Integrating Deep Learning with IOT: Combined Strategies for Botnet Detection

Sumit Kumar Soni
M. Tech Scholar
Department of Computer Science & Engineering-Artificial Intelligence and Machine Learning,
Oriental Institute of Science and Technology
Bhopal, Madhya Pradesh, India
sonisumit1001@gmail.com

Sreeja Nair
Head of Department
Department of Computer Science & Engineering-Artificial Intelligence and Machine Learning,
Oriental Institute of Science and Technology
Bhopal, Madhya Pradesh, India

Abstract: This study presents the study on intrusion detection in IoT networks that focuses on botnet attacks based on IoT device vulnerabilities. The proposed research will use a hybrid DL approach with architectures such as CNN2D-LSTM, DNN-LSTM, RNN, and RNN+FSA to enhance botnet attack detection on the N-BaIoT dataset. The optimized feature dimensionality is achieved without sacrificing performance by combining the strength of long-term dependency recognition with local pattern detection. A small labelled test set was developed to streamline the evaluation process, as well as to test how well the system works in comparison with attacks like Gafgyt and Mirai. The results from the RNN+FSA hybrid model are very excellent with 100% accuracy, precision, recall, and F1-score; better than other DL models. This study helps bring to the fore how hybrid DL techniques may be applied to boost the security of IoT and sheds the approach toward robust scalability in real-world applications.

Keywords: IOT Security, Botnet Detection, Deep Learning, Hybrid Models, Rnn+Fsa, Anomaly Detection

I. INTRODUCTION:

The Internet of Things (IoT), a vast network connected to the Internet and other connected devices, is made up of billions of intelligent physical items using sensors, software, and other embedded technologies [1]. The use of smart devices in daily life is growing quickly in the era of digital technology, affecting a wide range of sectors, including healthcare and agriculture. IoT-enabled devices generate big data with their sensing technologies, which is then transmitted to locations where deep learning algorithms can be applied to make precise judgments via fog computing or cloud computing [2]. With their numerous sensors and connection capabilities, these devices provide real-time data and facilitate better decision-making. However, a significant issue with the extensive use of IoT devices across numerous industries is the need to ensure the consistent and reliable operation of these networked systems. This challenge must be overcome in order to fully realize the potential benefits of IoT technology [3].

Smartphones, built-in systems, wireless sensors, and almost every other gadget in the era of the Internet of Things (IoT) are connected to the internet or a local network. Numerous new applications across a range of mobile and remote platforms have been made possible by the expansion of the Internet of Things (IoT), which includes smartphones, sensor networks, sensors for unmanned aerial vehicles (UAV), cognitively intelligent systems, and more. As the number of devices increases, so does the amount of data that can be gathered from them [4]. For instance, real-time physiological data, including blood glucose levels, body temperature, and other relevant information, is gathered from patients using wearable technology and other Internet of Things-based medical equipment. Indeed, the healthcare sector can benefit from the Internet of Things in terms of quick diagnosis and efficient remote clinical treatment. But because the IoT nodes in an IoT-enabled Healthcare System (HS) are always connected via an open, unprotected public channel, the network as a whole is susceptible to data manipulation, eavesdropping, and other security-related problems. More precisely, the lack of security considerations in communication protocols and the rapid development of hacking tools, which allow attackers to try to undermine the availability, integrity, and dependability of IoT devices and data, are the main causes of security concerns. These attacks can be launched on real IoT devices with the intention of reducing their functionality, in addition to deploying malware or malicious software to target healthcare network components [5].

IoT devices are vulnerable to several types of cyber-attacks since they connect objects to the internet and allow them to communicate with one another without human intervention. At the very beginning of the design and deployment of IoT devices, appropriate security requirements should be determined in order to guarantee the security of the network and devices. Since the Internet of Things is still in its infancy, it does not yet have a strong

security framework or system, which puts sensitive data at risk. To keep IoT entities, businesses, and individuals safe, modern security techniques must be implemented on IoT networks. Botnet-based DDoS attacks, in which hackers infect devices with scripts, pose the biggest security threat to the Internet of Things [6]. Once an IoT device has been infiltrated and infected, the attacker takes control of the compromised device and uses it to carry out various assaults. After the attacker has successfully taken over as many IoT devices as feasible, the subsequent step is performed. The attacker builds and grows his own IoT botnet in this manner. One of the most common illegal behaviours involving the Internet of Things is the creation of IoT botnets, which spread quickly and have the potential to do more damage than individual bad actions. IoT botnets may have detrimental effects [7].

Setting up security monitoring systems to identify illicit activity is one of the most efficient security defences against botnets. The focus of an organization that hosts a variety of IoT devices is on detection during the formation, C&C, or post-attack phases because it is interested in identifying devices that have been infected by IoT bot malware. However, companies that are targeted by IoT bot assaults want to stop malicious communications from being sent both during and after the attack. As a result, creating a monitoring system that covers the full botnet life cycle is crucial [8].

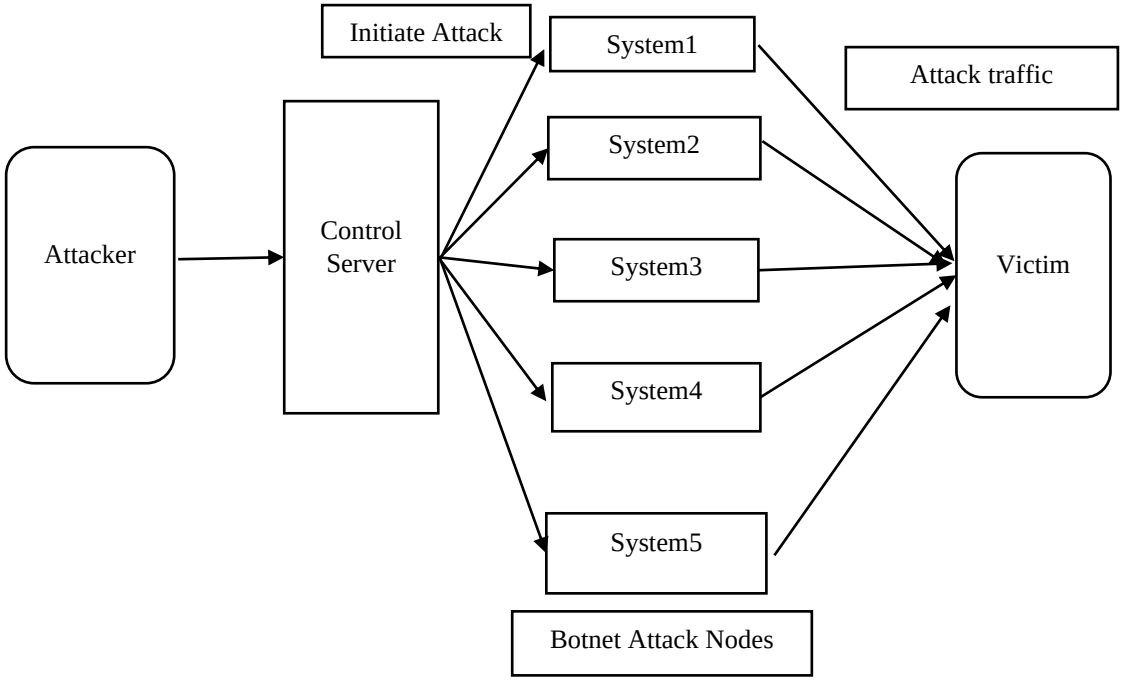

Figure1 Botnet Attack Architecture

This figure1 represents a botnet attack framework where an attacker communicates with a control server to initiate attacks. The control server directs compromised systems (botnet nodes) to generate attack traffic targeting the victim, creating a coordinated network-based attack.

II. LITERATURE SURVEY

Tran, M. Q.et al [9] introduced an innovative deep learning neural network (DNN) algorithm and Internet of Things (IoT) platform integration for online computer numerical control (CNC) machine monitoring. The suggested infrastructure is used to keep an eye on the cutting process while preserving the cutting stability of CNC machines. This ensures efficient cutting procedures that might contribute to higher product quality. The milling CNC machine center has a force sensor attached for this reason in order to measure the vibration conditions. Consequently, an Internet of Things (IoT) architecture is created to link the sensor node and the cloud server in order to use the message queue telemetry transport (MQTT) protocol to record the machine's condition in real time. To keep the CNC machine in a healthy state, an enhanced DNN model is created to categorize the various cutting conditions (i.e., stable cutting and unstable cuttings). Consequently, the deep learning system can precisely determine if the data sent by the smart sensor over the internet is authentic cutting data or fraudulent data resulting from cyber-attacks or the sensors poor reading due to noise, temperature, and humidity signals. The excellent outcomes of the suggested strategy show that deep learning can perform better for vibration control than other conventional machine learning techniques. The cutting information is shown on a graphical dashboard and the cutting process is tracked in real time using the Contact components for IoT. While putting the suggested deep machine learning and Internet of Things-based monitoring system into practice, experimental verifications are carried out to conduct various cutting circumstances of slot milling. Various scenarios are shown to test the efficacy of the created system, which can switch to the backup broker to continue

running operations and disconnect instantly to secure the system automatically upon detecting a cyber-attack.

Rane, N. L. et al [10] showed new era of increased productivity, information assurance, and data-influenced decision-making is being ushered in by the integration of the Internet of Things (IoT) and block chain technology with the power of artificial intelligence (AI), machine learning (ML), and deep learning (DL). Our study examines the ways in which these state-of-the-art technologies interact to facilitate intelligent industry innovations. In addition to providing conductive connectivity and communication between devices, this can generate enormous data pools, which are crucial for improving decision-making and, ultimately, for running more sustainably. The AI ML and DL algorithms then scale and interpret this data to obtain predictive insights, optimize processes, and enhance automation. The security and immutability of data are critical in an Internet of Things network. In addition to being very good at both, block chain technology ensures that data exchanged within these networks is safe and immutable. The demands of industrial applications, which extend well beyond supply chain optimization and predictive maintenance to include real-time monitoring and autonomous operations, can now be better met by recent developments in AI, ML, and DL. Rather, this study takes a pragmatic, real-world implementation perspective, emphasizing the advantages and challenges of combining various technologies. The findings demonstrate this integration's tremendous transformative potential and point to a level of efficiency, security, and innovation never before seen, which will redefine intelligent industries both now and-perhaps more importantly-in the future, effectively defining the fourth industrial revolution and beyond.

Abusitta, A., et al [11] introduced Systems for the Internet of Things (IoT) are now a necessary component of many government services and companies. Unfortunately, it is well known that IoT networks and devices are extremely susceptible to security threats that aim to compromise service availability and data integrity. Furthermore, compared to traditional information technology (IT) networks, the detection of aberrant behaviour and compromised nodes is made more difficult by the heterogeneity of the data gathered from different IoT devices as well as the disruptions experienced within the IoT system. Therefore, in order to ensure that harmful data is not used in IoT-driven decision support systems, there is an urgent need for efficient and trustworthy anomaly detection. In this research, we propose an anomaly detection system for IoT that is powered by deep learning. This system can learn and capture resilient and relevant features that are not greatly impacted by unstable situations. These features are then used by the classifier to increase the accuracy of detecting phony IoT data. More specifically, the proposed deep learning model is based on a denoising auto encoder and is utilized to produce features that are robust to the heterogeneous IoT environment. Experimental results based on real-world IoT datasets show how successful the proposed framework is at increasing the accuracy of identifying dangerous data when compared to the state-of-the-art IoT-based anomaly detection algorithms.

Nazir, A., et al [12] showed from home automation and industrial control systems to healthcare and transportation, the Internet of Things (IoT) has revolutionized many facets of contemporary life. But there are also more security risks as a result of the growing number of linked devices, especially from botnets. Several machine learning (ML) and deep learning (DL) methods have been put forth for the identification of IoT botnet attacks in an effort to lessen these risks. By closely examining benchmark datasets, evaluation criteria, and data pre-processing methods, this systematic research seeks to determine the best machine learning and deep learning methods for identifying IoT botnets. A thorough search for primary research published between 2018 and 2023 was carried out across several databases. Studies that reported using ML or DL algorithms for IoT botnet detection were considered. Twenty-five research were included in the final review after 1,567 records were screened. According to the results, ML and DL approaches outperform conventional signature-based approaches in identifying IoT botnet attacks. However, the methods' efficacy differed according to the features, dataset, and assessment criteria employed. This review offers suggestions for further research in this field and suggests a taxonomy for ML and DL approaches in IoT botnet attack detection based on the synthesis of the findings. This review illuminates the considerable potential of ML and DL approaches in bolstering the detection of IoT botnet attacks, thereby offering valuable insights to researchers involved in the domain of IoT security.

Nasir, M. H., et al [13] in recent years, Cyber-attacks against the Internet of Things (IoT) have significantly increased. The main causes of this include the widespread usage of IoT in homes and significant national infrastructures, as well as the inherent security vulnerabilities of IoT endpoints. Botnets have emerged as a serious threat to IoT-based infrastructures because they can produce an army of hacked devices that can function as a lethal cyber weapon against target systems, networks, and services. These networks target firmware vulnerabilities, such as weak or default passwords. In this paper, we describe our efforts to address this issue by creating an intrusion detection system that is integrated into an Internet of Things device to improve visibility and harden the device's security. Our research framework, BTC_SIGBDS (Block chain-powered, Trustworthy, Collaborative, Signature-based Botnet Detection System), includes the device-level intrusion detection described here. Through a thorough critical analysis of the body of current literature, we identify the research challenge and provide the device-level component of the BTC_SIGBDS

framework in detail. To improve defence against new threats, we employ a detection system based on signatures with trustworthy signature updates.

Through the creation of custom signatures for two of the most well-known signature-based intrusion detection systems (IDS) using the ISOT, IoT23, and BoTIoT datasets, we have assessed the suitability and improved the capability in order to evaluate the effectiveness of the system in detecting anomalous traffic in a typical resource-constrained IoT network in terms of peak CPU and memory usage, number of alerts, detection rates, and detection time.

Table 1 Summary of IoT-Based Monitoring and Security Approaches: Technologies, Contributions, and Limitations

Author(s)	Key Contributions	Technology Used	Limitations
Tran, M. Q. et al [9]	Introduced intelligent integration of IoT platform and DNN for online monitoring of CNC machines. Proposed a system using force sensors and MQTT protocol for real-time monitoring, ensuring cutting stability and quality.	IoT platform, Deep Neural Networks (DNN), Force Sensors, MQTT Protocol	Limited to specific industrial applications (CNC machines). Generalizability to other systems is unclear.
Rane, N. L. et al [10]	Explored integration of IoT, block chain, AI, ML, and DL to transform smart industries. Focused on automation, predictive insights, and data security using block chain for robust and unalterable networks.	IoT, Block chain, AI, Machine Learning (ML), Deep Learning (DL)	Scalability of integration across diverse industries is not fully validated. Computational requirements of combined systems could be high.
Abusitta, A. et al [11]	Proposed a DL-powered anomaly detection system using a denoising auto encoder to handle heterogeneous and unstable IoT environments. Demonstrated enhanced accuracy for detecting malicious data in IoT systems using real-life datasets.	Deep Learning (DL), Denoising Auto encoder, Real-Life IoT Datasets	Focuses mainly on malicious data detection; does not address specific countermeasures for detected anomalies. Performance in large-scale IoT networks is untested.
Nazir, A. et al [12]	Systematically reviewed ML and DL techniques for IoT botnet detection, identifying effective methods, benchmarking datasets, and proposing a taxonomy for future research. Highlighted ML/DL's superiority over traditional detection methods.	Machine Learning (ML), Deep Learning (DL), Benchmark Datasets	Relies heavily on quality and diversity of datasets for effective training. Practical implementation challenges in real-time IoT environments are not explored.
Nasir, M. H. et al [13]	Developed a block chain-powered, signature-based intrusion detection system (BTC_SIGBDS) for IoT botnet detection. Evaluated system effectiveness	Block chain, Intrusion Detection System (IDS), Signature-Based Detection, IoT Security Datasets (ISOT, IoT23, BoTIoT)	Signature-based systems may struggle with zero-day attacks. Computational and resource requirements may limit its deployment in low-resource IoT environments.

	using ISOT, IoT23, and BoTIoT datasets, focusing on anomalous traffic detection, detection time, and resource efficiency.		

III. RESEARCH METHODOLOGY:

Cybercriminals have taken notice of the increasing use of Internet of Things (IoT) technology in critical infrastructure sectors. They take advantage of Internet of Things flaws to create a botnet, which is a collection of compromised devices that are utilized to launch advanced cyber-attacks against the linked critical infrastructure. Significant research has recently been conducted to investigate the potential of machine learning (ML) and deep learning (DL) for the detection of botnet assaults in Internet of Things networks. Some difficulties remained, though, such as the inability to detect zero-day attacks, the need for a large amount of memory to store network traffic data, the inability to optimize model hyperparameters, extremely poor classification performance due to an unbalanced sample distribution in the training set, and data privacy issues. A hybrid technique is proposed for botnet attack detection in IoT-enabled critical infrastructure to overcome such bottlenecks. This article develops three deep learning algorithm models that can detect botnet attacks in IoT-enabled critical infrastructure. A hybrid DL technique that uses CNN2D-LSTM, DNN + LSTM, RNN, and RNN+FSA architectures to improve the feature dimensionality of network traffic data is presented with no noticeable negative impact on classification performance. Deep learning methods such as CNN2D-LSTM, DNN + LSTM, RNN, and RNN+FSA were used to develop predictive models, and all tests were carried out using Anaconda Python programming. The Confusion Matrix has been used to measure the models' performance. From the study findings, CNN2D-LSTM, CNN2D-LSTM, RNN, and RNN+FSA gave an accuracy of 100%. Consequently, this paper proposes a hybrid solution that utilizes RNN+ FSA to enhance botnet attack detection for IoT-enabled critical infrastructure.

This research paper presents the development of an innovative, smart hybrid architecture combining deep learning and nature-inspired optimization techniques to identify botnet attacks in IoT networks. The process is cast as a classification problem; that is, network traffic packets are to be classified as either benign or malicious in binary classification, or categorized into specific types of botnet attacks in multi-class classification. The several DL models and nature-inspired optimization methods are developed for effectively differentiating between harmful and benign communication. With the growth of cloud computing, IoT devices send data to central cloud servers for pre-processing and analysis. The proposed hybrid approach integrates DL with optimization for hyperparameter optimization, such as hidden layers, learning rates, optimizers, activation functions, batch sizes, and epochs, to improve the performance of botnet attack detection. To maximize the accuracy and efficiency of the IoT botnet detection, the designed hybrid model, RNN+FSA-based, is applied for binary, 5-class, 10-class, and 11-class classifications of network traffic data coming from the N-BaIoT dataset.

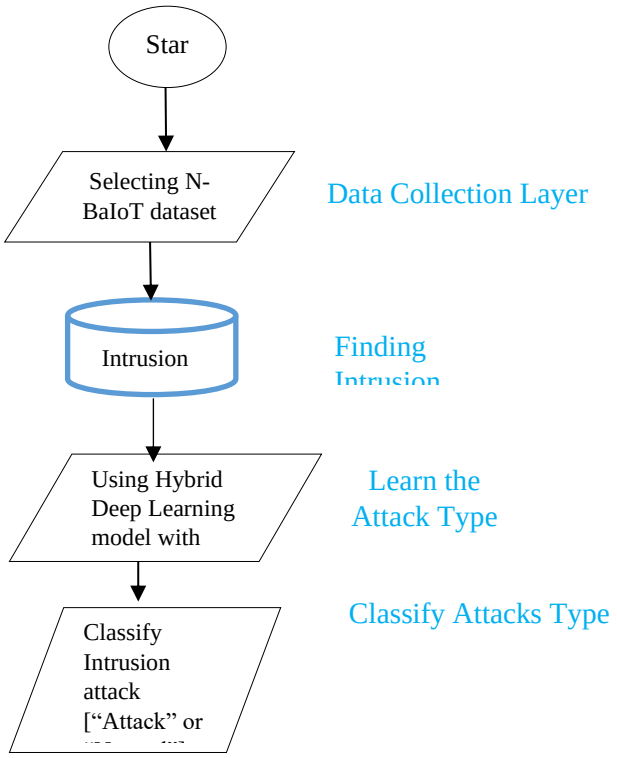

Figure 3: Proposed Architectural Framework for Detecting Intrusions on IoT data

Figure 3 illustrates the process that is continuous for intrusion detection based on the N-BaIoT dataset. This includes the data collection layer that utilizes the N-BaIoT dataset in terms of network traffic data and then analyzes it through the intrusion detection process to identify potential malicious activities. The system learns from the data using a hybrid deep learning model with optimization to improve its detection accuracy. Once trained, the model classifies the network behaviour as "Attack" or "Normal," and for detected attacks, it further categorizes the specific type of attack. This process is seamless to ensure efficient and precise intrusions detection in an IoT network.

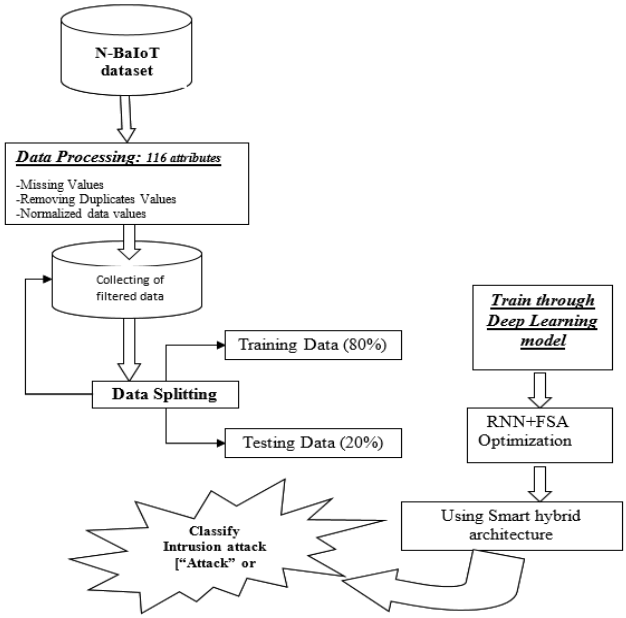

Figure 4 Proposed comprehensive flowchart of the suggested model.

In Figure 4 above, during the pre-processing stage the training-set data samples are encoded and normalized and fit into a data structure compatible to the Tensor Flow framework. The entire dataset will be split into two subsets following pre-processing: a training subset and a validation subset. The validation subset is used to verify the network that has already been trained, and the former, or training subset, is used to train the Smart hybrid architecture using the DL approach and nature-inspired optimization RNN+FSA. A different testing dataset is utilized to test the model's classification accuracy and other performance metrics once the validation phase is finished.

A. Data Collection:

In this step, the publicly available N_BaIoT dataset from the datasets from Kaggle is used to enhance our analysis to estimate whether which makes it probable to automate intrusion detections in IoT network. This dataset addresses the lack of public botnet datasets, especially for the IoT. The data suggests real traffic, collected from nine commercial IoT devices that have been verified to be infected with BASHLITE and Mirai. A significant challenge for IoT intrusion detection research is the lack of availability of a complete dataset based on networks that replicates the current state of network traffic. The N_BaIoT dataset, which was created by inserting botnet attacks from the Gafgyt and Mirai botnets into six different kinds of IoT devices, was used to construct our botnet dataset. Both Gafgyt and Mirai assaults use five different attack methods, such as TCP, ACK, and UDP. Our approach to botnet identification is based on the hybrid DL method, which maximizes the feature dimensionality of the network traffic data by utilizing CNN2D-LSTM, DNN + LSTM, RNN, and RNN+FSA architectures. We built a botnet detection paradigm that can identify severe botnet attacks by building on this training model. The method for detecting botnets is a component of a multiclass classification model that improves botnet identification for various Internet of Things devices by differentiating between sub attacks and benign data.

The N_BaIoT data set was selected for this study because it includes only two classes-Gafgyt and Mirai represent contemporary attack and regular traffic patterns. The recommended strategy is made easier by this class distribution because we are completing a binary classification problem. Second, N_BaIoT presents five different types of IoT assaults in a comprehensive data set. Thirdly, training recurrent neural networks is a great fit for the sequential dataset N_BaIoT. The Figure 5 bar chart illustrates the distribution of different classes in the IoT botnet attack detection dataset, showcasing the frequency of various attack types and benign traffic. The most common attack types are "mirai_udp" and "gafgyt_udp," followed by others like "gafgyt_tcp," "mirai_syn," and "mirai_ack," which also appear in significant numbers. Benign traffic is well-represented, though less frequent than the major attack types, while rarer attacks like "gafgyt_scan" and "mirai_junk" have lower frequencies. This distribution highlights the dominance of certain attack types and provides essential information for understanding dataset composition and ensuring balanced training for intrusion detection models.

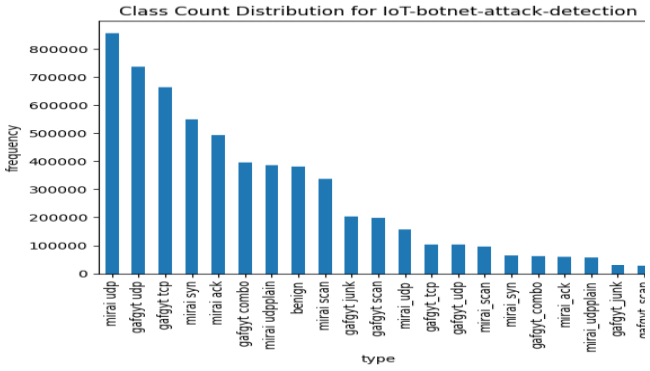

Figure 5: Different class count distribution for IoT-Botnet-Attack-Detection.

B. *Data Pre-processing Stage:*

In this study, checks and transformations in the data pre-processing stage were performed very rigorously to guarantee the quality and suitability of the dataset. Check for missing values - No Null data was found in the dataset as part of a generic check and the data set appeared to be complete. This suggested the dataset was of high precision and accuracy. Data was also scaled to a common 0-1 range in order to make comparisons between features more uniform and meaningful. Such a scaling improved data readability and analysis. The pre-processing of the N_BaIoT dataset has been completed. Z-score normalization is used to standardize the dataset, giving each voxel a unit variance and a mean of zero.

$$D_{norm} = \frac{\mathrm{D}-\mu_i}{\sigma_i} \quad \text{(i)}$$

Data are pre-processed using $\mu_i$andσ_i, which stand for the mean and standard deviation, to represent the normalized data (D_{norm}) and the original data (D).

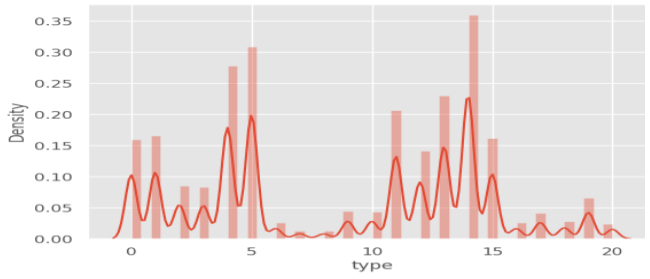

Figure 6: Different class attributes for IoT-Botnet-Attack-Detection data transformation.

C. *Data Splitting Stage:*

An important part of this study endeavour that focused on the N_BaIoT dataset was the data division method. To create an accurate and dependable intrusion attack detection model, the N_BaIoT dataset was divided into two parts: a 20% testing set and an 80% training set. By allowing the model to be trained on a significant amount of the data, this separation made it easier for the model to see trends and build connections. By evaluating the model's performance on data it had never seen before, the independent testing set provided an objective assessment of the model's predictive power.

D. *Visualize feature correlation to the target on N_BaIoT dataset:*

The N-BaIoT dataset, a publicly available resource for cyber security research, is utilized for enhancing botnet identification in IoT devices under various cyber-attack scenarios. The dataset, derived from an IoT testbed including devices like security cameras, webcams, and thermostats, contains 116 statistical features extracted from network traffic snapshots during botnet infections by BASHLITE (GAFGYT) and Mirai malware. It comprises 170,000 records, including 50,000 for Mirai traffic, 60,000 for benign traffic, and 60,000 for GAFGYT traffic. GAFGYT facilitates attacks like TCP/UDP flooding and spam data delivery, while Mirai targets IoT devices with ARC processors to launch various DDoS attacks. The dataset supports binary classification (benign vs. malicious) and multi-class classification across 10 attack types and one benign class, providing a robust foundation for studying botnet detection.

E. *Using Different Deep Learning Models to detect intrusion attack :*

LSTM (Long Short-Term Memory): LSTMs use a gating mechanism to address the vanishing gradient problem in back propagation, where it controls memory processes and stores, writes, or reads information through gates operating in an analog format, which makes them suitable for learning sequential data. It is very effective in maintaining long-term dependencies.

CNN-LSTM: This architecture hybridizes CNN's features at higher-level extraction ability, in strength within handling sequential data with LSTMs. Here, there is a convolution layer with the extraction of word embedding's to apply further pooling layers feeding through a fully connected layer, resulting into generation of predictions with outputs as it operates in 0-1 range; the inclusion of drop-out layers reduces the chances of overfitting.

Bidirectional LSTM: Bidirectional LSTM enhances traditional LSTM by processing the data in both forward and backward directions, which allows for more efficient sequence classification. The use of input, forget, and output gates helps to effectively handle memory, capturing both past and future context to further enhance model accuracy for sequential tasks.

CNN-BI-LSTM Model: It is CNN-LSTM where this architecture would combine local pattern capturing in the

CNN structure and process dependencies at both long and short lengths in both forward and reverse directions for the Bidirectional LSTM layers. These networks consist of embedding layers, convolutional layers including max-pooling layers, Bidirectional LSTM layers, fully connected layer, and dropout plus softmax activation on top.

Recurrent Neural Network (RNN): RNNs utilize outputs of previous steps as inputs at the current step, making them ideal for sequential jobs, such as speech recognition. However, the vanishing or exploding gradients that accompany long-term dependencies do present challenges for RNNs. Nevertheless, RNNs are useful for tasks requiring memory of past inputs.

Flamingo Search Algorithm (FSA): FSA is an evolutionary algorithm inspired by the foraging and migration behaviours of flamingos. Every potential solution is represented as a flamingo, and the algorithm optimizes solutions mimicking their communication and movement patterns. The aim of the algorithm is to find the global optimum solution within a search space by applying the principles of swarm intelligence.

IV. RESULTS AND DISCUSSIONS:

The model for machine learning was trained by the study using Python's TensorFlow in conjunction with the Keras framework on Google Colab. Training and testing used 90:10 percent of the dataset. The predictive model underwent training over more than 100 epochs using the optimization algorithm Adam with a rate of learning of 0.0001. There was a Tesla P100-PCIE GPU in use. Figure 7 shows our proposed smart hybrid model.

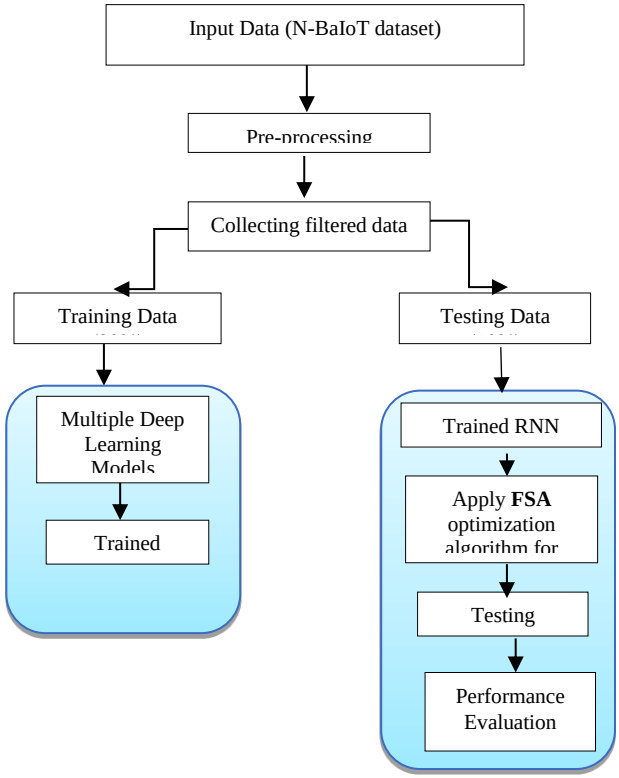

Figure 7: Flowchart for Proposed Smart Hybrid approach to detect benign and malicious behaviour by designing a DL-based system.

The main contributions of this study is that, it investigates and explains the efficiency of DL algorithms in addressing intrusion detection in IoT systems. Second, it demonstrates, via simulation results, the effectiveness of the hybrid architecture RNN+FSA in identifying IoT attacks and provides the parameter values that are necessary for RNN+FSA to produce high detection accuracy. Using the Google TensorFlow implementation framework and the Python programming language, this research also advances the effective implementation of the RNN+FSA technique.

A. Correlation Confusion Matrix Map of all the attributes:

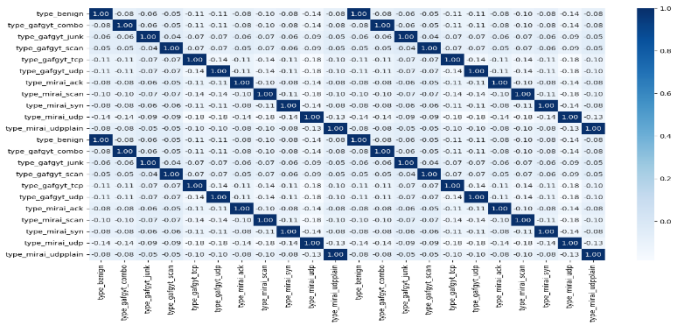

Figure 8: Correlation heat map to measure accuracy, sensitivity, and specificity for ECG attribute information.

The correlation heat map shown in Figure 8, which shows the relationship between intrusion detection of the N-BaIoT dataset and whether or not an intrusion assault ["Gafgyt" or "Mirai"] is viable, is shown in Figure 8. The test-set includes nine different types of attacks, five of which are frequently found in IoT attacks. The N_BaIoT dataset, which was created by directing botnet attacks from the Gafgyt and Mirai botnets onto six different kinds of IoT devices, served as the foundation for our botnet dataset. Both Gafgyt and Mirai attacks comprise five different attack types, such as UDP, TCP, and ACK.

B. Performance Measures:

$$Sensitivity = \frac{(T_P)}{(T_P + F_N)} \quad \text{(ii)}$$

$$Specificity = \frac{(T_N)}{(T_N + F_P)} \quad \text{(iii)}$$

$$Accuracy = \frac{(T_P + T_N)}{(T_P + T_N + F_P + F_N)} \quad \text{(iv)}$$

$$Precision = \frac{(T_P)}{(T_P + F_p)} / \times 100\%$$

$$Recall = \frac{(T_P)}{(T_P + F_N)} \times 100\%$$

Where,

T_P Denotes True Positive.

T_N Denotes True Negative.

F_P Denotes False Positive.

F_N Denotes False Negative.

C. Assessment of Outcomes:

The performance of the suggested model in comparison to industry standards is evaluated using the metrics covered in this section. The suggested model had been improved with ADAM (learning rate: 0.0001) after being constructed with Python, Keras, and TensorFlow. With 90:10 training to testing ratio, the combined set of data using a Google Colab Tesla T4 GPU and 25 GB of RAM.

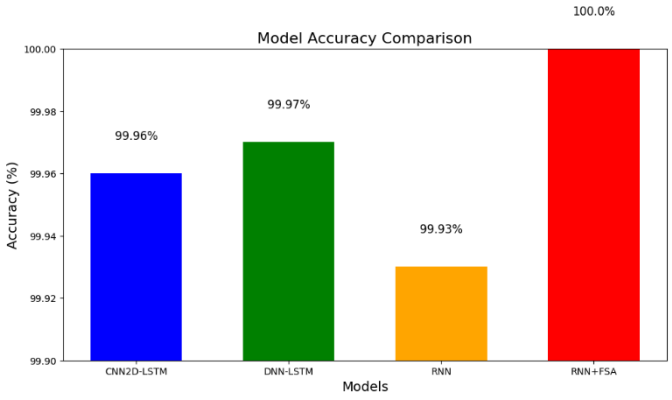

Figure 9 Model accuracy comparison

In Figure 9, the CNN2D-LSTM and DNN-LSTM were used earlier with accuracy score of 99.96% and 99.97% but RNN which we used has an accuracy score of 99.93 % and when it's combined with FSA it scores 100 %.

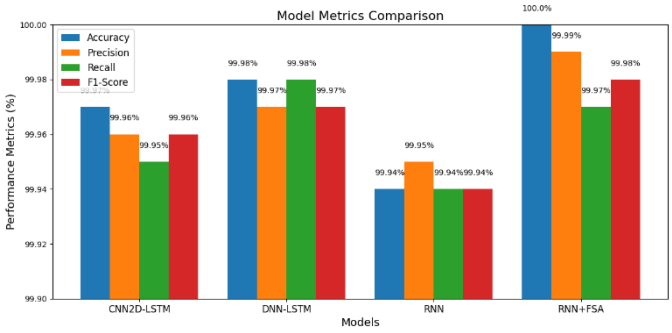

Figure 10 Model metrics Comparison

The graph Figure 10 presents a comparison of performance metrics-Accuracy, Precision, Recall, and F1-Score-for four machine learning models: CNN2D-LSTM, DNN-LSTM, RNN, and RNN+FSA. The y-axis represents performance as a percentage, while the x-axis displays the model names. Among the models, RNN+FSA demonstrates the best overall performance, achieving 100% accuracy and slightly higher values in other metrics compared to the others. DNN-LSTM and CNN2D-LSTM have very similar and high performances, with values ranging from 99.96% to 99.98% for all metrics, meaning they are reliable and robust. The RNN model, though slightly lower in comparison, still performs exceptionally well, keeping Precision, Recall, and F1-Score close to 99.94%. All models show near-perfect metrics, emphasizing their effectiveness, with RNN+FSA emerging as the standout due to its 100% accuracy and marginally better performance.

The performance of hybrid deep learning models on the N-BaIoT dataset is analyzed for detecting intrusion attacks such as those caused by Gafgyt and Mirai on IoT devices. For speedier testing and optimization, a smaller testing set with samples of five different attack categories and typical traffic has been created. By taking advantage of advantages

in local pattern recognition and long-term dependency recognition, hybrid architectures including CNN2D-LSTM, DNN-LSTM, RNN, and RNN+FSA were created to improve detection capabilities. RNN+FSA beat all other models and demonstrated the efficacy of the suggested strategy by achieving 100% accuracy, precision, recall, and F1-score. The viability of employing hybrid deep learning approaches to maximize the dimensionality of network traffic features and attain strong diagnostic performance in identifying IoT botnet incursions is demonstrated by this study.

V. CONCLUSION

The proposed hybrid deep learning framework effectively addresses the challenge of botnet attack detection in IoT networks. Employing the CNN2D-LSTM, DNN-LSTM, RNN, and RNN+FSA models, this study demonstrates the ability to accurately classify network traffic as either benign or malicious in a reliable and efficient manner. From the results, it was found that the RNN+FSA model is the standout and performed at 100% accuracy for real-time intrusion detection. This approach not only optimizes feature dimensionality but also scales well to a variety of IoT scenarios and, hence, is a promising solution for bolstering IoT security. Future work includes deploying the model in real-world environments, enhancing its adaptability with continuous learning, and integrating it with IoT platforms to improve scalability and resilience against emerging threats. This research lays the foundation for a strong intrusion detection framework that can mitigate security risks in complex IoT ecosystems.

Conflict of Interest: The corresponding author, on behalf of all authors, confirms that there are no conflicts of interest to disclose.

References:

1. Syamala, M., Komala, C. R., Pramila, P. V., Dash, S., Meenakshi, S., & Boopathi, S. (2023). Machine learning-integrated IoT-based smart home energy management system. In *Handbook of Research on Deep Learning Techniques for Cloud-Based Industrial IoT* (pp. 219-235). IGI Global.
2. Verma, P., Tiwari, R., Hong, W. C., Upadhyay, S., & Yeh, Y. H. (2022). FETCH: a deep learning-based fog computing and IoT integrated environment for healthcare monitoring and diagnosis. *IEEE access*, *10*, 12548-12563.
3. Raparthy, M., & Dodda, B. Predictive Maintenance in IoT Devices Using Time Series Analysis and Deep Learning. *Dandao Xuebao/Journal of Ballistics*, *35*, 01-10.
4. Lakshmanna, K., Kaluri, R., Gundluru, N., Alzamil, Z. S., Rajput, D. S., Khan, A. A., ... & Alhussen, A. (2022). A review on deep learning techniques for IoT data. *Electronics*, *11*(10), 1604.
5. Kumar, P., Kumar, R., Gupta, G. P., Tripathi, R., Jolfaei, A., & Islam, A. N. (2023). A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system. *Journal of Parallel and Distributed Computing*, *172*, 69-83.
6. Pokhrel, S., Abbas, R., & Aryal, B. (2021). IoT security: botnet detection in IoT using machine learning. *arXiv preprint arXiv:2104.02231*.
7. Wazzan, M., Algazzawi, D., Bamasaq, O., Albeshri, A., & Cheng, L. (2021). Internet of Things botnet detection approaches: Analysis and recommendations for future research. *Applied Sciences*, *11*(12), 5713.
8. Kalakoti, R., Nõmm, S., & Bahsi, H. (2022). In-depth feature selection for the statistical machine learning-based botnet detection in IoT networks. *IEEE Access*, *10*, 94518-94535.
9. Tran, M. Q., Elsisi, M., Liu, M. K., Vu, V. Q., Mahmoud, K., Darwish, M. M., ... & Lehtonen, M. (2022). Reliable deep learning and IoT-based monitoring system for secure computer numerical control machines against cyber-attacks with experimental verification. *IEEE Access*, *10*, 23186-23197.
10. Rane, N. L., Kaya, O., & Rane, J. (2024). Integrating internet of things, blockchain, and artificial intelligence techniques for intelligent industry solutions. *Artificial Intelligence, Machine Learning, and Deep Learning for Sustainable Industry*, *5*, 2.
11. Abusitta, A., de Carvalho, G. H., Wahab, O. A., Halabi, T., Fung, B. C., & Al Mamoori, S. (2023). Deep learning-enabled anomaly detection for IoT systems. *Internet of Things*, *21*, 100656.
12. Nazir, A., He, J., Zhu, N., Wajahat, A., Ma, X., Ullah, F., ... & Pathan, M. S. (2023). Advancing IoT security: A systematic review of machine learning approaches for the detection of IoT botnets. *Journal of King Saud University-Computer and Information Sciences*, 101820.
13. Nasir, M. H., Arshad, J., & Khan, M. M. (2023). Collaborative device-level botnet detection for internet of things. *Computers & Security*, *129*, 103172.