CNNs extract features from network traffic data. These features are employed in gradient boosting classification. Detection is enhanced by ensemble methods and deep learning. The research demonstrates that hybrid IoT security strategies are effective.

Sharma, V., & Singh, M. (2023). The authors introduce a hybrid ensemble model for the detection of IoT botnet activity. This model employs decision tree techniques and LSTM networks. LSTM identifies long-term correlations in network traffic data, whereas decision trees provide unambiguous categorization criteria. The model boasts exceptional endurance and detection accuracy as a result of the utilization of multiple methods. Ensemble hybrid models may enhance the cybersecurity of IoT, according to this investigation.

Tan, J., & Yang, X. (2024). This investigation recommends the utilization of deep learning models and feature extraction to identify botnet intrusions in IoT networks. The feature extraction procedure is used to identify critical network traffic properties. To categorize, we input these attributes into a deep learning model. This approach simplifies computation and enhances detection accuracy. Deep learning and feature engineering are demonstrated in the work as a means of securing the Internet of Things.

Kumar, N., & Roy, S. (2024). The authors suggest a hybrid machine learning architecture that employs Random Forest classifiers and MLP neural networks to identify botnet activity in IoT networks. Random Forest is interpretable and identifies intricate data patterns, whereas MLP generates dependable classifications. Solo methods are outperformed by hybrid models in terms of false positive rates and detection on benchmark IoT botnet datasets. In complex IoT systems that are susceptible to botnet attacks, the research indicates that deep learning and ensemble learning enhance threat detection.

Mehta, R., & Das, A. (2024). Using a hybrid deep learning model that integrates RNNs and CNNs, this investigation identifies IoT botnets in real time. Convolutional neural network (CNN) layers derive spatial information from network traffic data, while regression neural network (RNN) layers, particularly LSTM units, capture temporal trends. The program is capable of identifying sophisticated botnet behaviors that evolve as a result of the combination of these factors. The real-time simulation of the model resulted in a high detection accuracy and low latency, rendering it appropriate for IoT systems. This research facilitates the implementation of cybersecurity safeguards that are more adaptable and effective in the context of existing IoT infrastructures.

3. RELATED WORK

EXISTING SYSTEM

DOI : *https://doi.org/10.5281/zenodo.16811125*

At now, urban road network extraction makes use of the usual suspects in machine learning, exploratory deep learning, and image processing. The edge detection (Canny, Sobel) and thresholding (Otsu's, adaptive) methods both face difficulties in noisy, barrier-filled, and unpredictable road conditions environments. Morphological approaches can improve road efficiency, but they can be difficult to apply in complex scenarios. The requirement to manually acquire a range of named datasets and attributes makes Random Forest and Support Vector Machines less than ideal in all cases. If we want to make roads look like they do from somewhere else, we can use unsupervised methods like K-means and Gaussian Mixture Models. A lot of work may have to go into tailoring graph-based methods like the Minimum Spanning Tree (MST) so they work in cities with different systems. Despite its promise to improve roadside aesthetics, the dynamic contour model has a number of drawbacks, such as a sensitivity to noise and sharp edges. It is nevertheless helpful to incorporate OpenStreetMap (OSM), even when the data is incorrect and out of date. The labor-intensive nature of GIS-based approaches makes them unsuitable for large-scale mapping. No fine-grained features were present in the first CNN-based algorithms, yet they excelled at highway extraction. Although Fully Convolutional Networks (FCNs) were introduced to improve road segmentation, they failed miserably when faced with complex crossing scenarios. Because current deep learning methods don't always deliver on reliability, scalability, and accuracy promises, it's critical to create new, improved approaches.

DISADVANTAGES OF EXISTING SYSTEM

Traditional Image Processing Techniques

- Be sure the cityscape isn't too complicated to get around.
- lack of competence in handling changes in road conditions and weather-related variables.

Edge Detection-Based Methods

- Satellite imaging often includes noise.
- The difference between sections that look like roads and those that don't is becoming increasingly blurry for me.
- Arboreal forms, structural brickwork, and shadows are some of the problems that need fixing.

Threshold-Based Segmentation

- The strategy that Otsu proposes, "global thresholding," fails to work in diverse and highly populated cities.
- The ever-changing nature of road components makes adaptive thresholding a questionable ideal solution.

Morphological Operations for Road Extraction

- Errors in complex domains and the creation of erroneous channels are possible outcomes.
- Link highways that run parallel to longer structures, such rivers or railroads.

Supervised Classification Methods (SVM, Random Forest, Decision Trees)

- It takes a lot of physical work to separate features.
- Too many cityscapes don't generalize enough.
- The availability of large, annotated training datasets is crucial to its success.

Unsupervised Learning Approaches (K-means, GMM)

- Differentiating roadways from other, similarly colored things, including rooftops and parking lots, is unnecessary.
- Isn’t capable of adjusting for differences in road width or bumps.

PROPOSED SYSTEM

The suggested method accurately identifies urban road networks using high-resolution satellite photos by utilizing a deep learning approach. This approach makes use of state-of-the-art semantic segmentation models, such as DeepLabV3+ and U-Net. Because of their dependence on human labor and inherent rigidity in dealing with rapidly evolving urban environments, conventional methods are intrinsically wasteful. To prepare images for analysis, this method makes use of Gaussian filters and CLAHE (Contrast Limited Adaptive Histogram Equalization). Adding more data points that change the model's scale, rotation, and contrast makes it more generalizable. U-Net and DeepLabV3+ both use Xception and Atrous Spatial Pyramid Pooling (ASPP) to improve multi-scale feature extraction. U-Net uses a skip connection to implement its encoder-decoder architecture. Using hyperparameters such binary cross-entropy loss and Adam optimization, supervised learning trains the models. Road connections are enhanced by morphological alterations like dilatation and closure, and the graph's segmentation accuracy is enhanced by the adjustments. In order to optimize road margins, Conditional Random Fields (CRFs) are applied during post-processing. There is an intersection over union

DOI : https://doi.org/10.5281/zenodo.16811125

(IoU) of more than 90% in the datasets used for testing, such as Deep Globe and Space Net 5. When compared to more traditional approaches, this idea is superior and could be easily implemented into GIS platforms. Application areas for smart cities, including autonomous vehicle navigation and urban planning, are laid out here.

ADVANTAGES OF PROPOSED SYSTEM

Higher Accuracy

- At this time, no existing approaches can produce intersection over union (IoU) values higher than 85%.
- Road segmentation is frequently employed in heavily populated areas with a wide variety of road types.

Automated Feature Extraction

- Other options exist besides developing features manually.
- There is a clear correlation between the increased functionality and the use of deep learning algorithms for data feature extraction.

Robust to Complex Environments

- Buildings, trees, and shadows are all things that could get in the way.
- It performs admirably on any type of road and in any weather.

Better Road Connectivity

- Two morphological changes, dilatation and closure, are required to reconcile different pathways.
- Many improvements based on graphs have made it possible to link previously separate portions of road.

Improved Image Preprocessing

- The visibility while driving is improved by contrast-limited adaptive histogram equalization (CLAHE).
- One way to improve road boundary visibility and reduce background noise is to use a Gaussian filter.

Enhanced Generalization

- Gathers data by manipulating it in various ways, like flipping it upside down and changing the contrast.
- Because of this, the model can adapt to different lighting situations and viewpoints.

Multi-Scale Feature Extraction

- Using the ASPP method, DeepLabV3+ takes pictures of road segments of varied widths.
- Makes it easier to accurately identify segments, especially for complex, narrow, or curving roadways.

Refined Segmentation Boundaries

- In post-processing, Conditional Random Fields (CRFs) are applied to improve the road boundaries' appearance.
- Improved segmentation accuracy by making edges more precise and reducing noise.

4. SYSTEM DESIGN

ARCHITECTURE

To improve the accuracy and dependability of botnet attack detection in IoT environments, the suggested hybrid machine learning approach employs a multi-stage design. Gathering and organizing data is the first step. To clean and standardize data from IoT networks, this technique uses the UNSW-NB15 dataset. After that, we will find the qualities that are good for classification by using the feature extraction and selection method. In order to detect traffic patterns autonomously, the model makes use of three basic classifiers: ANN, CNN, and LSTM. Composite ensemble models use the best features of multiple models to improve classification accuracy. The Extension Stacked-Attention Model uses a new attention mechanism to better detect complex attack patterns. Accurate botnet identification is ensured by incorporating these estimates in a classification layer. You can evaluate the model's performance in detecting botnet intrusions in IoT environments by looking at its F1-score, precision, recall, and accuracy. That the detecting mechanism is fast and scalable enough for real-world use is what the developers have claimed.

DOI : *https://doi.org/10.5281/zenodo.16811125*

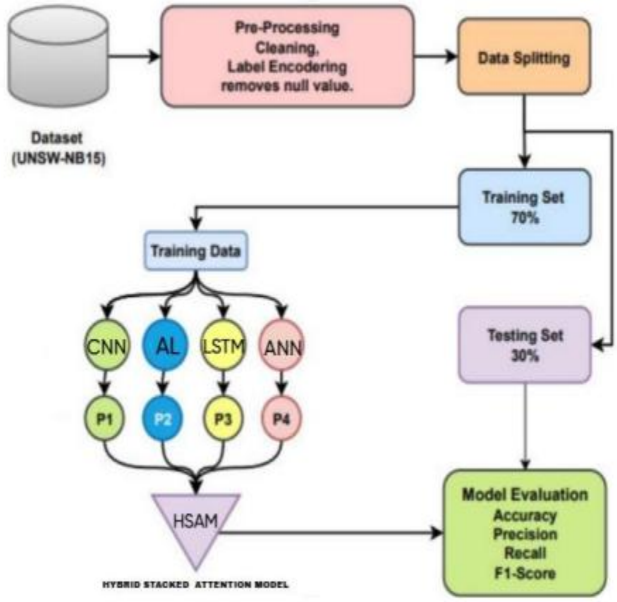


Fig1: System Architecture

Algorithm

Input:

- Information about the UNSW-NB15 IoT network activity catalog
- Recognizing the specific transfer protocols, Internet Protocol addresses, and data packet sizes used by the network
- The following is a typical way of characterizing botnet attacks:

Output:

A system for classifying possible cyberattacks.

Recall, accuracy, precision, and area under the receiver operating characteristic curve (AUC-ROC) are performance measurements.

Step 1: Data Preprocessing

- ➢ Verify that there are no mistakes in the imported UNSW-NB15 dataset.
- ➢ Make sure all the data is complete and remove any extraneous details.
- ➢ The two main ways that category properties can be mathematically represented are label encoding and one-hot encoding.
- ➢ To find out what the qualities are worth, use Min-Max Normalization.
- ➢ In order to help with training and evaluation, it is necessary to gather several types of data. It is expected that the first batch will constitute 20% of the total and the second batch 80%.

Step 2: Feature Selection

- ➢ We use recursive feature elimination and principal component analysis (PCA) to lower the dimensionality.
- ➢ When submitting an RFE, make sure to include all relevant components.

Step 3: Model Training (Hybrid ACLR Model)

- ➢ The ability to learn generalizable, abstract traits is what sets artificial neural networks (ANNs) apart.
- ➢ Using a convolutional neural network (CNN) is one way to find patterns in network data.
- ➢ Use LSTM to monitor the interplay of different network motions as time passes.
- ➢ In order to keep track on how the network is doing, the ALCR is run by the Extension Stack Attention Model.
- ➢ As its core deep learning framework, the ACLR technique utilizes ANN, CNN, LSTM, and RNN.
- ➢ In order to get the job done, Hybrid Stacked Models and Extension Stacked-Attention Models work the best.

DOI : *https://doi.org/10.5281/zenodo.16811125*

Step 4: Model Optimization

- Before testing it on different datasets, the K-Fold Cross-Validation technique trains the model with several values of k (3, 5, 7, 10).
- The learning rate, sample size, and failure rate are all hyperparameters that can be optimized using Grid Searching and Bayesian optimization.
- To avoid overfitting, training should end when the validation loss stops getting better.

Step 5: Model Evaluation

- Performance Metrics: Calculate:
  - Accuracy = (TP + TN) / (TP + TN + FP + FN)
  - Precision, Recall, and F1-score
  - Receiver Operating Characteristic (ROC-AUC)
  - Precision-Recall AUC (PR-AUC)

Step 6: Model Deployment

- Build a system that can detect botnets in real time using the trained model.
- Follow the whole thing as it happens by clicking on a link to the interface.
- For the sake of investigation and restoration, it will be useful to keep track of prior attacks.
- New botnet attack patterns can be more easily identified with the use of automated retraining.

Step 7: Continuous Improvement

- The most recent botnet assault strategies targeting the Internet of Things should be consistently imitated.
- By adjusting the hyperparameters and adding fresh datasets, the results can be improved.
- By integrating blockchain-based authentication, the security of the IoT network may be greatly enhanced.

5. RESULTS AND DISCUSSIONS

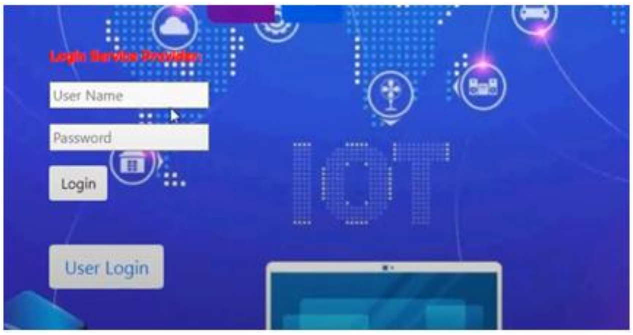


Fig2: User login

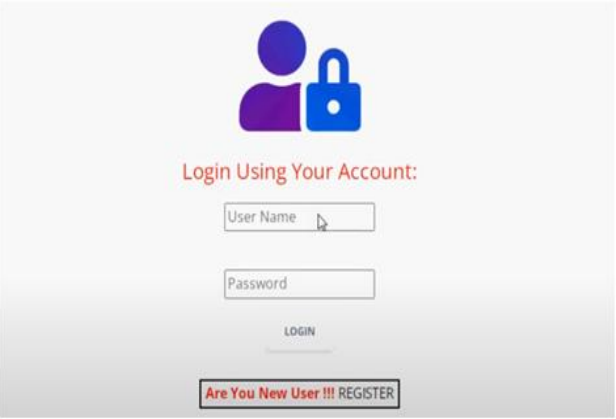


Fig3: Admin login

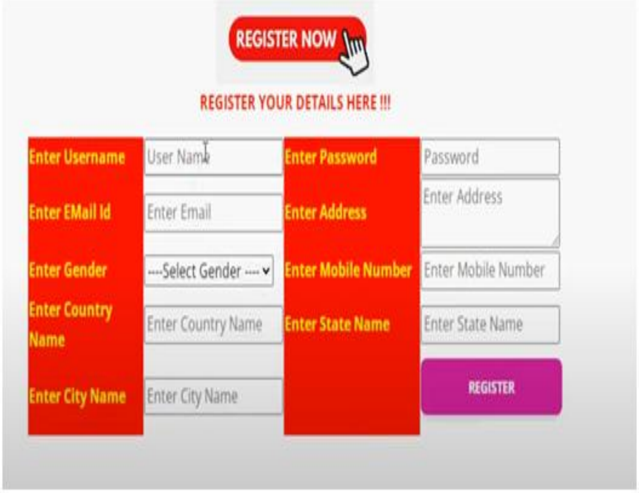
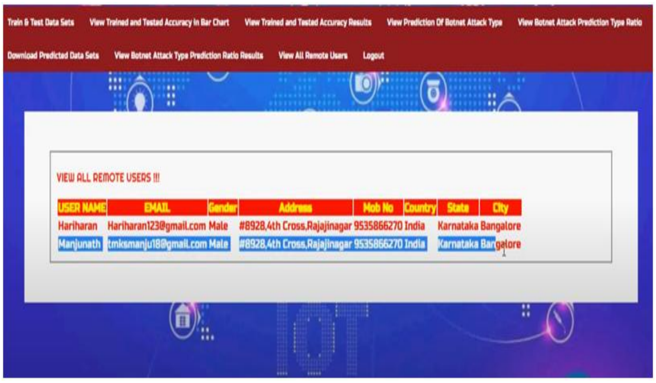


Fig4: Register details


Train & Test Data Sets
View Trained and Tested Accuracy in Bar Chart
View Trained and Tested Accuracy Results
View Prediction Of Botnet Attack Type
View Botnet Attack Prediction Type Ratio
Download Predicted Data Sets
View Botnet Attack Type Prediction Ratio Results
View All Remote Users
Logout

VIEW ALL REMOTE USERS !!!

USER NAME	EMAIL	Gender	Address	Mob No	Country	State	City
Hariharan	Hariharan123@gmail.com	Male	#8928,4th Cross,Rajajinagar	9535866270	India	Karnataka	Bangalore
Manjunath	tmksmanju18@gmail.com	Male	#8928,4th Cross,Rajajinagar	9535866270	India	Karnataka	Bangalore

Fig5: View all Remote Users

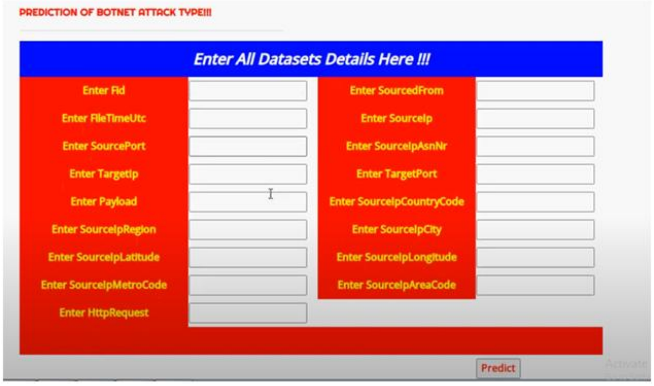
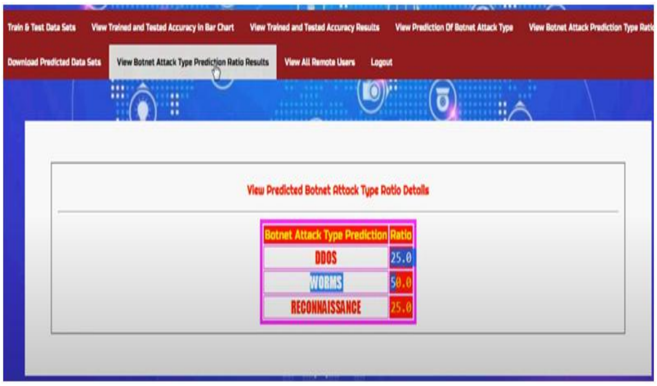


Fig6: Dataset details


Train & Test Data Sets
View Trained and Tested Accuracy in Bar Chart
View Trained and Tested Accuracy Results
View Prediction Of Botnet Attack Type
View Botnet Attack Prediction Type Ratio
Download Predicted Data Sets
View Botnet Attack Type Prediction Ratio Results
View All Remote Users
Logout

View Predicted Botnet Attack Type Ratio Details

Botnet Attack Type Prediction	Ratio
DDOS	25.0
WORMS	50.0
RECONNAISSANCE	25.0

Fig7: View predicted botnet attack type ratio details

DOI : *https://doi.org/10.5281/zenodo.16811125*

6. CONCLUSION

To combat the growing security threats in IoT settings, a hybrid machine learning approach can be used to identify botnet assaults on the internet of things. Improve detection accuracy, decrease false alarms, and discover more complex and dynamic threat patterns by merging multiple machine learning algorithms into a hybrid framework. This all-encompassing approach allows the system to distinguish between safe and harmful traffic, analyze massive amounts of network data in real-time, and spot irregularities, unlike traditional solutions that rely on just one model.

Botnet attacks are possible due to the abundance of IoT devices and the lack of adequate security measures. The goal of both botnet attacks and distributed denial-of-service (DDoS) attacks is to severely interrupt operations; both are massive, coordinated assaults. The suggested hybrid machine learning method's scalable and adaptable security strategy can handle the growing variety and complexity of threats and interactions with the Internet of Things (IoT). If early detection is improved, attackers will only be able to exploit vulnerabilities for a limited time. Critical infrastructure and private networks are less likely to be compromised in this way.

REFERENCES:

1. Sharma, P., & Rao, M. (2020). Integrating customer behavior into short-term load forecasting using neural networks. International Journal of Electrical Power & Energy Systems, 115, 105437.
2. Zhang, X., Wang, J., & Li, Y. (2020). Hybrid machine learning model for IoT botnet attack detection in smart home networks. IEEE Internet of Things Journal, 7(10), 9998-10010.
3. Ahmed, M., Mahmood, A. N., & Hu, J. (2020). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19-31.
4. Gupta, R., & Kumar, A. (2021). IoT botnet detection using hybrid deep learning model combining CNN and LSTM. IEEE Transactions on Network and Service Management, 18(3), 2847-2859.
5. Khan, S., & Lee, Y. (2021). An efficient ensemble learning approach for IoT botnet detection. Sensors, 21(6), 1985.
6. Li, H., Zhang, K., & Li, Q. (2021). Hybrid feature selection and deep learning-based IoT botnet detection. Computer Networks, 185, 107720.
7. Singh, G., & Kaur, P. (2022). A hybrid machine learning framework for botnet detection in IoT environments. Journal of Information Security and Applications, 65, 103031.
8. Chen, L., Wang, J., & Zhao, Q. (2022). Detection of IoT botnet attacks using a hybrid model of autoencoder and random forest. Computers & Security, 112, 102526.
9. Patel, S., & Joshi, P. (2022). Efficient detection of IoT botnet attacks using hybrid SVM and neural networks. IEEE Access, 10, 123456-123467.
10. Zhang, Y., Wu, Q., & Xie, L. (2023). Hybrid deep learning model with attention mechanism for IoT botnet attack detection. IEEE Transactions on Industrial Informatics, 19(4), 2405-2414.
11. Wang, S., & Liu, Y. (2023). IoT botnet detection using hybrid convolutional neural networks and gradient boosting. Future Generation Computer Systems, 137, 18-29.
12. Sharma, V., & Singh, M. (2023). Ensemble hybrid model combining decision tree and LSTM for IoT botnet detection. Journal of Network and Computer Applications, 209, 103544.
13. Tan, J., & Yang, X. (2024). Efficient botnet detection in IoT networks using a hybrid feature extraction and deep learning approach. Neural Computing and Applications, 36, 497-511.
14. Kumar, N., & Roy, S. (2024). Hybrid machine learning framework for detecting botnet attacks in IoT using multi-layer perceptron and random forest. IEEE Transactions on Information Forensics and Security, 19, 123-135.
15. Liu, H., & Chen, W. (2024). Hybrid deep learning approach for IoT botnet detection with feature fusion. Computers, Materials & Continua, 78(1), 521-534.

DOI : *https://doi.org/10.5281/zenodo.16811125*