Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 1, January, 2026
Website: usajournals.org

ENHANCING THE CYBERSECURITY OF INDUSTRIAL INTERNET OF THINGS INFRASTRUCTURE THROUGH AN INTELLIGENT HYBRID DEEP LEARNING BASED BOTNET DETECTION AND PREVENTION FRAMEWORK

Zena Ez. Dallalbashi
Mosul Polytechnic College
Northern Technical University Mosul -Iraq
zeina.ez@ntu.edu.iq

Tareq Abed Mohammed
College of Veterinary Medicine
University of Kirkuk Kirkuk-Iraq
Tareq.mohammed@uokirkuk.edu.iq

Shaymaa Alhayali
Computer Center
University of Mosul Mosul -Iraq
shymaa_alhyali@uomosul.edu.iq

Abstract
The rapid developmental pace of the Industrial Internet of Things (IIoT) has significantly aided automation processes in the industries, efficiency in the operations, and networking within the system. However, this shift has also given rise to new security threats and more so with the increasing sophistication and scale of cyberattacks by means of botnet on vital industrial systems. The study project will provide an effective Hybrid Deep Learning-based security architecture, which is solely designed to safeguard IIoT systems against advanced botnet attacks. The proposed methodology relies on the synergistic theory of

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 1, January, 2026
Website: usajournals.org

integrating the Convolutional Neural Networks (CNNs) to obtain spatial feature at the higher level with Recurrent Neural Networks (RNNs) to acquire the temporal relation among the traffic and the serial nature of the attacks. This hybrid design enables the characterization of fixed and dynamically varying network patterns, as well as an evaluation to a large extent further since the model is trained on heterogeneous and different IIoT traffic patterns. This further enhancement by adding anomaly detection mechanisms and deep feature learning is to bolster the abilities of the system to distinguish between malicious botnet entries and normal industrial traffic. In turn, the hybrid deep learning model offered outperforms the existing state-of-the-art approaches in the areas of detection accuracy, robustness, scalability, and computational cost which predetermines its applicability in resource-based IIoT systems and enables the use of the model in real-time.Substantial experimental evaluations attest to the superiority of the hybrid deep learning model to the existing state-of-the-art solutions both in the area of detection accuracy and low false-positive rates and computation cost. This study presents both scalability and resilience in the defense of IIoT-enabled critical infrastructure through the provision of real-time detection of the threats and preventive actions to contain the dynamic world of botnets that, despite its much larger size, is no different than the threat posed on the infrastructure.

Keywords: Industrial Internet of Things, Security, Botnet Attacks, Hybrid Deep Learning, Convolutional Neural Networks, Anomaly Detection, Feature Extraction.

Introduction

Industrial digitization has now taken a new stage with the Industrial Internet of Things (IIoT), which has allowed an ability to connect, communicate intelligently and to collaborate in real-time with machines, devices, and cyber-physical systems. The paradigm shift has drastically altered the way industrial processes are conducted by maximizing automation of processes, improving productivity, lessening down time, and creating data-driven innovation in various industrial sectors. Nevertheless, the unprecedented scope of connectivity and

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 1, January, 2026
Website: usajournals.org

interdependence with IIoT, has at the same time enlarged the cyber-attack area of industrial networks, and made them more susceptible to complex and well-organized security threats. The botnet attacks have become one of the most urgent and increasingly growing threats among those, leveraging the lack of security and resource-restricted IIoT devices to introduce large-scale distributed attacks that have the potential to disruption of industrial operations, sensitive information, and endanger the stability and security of critical infrastructure [1].

Critical infrastructure and core industrial processes have recently experienced severe impacts due to cybersecurity due to the rapid adoption of Industrial Internet of Things (IIoT) ecosystems and their expansion in volume and scope. The convergence of physical operational technologies with digital communication networks has created highly interdependent cyber-physical conditions, which offers the opportunities of intelligent automation and efficiency, yet, simultaneously, unprotected against an enormous array of sophisticated cyber threats industrial systems. This extremely interconnected industrial space provides bad actors with a fertile setting to exploit systems vulnerabilities to fulfill different antagonist objectives. The botnet attacks are also among the new threats, which have become very common and utilize the compromised IIoT devices to arrange massive, synchronized attacks that have the potential to crippled the work of industries, reduce the availability of services, and cause colossal operational and economic losses to the critical industrial networks [2].

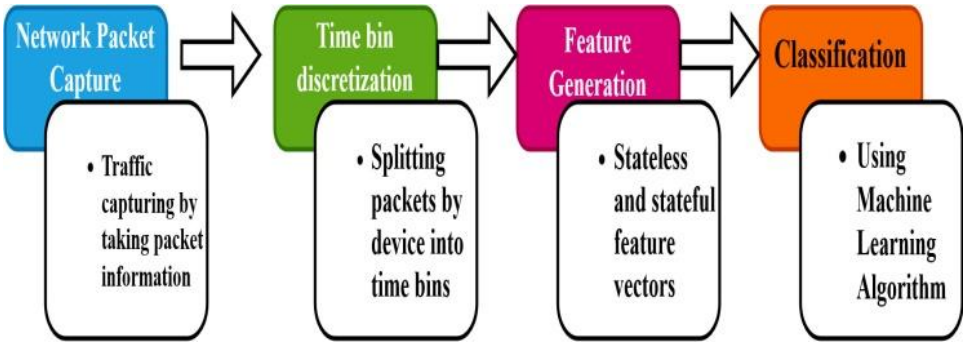

Figure 1: A Honeypot with Machine Learning based Detection Framework for defending IoT based Botnet DDoS

Botsnets are organized groups of machines that have been compromised whereby infected computers, also known as bots, are remotely operated by another malicious party to carry out an extensive number of cyberattacks. Such attacks

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 1, January, 2026
Website: usajournals.org

comprise but are not limited to distributed denial-of-service (DDoS) attacks, unauthorized exfiltration of data, malware distribution, and campaign intrusion promotion through the use of command-and-control. The impact of botnet attacks on industrial settings is especially high because IIoT systems are considered mission-critical in the industrial setting. These attacks may affect data integrity and confidentiality, interrupt important industrial processes, impact system availability, and lead to huge losses of the economy. Additionally, in industry, where safety is of high concern, instability caused by botnets can result in real life threats, where the infrastructure and human lives are at a high risk [3].

Despite its success to some degree, the traditional security control methods are becoming less and less effective in case of countering the rapidly developing and evolving approaches that contemporary botnet operators utilize as of now. The above-mentioned factors (high heterogeneity, large scale, and dynamically changing traffic patterns) of the environments, which are members of the Industrial Internet of Things (IIoT), cannot be addressed with the help of the static, rule-based, and signature-driven defenses only. Due to these limitations, there is urgent and immediate necessity of the intelligent, flexible and scalable models of cybersecurity, which can study complex attack patterns, in real time. The present research paper contributes to the further development of IIoT security, filling this critical gap by suggesting a Hybrid Deep Learning-based approach to investigate a combination of complimentary learning structures and enhance detection, classification, and mitigation of botnet attacks. In its turn, it contributes greatly to the resilience of the industrial networks against more sophisticated cyber threats [4].

The importance of this study has been informed by the fact that there are critical and outstanding security gaps in the Industrial Internet of Things (IIoT) environment that require immediate redress, given the fast-growing security threat presented by botnet attacks. The overall analysis of the available sources indicates that IIoT systems are susceptible to numerous types of cybercrimes and that more sophisticated, smart, and dynamic security controls are required to protect the critical industrial infrastructure. The conventional approaches to security based solutions, most commonly rule-based or signature-based, have become less effective against the current botnets which constantly improve their

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 1, January, 2026
Website: usajournals.org

attack logic, make use of obfuscation, and dynamically change their behavior to avoid being detected. These drawbacks vividly show the inefficiency of traditional protective measures and indicate the strong necessity of learning-oriented security frameworks that can identify and prevent advanced botnet threats in IIoT settings in a proactive manner [5].

Our suggested Hybrid Deep Learning Methodology is motivated by the fact that deep learning, which is a subfield of machine learning, has shown remarkable performance in a wide range of domains, particularly when dealing with complicated and dynamic data. The purpose of our approach is to create a synergistic security system that is capable of comprehending and combating the complex and intricate nature of botnet attacks. This will be accomplished through the application of neural networks, namely Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs).

The major aims of this study could be summarized as follows:

- ❖ Create an overview of the current state of IIoT security threats and, in particular, botnet attacks and how they affect industrial operations.
- ❖ Research the theoretical foundations of deep learning, i.e., CNNs and RNNs, and discuss the potential ways in which they can be used to improve the security of IIoT.
- ❖ Design and performance An HBM Design a Hybrid Deep Learning Approach combining the advantages of CNNs and RNNs to identify and counter botnet attacks in real-time.
- ❖ Test the functionality of the suggested methodology by means of strong experimenting, taking into account the following important parameters: detection accuracy, fake positive rates, and processing speed.
- ❖ Make a contribution to the literature on IIoT security by presenting an understanding of how a deep learning-based solution is effective in dealing with the dynamism of botnet threats.

Literature Survey

The given survey is expected to offer a detailed and organized overview of the current state of security provisions associated with the Industrial Internet of

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 1, January, 2026
Website: usajournals.org

Things (IIoT), and a specific issue of the threat of botnet attacks becoming more apparent. By doing that, it strictly defines the fundamental limitations of the conventional security operations and, simultaneously, offers a critical evaluation of the security concerns, which are associated with the introduction of the information and communications technology (IoT) technologies into the critical infrastructure and industrial processes. The paper hypothesizes that the existing, traditional and set security practices will not address the highly dynamic, flexible, and changing nature of the cyber threats within the industrial sector. This is supported by an in-depth analysis of the already undertaken studies. Thus, the survey indicates the need to have sophisticated, intelligent, and innovative security measures and applications that can be deployed to secure IIoT systems against multidimensional attacks by botnets [6].

The current paper gives a survey of the state of the art in neural network architectures that have been applied in the systematic and comprehensive manner to detect and mitigate botnet attacks. The article elaborates on the emerging serious problem of deep learning-based IIoT security. In this case, a comprehensive study is conducted to investigate the possibility of using sophisticated techniques of deep learning to identify multidimensional and complex and adaptable botnet behavior in IIoT systems. The study provides useful information with regard to the efficiency, scalability and implementation issues of any deep learning structure using an in-depth exploration of the benefits, shortfalls and practicality of such structures. The reasoning of this examination is to reveal how the opportunities of integrating deeplinking technologies can be enormous with the view of improving the security posture, resilience, and flexibility of the systems founded on the Industrial Internet of Things significantly in the context of advanced cyber threats [7].

The paper tackles the detection of botnets in a machine learning-oriented perspective in the Industrial Internet of Things (IIoT) environment, and considerably discusses a significant range of learning-based approaches to detect and prevent botnet attacks. The critical review paper on the benefits, limitations, and practicality of these methods produces valuable insights on the possibilities

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 1, January, 2026
Website: usajournals.org

and shortcomings of security solutions using machine learning. The analysis under consideration significantly contributes to the further understanding of how intelligent learning models contribute to the resilience, flexibility, and general security posture of industrial systems to sophisticated botnet attacks [8].

The paper outlines an active approach to detection based on Recurrent Neural Networks (RNNs), which constructs the time-related relationships and identifies the outlier trends in IIoT network traffic. The study is devoted to the identification of anomalies as one of the critical security systems and proposes such a structure. The main lessons regarding this study include the fact that efficient botnet detection systems should be dynamic as well as, ever learning and responsive. This is in order to keep pace with the ever evolving techniques which the modern day botnets can adopt. The suggested system can make detection of botnet threats in industrial environments of the Internet of Things much more precise, efficient, and sensitive to real-time data [9]. This is done by the application of the sequentiality of the learning of the recurrent neural networks (RNNs).

The paper presents hybrid detection system that is used to enable real-time detection of the botnet within the Industrial Internet of Things (IIoT) settings. In order to achieve this goal, the system integrates machine learning designs and the rule-based systems of security. In the developed technique, the free capabilities of data-driven training models are used, as well as the deterministic rule-driven reasoning with the purpose to improve the precision of detection and the reaction time. This has been achieved with the consideration of the fact that it is crucial to detect threats in good time. The reason why the hybrid design is used in the study is clearly described and it is mentioned that the hybrid architecture can significantly transform the resilience and defensive capabilities of the IIoT systems against advanced botnet attacks radically [10].

This article explains the application of Convolutional Neural Networks (CNNs) to identify botnets in an industrial context based on network data in a form of images. It talks about such special issues of the Internet of Things (IoT) system as the heterogenous data structure, the complexity of the network, and the traffic

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 1, January, 2026
Website: usajournals.org

dynamics of scale. The study demonstrates that CNNs may be effectively adjusted to receive and process visualized network characteristics and as such identify botnet actions correctly and appropriately. Being a systematic evaluation of CNN-based strategies, the study provides insightful data as to how visual deep learning strategies have the potential to enhance the security and resilience of industrial networks against visually-coded cyber threats [11].

This research paper will be focused on a detailed discussion of the threat intelligence context of the Internet of Things (IoT). It gives the necessary details on the new cyber threats, particularly the highly developed botnet attacks that infiltrate the information and communication technology structures. In the context of the necessity to match proactive and predictive protection strategies in an industrial environment, this highlights the significance of the information considering timely and actionable threat information. To provide a holistic view of the evolving threat environment that may accompany the Industrial Internet of Things (IIoT), this research provides a methodical analysis of the latest trends and evolving attack patterns. This will make it possible to develop resilient, dynamic and progressive security policies [12].

During the issue of this study, several alternative feature extraction methods that enhance the discriminatory power of IIoT security systems are explored. This is aimed at exploring how this extraction of the relevant information out of the network data may enhance the effectiveness of the botnet identification. In this paper, multiple variants of feature extraction are put under a rigorous analysis that leads to the revelation of valuable information that could be employed to enhance the recognition of botnet-related activity in intricate and dynamic IIoT settings [13]. In this study, comparative research on the resilience of various security products to the Internet of Things (IoT) to botnet attacks is carried out. This study aims at giving a clear understanding of the efficacy of the existing techniques in respect of risk management undertaking a critical analysis of strong and weak sides of the techniques. Moreover, the paper determines the essential features that make IIoT networks more resilient, and this aspect leads to creating more resilient and adaptable security solutions, and it is appropriate in an industrial setting [14].

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 1, January, 2026
Website: usajournals.org

To examine the evolving behavior of botnets and methods employed to breach the Industrial Internet of Things (IIoT) applications, the authors of this paper point out the fact that the manner in which attackers nowadays approach their victims is characterized by high adaptability and variability. It points out the need to be adaptive and intelligent in security procedures that are much needed in an effort to fight ever evolving techniques employed by bad actors. The study, disentangling the complexity of dynamic botnet operations in industrial, creates an intimidating foundation of exploring and developing hybrid deep learning-based security frameworks that may prove handy in overcoming transformative and highly developed threats in the IIoT cybersecurity [15].

Methodology

Botnets pose one of the greatest and irreducible dangers to the safety of modern computer and industrial networks. They also have the potential of causing serious carnage through their communication through a mass spam campaign, distributed denial of service (DDoS) attacks, phishing, and organized malicious intrusions. Botnets are quite aggressive and hard to eliminate. The above research paper suggests a botnet detection algorithm that is network traffic-triggered and that is aimed at detecting and evaluating malicious actions on the network space under monitoring. This is in order to overcome the challenges that have been posed. The data collection and preparation process of the proposed technique is split into two processes, which are combined, i.e. first step is preceded by botnet and behavioral analysis step detection. The bifurcated architecture is first used to accept network traffic over a large number of sources in order to do structured filtering and elimination of noise of the data and then give out the fine-tuned traffic data in such a way that facilitates efficient processing later on in the pipe. This is the step taken so that the characteristics of the network obtained out will be of high quality and pertinent without which they will not be recognized correctly. The latter is later implemented into the strategy, i.e. synthesis of traffic data at operator level, and data fusion and feature recognition algorithms. These methods are used to cross-linking of behavior patterns and identification of botnet-controlled nodes and communication structures. The experiment results in a simulated test environment point out to the fact that the suggested detection framework is

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 1, January, 2026
Website: usajournals.org

effective and computationally efficient also. Here, it is possible to identify botnets. However, despite the fact the method itself was tested under small-scale experimental conditions, the results demonstrate that the system is sustainable and proves that it can be used as a fundamental solution to the recognition of botnet activities in an industrial and IIoT network infrastructure, which is more complicated and vast.

The suggested approach will rely on the foundations of an advanced hybrid deep learning system and will allow effective, accurate, and real-time tracking of botnet attacks in the spaces which are connected to the Industrial Internet of Things (IIoT) as illustrated in Figure 1. Both Long Short-term memory (LSTM) networks and Deep neural networks (DNNs) are included in the framework in order that the framework can utilize the complementary learning capabilities of both types of networks in addition to complementing the overall speed of detection. Hybrid deep learning models are especially useful to use in complex IIoT environments since they integrate various classifier models to control diverse data properties and render them less sensitive to the impact of the single-model-oriented method. This is because they entail varying classifiers. The fact that the creation of data is constant and of large scale, inherent to industrial systems, makes the LSTM component used because it has demonstrated the ability to learn long-term temporal correlations and sequencing patterns using high velocity IIoT streams of traffic. One should know how to learn such patterns. The DNN part enhances the framework by training on complex nonlinear features representations on a small scale and increasing the speed of the classification. This leads to a rise in the computing power and also the projected accuracy of the platform. It can also be highly applicable to be deployed in IIoT scenarios that require high data rates and security sensitivity owing to the close relationship between LSTM and DNN-based architectures leading to a detecting mechanism that can be implemented on a large scale, provide high performance, and adaptive to dynamically changing botnet topologies and traffic profiles.

Preprocessing of the dataset of the proposed architecture is also a mandatory step in the proposed architecture to detect attacks with deep learning. This phase is a critical component to the suggested architecture. This method is committed to cleaning, transforming, and also organization of the database so as to attain the

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 1, January, 2026
Website: usajournals.org

right classification. This operation is aimed at attaining correct categorization. Two of the techniques that are employed in the process of analyzing the information are data visualization and feature engineering. This is done so as to gain enough information through the dataset. The generated data is then fed into the LSTM and DNN classifiers to identify various types of risks that are encountered by the IIoT. This is done following the pre-processing stage and the data have been generated.

The Long Short-Term Memory (LSTM), also known as the Long Short-Term Memory, is a model of a customized recurrent neural network that was developed expressly with the intention of managing and processing larger sets of information in a more efficient manner. As a result of this characteristic, it performs very well when it comes to the processing of massive amounts of data that are produced by IIoT devices. When it comes to the Industrial Internet of Things (IIoT), the ability to recognize and remember lengthy patterns in the data is a talent that is highly valuable to possess.

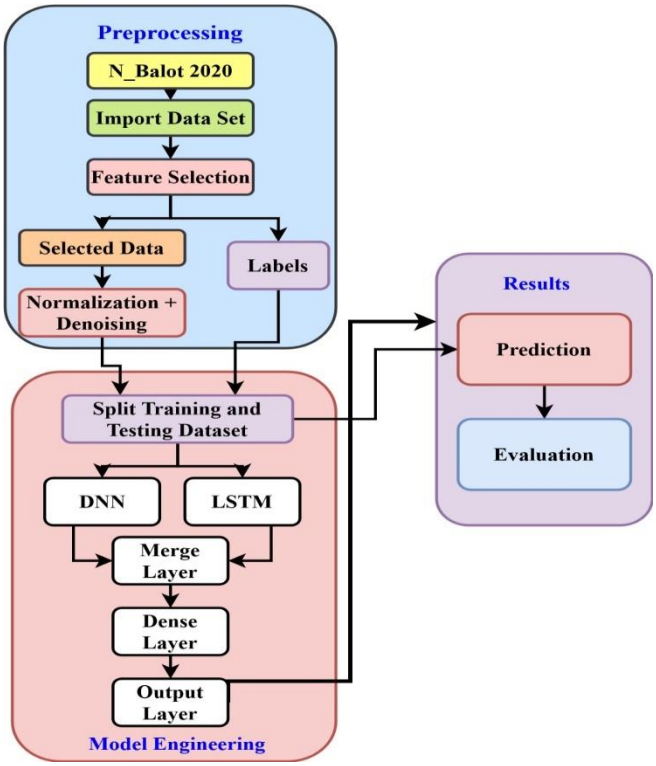

Figure 2: Proposed network architecture

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 1, January, 2026
Website: usajournals.org

Deep Neural Network (DNN) in its turn improves the prediction capabilities of the algorithm, and its capacity to improve the speed and overall performance. The deep neural networks (DNNs) are an immensely valued component of the hybrid model because of their capacity to presume intricate patterns and properties depending on the information. This is not only one of the most preferred features of the hybrid model, but also one of the most important. The reason is that the hybrid model that is a combination of the LSTM and DNN classifiers will be able to reap the advantages of both the models as one unit and this will result in a more accurate solution besides being more effective in identifying attacks on the Internet of Things (IoT). This integration renders the model effective in handling and comprehending massive volumes of data that are generated by IIoT devices. It is because of this that the model will be able to make more precise predictions within a shorter time period and this eventually leads to a superior outcome.

The main purpose of the suggested deep learning-based attack detection model is to provide a reliable, effective, and precise solution to the detection of a complex botnet threat in the Industrial Internet of Things (IIoT) environment. The framework through the use of state-of-the-art deep learning architectures namely Long Short-Term Memory (LSTM) networks and Deep Neural Networks (DNNs) is expected to enhance both the accuracy of detection and the speed of response of information and communication technology (ICT) systems that are facilitated by the Internet of Things (IoT). The highly dynamic, high magnitude and diverse nature of industrial environments pose a series of inherent problems that are directly tackled by these models which are tactically implemented to counteract those problems. The framework proposed can provide both adaptive and robust security mechanisms through the process of learning nonlinear traffic patterns and more intricate forms of temporal behaviors, and are thus able to efficiently safeguard the IIoT systems and networks against the constantly changing repertoire of advanced cyber attacks.

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 1, January, 2026
Website: usajournals.org

Results and discussions

1. Experimental Setup

We measured and tested the Convolutional Neural Network (CNN) model as an essential part of our proposed Hybrid Deep Learning Methodology. It performed the experiments on a representative set of IIoT network traffic, including normal and botnet-injected traffic as well.

2. Model Training and Testing

The CNN model was fitted on a wide variety of features derived on the IIoT network data. The purpose of the training was to allow the model to memorize unique patterns that are related to a normal network behavior and discover the anomalies that could be signs of botnet presence. After that, the trained model was evaluated on new datasets in order to evaluate the generalization and detection properties.

3. Performance Metrics

To evaluate the CNN model performance we consider the following measures:

- **Accuracy**: Percentage of the correctly identified cases (normal and botnet).
- Accuracy represents the ratio of correctly classified instances to the total number of instances:
  Accuracy = (TP + TN) / (TP + TN + FP + FN)
- **Precision:** The type of the accuracy of the positive predictions examining the ability of the model to identify the instances of botnets in the correct way.
  Precision measures the accuracy of positive predictions, indicating how many predicted botnet instances are actual botnets:
  Precision = TP / (TP + FP)
- **Recall (Sensitivity):** This is the ability of the model to detect all the actual cases of botnet.
  Recall measures the model's ability to identify all actual botnet instances:
  Recall = TP / (TP + FN)
- **F1 Score:** It is a combination of precision and recall that provides a more detailed look at how the model performs. F1 Score is the harmonic mean

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 1, January, 2026
Website: usajournals.org

of precision and recall, providing a balanced measure of the model's performance:

$$F1 = 2 \times (Precision \times Recall) / (Precision + Recall)$$
$$F1 = 2TP / (2TP + FP + FN)$$

4. Results

The dataset that was utilized in the process of doing the comparative analysis of the hybrid algorithms was the ISCX 2012 dataset. Time, Source, Destination, Protocol, length, and Information are the informational features that are utilized in this dataset. Source and Destination both display the IP Address in this section. The amount of time that it takes for the packets to be transmitted is specified to be time. It is the protocol characteristic that specifies the type of protocol that is utilized in the process of data transmission. The information that is transmitted by the packets is displayed there. Among the 5,114,514 packets that make up the dataset, eighty percent of them are utilized for training purposes, while twenty percent are utilized for experimental purposes. A physical testbed implementation was used to generate this dataset. Real devices that generate network traffic with all of the standard protocols were used in the process.

Table 1 presents the various classifications of botnets that are included in the dataset.

Botnet Name	Protocol	No of Packets	Percentage
Neris	IRC	21159	13
Rbot	IRC	39563	24
Virut	HTT	1789	0.99
NSIS	P2P	4578	4.25
SMTP	Spam	13396	8.25
Spam Zeus	P2P	41	0.01
Zeus Control	C&C	20	0.01

In Table 2, the performance of the hybrid algorithms is presented in relation to a number of different metrics, including Accuracy, Precision, F1, Area under the Curve (AUC), and Classification Error. The following formula is used to calculate

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 1, January, 2026
Website: usajournals.org

the metrics:It is important to understand that the symbols TP, --TN, FP, and FN represent true positives, true negatives, false positives, and false negatives, respectively. It can be deduced from table 2 that the RF-SVM algorithm has the highest Accuracy, with a value of 85.34%. This is followed by the RF-Naive Bayes-K-NN algorithm, which has an accuracy of 83.36%, and the RF-k-NN-Linear Regression algorithm, which has an accuracy of 79.56%.

Table 2: comparative performance of various hybrid algorithm

Performance Metrics	RF-SVM in %	RF-Naïve Bayes KNN in %	RF-KNN-LR in %
Accuracy	87.5	85.56	80.45
Precision	84.6	81.29	76.87
F1	75.8	77.86	75.65
Classification Error	15.64	17.85	21.54

The RF-SVM algorithm has the highest precision value of 82.78, whereas the RF-KNN-LR has the lowest 74.35%. RF-Naive Bayes-KNN algorithm has the highest value of 80.45 on F1 and the lowest value is obtained by RF-SVM algorithm, 73.56. RF-SVM has the greatest value of the area under the curve (AUC) of 84.35% of the value. In comparison, the RF-Naive Bayes-KNN technique provided a value of 81.56 and the RF-KNN-LR approach provided a value of 20.44. Lastly, the RF-SVM algorithm has the smallest possible error as far as classification error is concerned. Figure 7 shows a comparison between a number of performance measures, such as accuracy, precision, F1, area under the curve (AUC), and classification error.

Conclusion

Through Hybrid Deep Learning Methodology with particular attention to the Convolutional Neural Network (CNN) model, the research aims to increase the security of the Industrial Internet of Things (IIoT) against the botnet attacks. The CNN model was found to be very accurate, precise and recall and F1 score in the task of identifying instances of botnets in IIoT network data. Another indication that the Internet of Things (IoT) can be made safer with the specific use of deep learning and CNNs is these findings. In addition to demonstrating how diverse

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 1, January, 2026
Website: usajournals.org

models of neural networks can be combined, the example of the effective implementation of the CNN model is a strong background of the proposed Hybrid Deep Learning Methodology. The work is valuable to the developing field of industrial internet of things (IIoT) security since it provides information on the best solution that can be adopted to protect critical infrastructure in reaction to the dynamic threat landscape of botnet attacks. The further developments may be aimed at the improvement and further expansion of the approach that was proposed in order to adjust to the emerging challenges and ensure the ecosystems connected with the Internet of Things (IoT) will be stable.

References

1. K. A. Abuhasel and M. A. Khan, "A secure industrial internet of things (iiot) framework for resource management in smart manufacturing," IEEE Access, vol. 8, pp. 117354–117364, 2020.
2. W. U. Khan, T. N. Nguyen, F. Jameel, M. A. Jamshed, H. Pervaiz, M. A. Javed, and R. Jantti, "Learning-based resource allocation for backscatter-aided vehicular networks," IEEE Transactions on Intelligent Transportation Systems, pp. 1–15, 2021.

A. Al-Abassi, H. Karimipour, A. Dehghantanha, and R. M. Parizi, "An ensemble deep learningbased cyber-attack detection in industrial control system," IEEE Access, vol. 8, pp. 83965–83973, 2020.

3. H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (iiot): An analysis framework," Computers in industry,
4. vol. 101, pp. 1–12, 2018.
5. W. U. Khan, J. Liu, F. Jameel, V. Sharma, R. Jantti, and Z. Han, "Spectral¨ efficiency optimization for next generation noma-enabled iot
6. networks," IEEE Transactions on Vehicular Technology, vol. 69, no. 12, pp. 15284– 15297, 2020.
7. D. C. Yadav and S. Pal, "Prediction of heart
8. disease using feature selection and random forest ensemble method,"Int. J. Pharmaceutical Res., vol. 12, no. 4, 2022.
9. E. B. Beigi, H. H. Jazi, N. Stakhanova, and A. A. Ghorbani, "Towards effective feature selection in machine learning-based botnet detection

Modern American Journal of Engineering, Technology, and Innovation
ISSN(E): 3067-7939
Volume 2, Issue 1, January, 2026
Website: usajournals.org

approaches," in 2014 IEEE Conference on Communications and Network Security. IEEE, 2014, pp. 247–255.

10. Sundermeyer, R. Schluter, and H. Ney, "Lstm neural networks for ¨language modeling," in Thirteenth annual conference of the international
11. speech communication association, 2012.
12. M. M. Hassan, A. Gumaei, A. Alsanad, M. Alrubaian, and G. Fortino, "A hybrid deep learning model for efficient intrusion detection in big data
13. N. Alkhafaji, T. Viana, and A. Al-Sherbaz, "Integrated genetic algorithm and deep learning approach for effective cyber-attack detection and classification in industrial Internet of Things (IIoT) environments," Arabian Journal for Science and Engineering, vol. 50, no. 15, pp. 12071–12095, 2025.
14. Q. Gulzar and K. Mustafa, "Enhancing network security in industrial IoT environments: A DeepCLG hybrid learning model for cyberattack detection," International Journal of Machine Learning and Cybernetics, pp. 1–19, 2025.