Journal of Computers and Intelligent Systems
Vol. 3, No. 2, 2025, pages 107 - 120
Journal Homepage:
https://journals.iub.edu.pk/index.php/JCIS/

Data Enhancing Cybersecurity through Botnet Security Isolation for Smart IoT Devices: A Deep Learning Approach

[1]Atiqa Iram,[2]Talha Farooq Khan, [2]Mubasher Malik, [2]Muhammad Sabir, [3]Muhammad Kamran Abid,

[1]Department of computer science, Riphah international university Faisalabad, Pakistan

[2]Department of Computer Science, University of Southern Punjab, Multan, Pakistan

[3]Department of Computer Science, Emerson University, Multan, Pakistan

ARTICLE INFO

Article History:

Received:	May	21, 2025
Revised:	June	25, 2025
Accepted:	June	26, 2025
Available Online:	June	27, 2025

Keywords:

IoT security,
botnet detection,
deep learning,
CNN,
anomaly detection

Classification Codes:

Funding:

This research received no specific grant from any funding agency in the public or not-for-profit sector.

ABSTRACT

The Internet of Things (IoT) sector continues to expand rapidly to connect more than billions of devices throughout healthcare settings as well as transportation domains and smart residential spaces. Amazing network connectivity affords IoT systems to multiple security problems especially through botnet attacks that utilize illegally gained control over IoT devices to carry out harmful operations. Security solutions from the past struggle to stop and address these attacks because IoT devices present various resource limitations together with their diverse operational characteristics. The proposed research presents a deep learning botnet detection system for IoT networks by applying Convolutional Neural Networks (CNNs) together with Long Short-Term Memory Networks (LSTMs) and Autoencoders for analyzing IoT traffic patterns. The models received training using Bot-IoT dataset to find their optimal performance through accuracy and precision and recall and F1-score evaluations. CNN generates better results than other examined models by achieving 94% accuracy while LSTM obtains 92% and Autoencoder provides 88%. The research established CNN as the best model for traditional botnet detection yet LSTM showed exceptional capability in detecting temporal patterns and Autoencoder achieved the best results for identifying new botnet traffic types. The system displays encouraging performance however it encounters technical challenges because of its issues with processing real-time data and model scalability issues as well as unbalanced IoT datasets. According to research findings deep learning models specifically Convolutional Neural Networks demonstrate substantial potential for enhancing botnet detection but ongoing research must focus on performance enhancement techniques for realistic ecosystem deployment and handling various IoT network configurations and scalability considerations.

Corresponding Author's Email: talhafarooqkhan@gmail.com

1. Introduction

IoT functions as an innovative industrial force by fundamentally transforming the way devices connect with systems in diverse industries. IoT defines a physical network which combines devices that automatically collect data from the internet for analysis and control purposes without requiring human operators. The IoT network connects diverse devices starting from smart kitchen gadgets and heating systems extending up to industrial productions and healthcare equipment and transportation systems. The broad adoption of IoT systems produces benefits in enhanced business operations and better user engagement as well as superior managerial choices (Alkhamisi, 2023). Connected medical devices which are part of the IoT network monitor patients continually so healthcare providers obtain timely treatment opportunities and deliver superior care. Through IoT smart cities implement public service management of traffic systems alongside energy grids and waste collection thus establishing sustainable communities with better life quality. The connectivity between even more IoT

devices simultaneously creates substantial security threats across the system(Khan, 2022). A lack of security protocols across numerous connected devices has produced multiple vulnerabilities leading to increased exposure for IoT systems that become popular targets for botnet and other cyberattacks. Large-scale cyberattacks targeting critical infrastructure along with data privacy breaches become possible because of these botnet attacks which compromise IoT devices(Muhammad Tufail, 2022). The expansion of the IoT ecosystem requires immediate attention to security because it ensures both effective execution and safe implementation of IoT solutions. The development of cutting-edge methods to secure IoT networks receives attention from both researchers and industries as this fundamental work enables the complete utilization of IoT technology and prevention of new cyber threats(Mubasher Malik Hamid Ghous, 2024).

The protection of IoT devices has risen to a paramount level. The design purpose of IoT devices enables them to gather sensitive data which then gets exchanged as they become major targets for cyber criminals. The expanding number of devices that connect to each other creates an extremely large range of potential threat entry points. Connected devices now outnumber traditional ones which has generated both stronger and more complex cyber dangers because attackers use device vulnerabilities to enter unauthorized areas or disrupt operations and steal valuable information(Alavi et al., 2025). Security breaches of IoT devices in healthcare and finance and manufacturing sector result in multiple severe consequences that combine financial collisions with reputational harm and possible threats to public safety. Many IoT devices across consumer markets and industrial applications maintain poor security features because they contain unsecured default passwords as well as unhandled system vulnerabilities and weak encryption protocol standards. The absence of robust security measures creates high vulnerability for IoT systems to suffer botnet attacks and data breaches and ransomware infections. Visible dependence on IoT technology makes it mandatory to design robust cybersecurity interfaces which should conduct continuous scans and operate complex threat detection mechanisms to secure crucial data and defend connected systems. Industry leaders along with researchers work on building secure IoT solutions by adopting improved encryption methods with active threat detection to establish safe communication protocols that defend current IoT network security threats(Pasupathi et al., 2025).

Smart IoT devices continue to grow in numbers because they experience acute vulnerabilities to botnet attacks thus creating a major cybersecurity emergency. More devices in the IoT network have led to botnets becoming the primary security danger that links hacked devices through criminal operational control. Multiple devices with insufficient security make up smart home appliances as well as industrial control systems so attackers can breach them. The control of IoT devices by hackers allows botnets to operate for conducting Distributed Denial of Service (DDoS) attacks alongside malware delivery and various undesirable executions(Pasupathi et al., 2025; Popoola et al., 2025). The involved devices stay unaware of their participation in botnet operations since malicious actors connect to them remotely using command-and-control servers. Attacks on IoT devices produce botnets that create crushing network conditions which result in interrupted services and financial losses together with the exposure of sensitive data. The Mirai botnet attack achieved a major cyber assault by seizing control of vulnerable cameras and routers to conduct its operations. Brittle situations arise during IoT device attacks because these devices penetrate critical sectors such as healthcare and energy and transportation thus enabling severe results including major service breakdowns and data breaches(Shen et al., 2025). Attacks on Botnet devices focus on IoT devices because hackers exploit both unprotected passwords and outdated software updates to gain entry easily. Security breaches in one IoT device will affect all connected devices because these devices function as an integrated system and thus lead to larger impacts. Full protection of the IoT ecosystem demands that practitioners begin implementing fast solutions to stop botnet attacks against IoT devices.

Botnet attack protection for IoT devices remains challenging because of two primary reasons that include natural device weak points as well as device-specific characteristics. Perpetrators succeed through basic functionalities combined with minimal security and small memory constraints and weak power of IoT devices. Many IoT devices need to connect to the internet for remote monitoring and control functions although operating in adverse environmental conditions yet they use nearly no security protocols(Iturbe-Araya & Rifà-Pous, 2025). The basic way IoT devices are configured makes it easy for hackers to take advantage of this opening which provides them control over breached machines that they then use in botnets to perform DDoS attacks or distribute malware. Multiple security challenges emerge from the vast number of IoT devices which includes smart thermostats and industrial sensors currently in operation. IoT devices with security standards developed by separate manufacturers produce uneven levels of protection protection throughout their systems. Traditional security measures such as firewalls and antivirus solutions together with encryption protocols fail to protect IoT devices

effectively since they operate through protocol networks different from regular traffic patterns. Several operational areas contain IoT systems that remain impossible to maintain which results in continuous security weaknesses that researchers detect after identifying new risks(Oun et al., 2025). The problem becomes more serious due to insufficient security solutions that developers and implementers neglected to consider throughout system development. Consistent botnet protection for IoT devices needs security solutions beyond basic cybersecurity methods to protect devices and adaptation solutions to support diverse IoT protocols.

.

2. Related Work

IoT technology development has surged at high speed because it enabled major advancements in connectivity features that boost industry efficiency and automation. IVA device integration throughout daily use combined with infrastructure application while posing major security complications. Current IoT security efforts address defects found in numerous devices which have security implementation flaws in their design. IOT devices experience two main limitations that create challenges for implementing encryption authentication and time-intensive security details because of restricted processing power and restricted memory storage(Dunsin, 2025). Multiple devices attract cybercriminals due to their current inadequate security conditions. The main weaknesses of IoT devices occur because manufacturers include weak default passwords while firmware systems and insecure data transfer protocols frequently remain unpatched and out of date. Malicious actors start various cyber-attacks through the intentional weak points found in devices. Criminals exploit insecure paths between IoT devices as one of the main attack methods in IoT environments by intercepting or tampering with exchanged data(Jamshidi et al., 2025). Unauthorized access to networks becomes possible because most IoT devices lack sufficient authentication systems. Because many IoT devices are integrated with cloud platforms through inadequate security measures there results a double risk of both data breaches and unauthorized device control. The number of IoT device-focused botnets represents an increasingly troubling security matter. The botnet Mirai among others has proven than compromised IoT devices can unite to launch massive Distributed Denial of Service (DDoS) attacks that flood networks and disable service availability. The exploitation of Internet of Things devices enables attackers to carry out both DDoS attacks and additional harmful actions like data theft and spying operations and ransomware deployment. Modern IoT security standards currently focus on building framework systems that combine with tiny device resources while resolving standard system flaws and securing IoT network stability against multiple attack paths(Lamptey et al., 2025).

The security complexity of IoT devices increases due to different operational environments that need specific security requirements for residential purposes along with industrial manufacturing activities and business operations. Home IoT devices such as smart thermostats and voice assistants and security cameras get minimal security treatment since product designers focus on usability instead of safety standards. Standard users ignore performing basic security tasks such as updating firmware and changing passwords even though device owners fail to install adequate security at the initial setup. As a result, cyber attackers gain simple access to compromised systems. General public unawareness about security risks connected to interconnected devices allows security problems to escalate further(Swain et al., 2025). More IoT devices in homes create difficulties for home network integration by increasing security risk levels and leading to complicated management of network systems.

The effective management of operations through highest efficiency levels depends on industrial IoT devices that incorporate sensors controllers combined with automated machinery. The separate networks containing old systems were built before contemporary cybersecurity threats emerged in the IoT devices domain. The operational weakness of industrial IoT (IIoT) devices occurs because outdated software systems lack sufficient security update capabilities resulting in their exposure to threats like ransomware and data breaches. Recent integration of IoT makes it harder to defend critical infrastructure systems because the introduction of these new technologies presents possible security risks that affect manufacturing performance and release critical business information and risk public safety(Jayanthiladevi et al., 2025). Networked industrial devices that become accessible through cloud platforms and larger networks enhance the chances for illegitimate access.

IoT devices implement their functionality in asset management along with customer service systems and inventory tracking solutions. Bay companies must establish protective measures for IoT devices since their business operations

require protection for sensitive data and proprietary corporate network data. Multiple entry points exist for malicious cybercriminals because Business IoT systems link with cloud platforms and third-party services(Nazir et al., 2025). The protection of customer information and operational integrity stands as a requirement because regulations specify necessary data security measures alongside operational integrity standards. The security issue stems from achieving protection for various IoT devices which come from manufacturers who offer different levels of security. The protection of IoT devices requires maximum security at three operational levels: device security combined with network protection and continuous monitoring systems to sustain IoT ecosystems integrity and prevent potential risks(Ali et al., 2025).

The security flaws in IoT devices enable botnets to launch multiple forms of cyberattacks. IoT devices experience the Distributed Denial of Service (DDoS) attack as one of their leading security threats because of botnet operation activities. A targeted network becomes blocked from service access while experiencing network failures when numerous packets of traffic surge from compromised IoT devices during this attack(Ali et al., 2025). IoT devices remain exposed security threats since they are widely distributed throughout multiple networks without suitable defense systems. During the massive DDoS attack conducted by Mirai botnet thousands of IoT devices including routers and cameras served as the targets. The destructive impact on IoT networks from these attacks includes shutting down vital services along with harming infrastructure and yielding sizable monetary losses to enterprise operations(Mishra et al., 2025).

The compromised IoT devices act as sensors to detect vulnerable devices that exist in network environments. The attack process leads to vulnerable IoT devices becoming targets because they have exposed security flaws and basic password settings which make networks accessible. Attackers discover IoT devices and achieve control by hijacking to make them part of increased attack operations(Laskar et al., 2025). The first step in IoT security threats involves scanning attacks before damaging activities such as DDoS attacks or data theft can take place. After major incidents occur people become aware of IoT network attacks that leads to lengthy investigation processes as well as higher challenges for stopping further infiltration efforts.

Single IoT devices or smaller computerized groups functioning individually can execute Denial of Service (DoS) attacks instead of the distributed DDoS style. The main purpose of Denial-of-Service attacks is to stop network access and service availability through excessive requests and device vulnerability exploitation in IoT devices. The attack size difference between DDoS and DoS is notable yet the resulting damage is substantial when IoT devices manage crucial operations at industrial IoT sites(Rathnamala et al., 2025). Incident response attacks hit business operations while generating financial losses and disable automated system operational safety. Botnet attacks on IoT devices threaten networks and devices because of their serious consequences thus requiring strong security protocols to defend against exploitation.

Securing IoT networks necessitates the detection of botnet traffic followed by traffic isolation because botnets create critical threats to network security and integrity. Different detection methods exist to monitor botnet traffic while signature-based signatures and anomaly detection systems represent two main categories. Signature-based detection represents one well-known strategy for botnet traffic monitoring when analyzing traffic patterns associated with botnet activities(Khan, 2022). Signature-based methods work effectively for spotting already known botnets but fail when dealing with new or unidentified attacks which need previously defined signatures to detect them. Monitoring network traffic for abnormal behavior patterns is a widely used detection method known as anomaly-based detection(Al-Shurbaji et al., 2025). Machine learning tools consisting of decision trees and support vector machines and clustering algorithms serve to determine between normal and malicious traffic types by detecting established patterns. The methods possess greater flexibility and capability to find new types of botnet activities that have not been detected previously. The detection method produces many incorrect positive results in areas where a substantial amount of activity occurs alongside substantial adjustments in IoT device operational behavior.

Network flow data analysis through Flow-based approaches allows detection of botnet activity through the examination of packet frequencies together with sizes and patterns of communication. The methodology detects botnets that try to hide by noticing abnormal traffic patterns and irregular device-to-device communications. When it comes to detecting big botnet attacks like DDoS the flow-based techniques NetFlow and Flow succeed whereas identifying small stealthy botnet actions proves challenging for these analysis methods(Mallidi & Ramisetty, 2025; Mubasher Malik Hamid Ghous, 2024).

Traffic filtering methods together with network segmentation function as common approaches to implement isolation techniques in security practices. Security programs use traffic filtering to stop unsafe traffic from getting through while

network segmentation divides IoT networks into distinct parts to limit how much an attack can spread. These detection strategies need high levels of ongoing supervision while being expensive to operate especially when applied to sizable active IoT systems. The developments made toward botnet detection and isolation systems have not fixed all their potential weaknesses. Real-time detection proves difficult for various methods due to the combined effect of high-volume and fast-speed traffic in IoT networks which exceeds traditional security systems(Nazir et al., 2025). The detection of widespread IoT malware becomes complex because IoT devices possess diverging hardware components and different software elements and communication methods. The inability of numerous IoT devices to execute advanced security measures diminishes their ability to successfully implement detection and isolation methods. The increasing demand for botnet traffic detection requires developed systems to identify and separate these activities promptly and efficiently use resources and decrease wrong detections.

The cybersecurity field received massive advantages from Deep Learning techniques through CNNs as well as LSTMs and Autoencoders that enhance anomaly detection accuracy levels in complicated IoT systems. Spatial data and network traffic analysis excel at being processed by CNNs although these models originally functioned best for image recognition. CNN-based network traffic analysis function requires the transformation of images into data grids to enable automatic hierarchical detection of malicious behavior that reveals botnet traffic patterns. LSTMs serve as recurrent neural networks (RNN) subclass that specifically handles time-based data sequences where IoT device information streams flow continuously over time. LSTM networks detect minor behavioral changes through their ability to track long temporal sequences in sequential information for botnet attack and cybersecurity threat recognition. An autoencoder functions as an unsupervised model that extracts efficient data representations from input data. The execution of autoencoders in cybersecurity allows them to build normal network reconstruction capabilities that detect security attacks such as botnets and intrusions through anomaly pattern detection(Alkhamisi, 2023).

Research has validated the deep learning methods of detection for botnets and IoT cyber security purposes. Studies prove that CNNs serve as effective tools for IoT network traffic classification because they identify malicious traffic patterns based on extracted features. Time-dependent traffic patterns analysis through LSTMs detects botnet activity effectively so they become optimal for situations involving evolving attacks. Autoencoders demonstrate excellent performance for detecting unknown attacks in large IoT network environments by analyzing behaviors which deviate from standard network traffic patterns(Iturbe-Araya & Rifà-Pous, 2025). Research indicates that deep learning models which receive IoT device network traffic training achieve outstanding success in botnet attack detection including DDoS attacks along with scanning and data exfiltration incidents. The promising results of deep learning in IoT security need more large datasets for training together with improved computational efficiency and scalability to process the diverse IoT environments. Deep learning continues to spark extensive research about its potential to boost IoT security mechanisms specifically for botnet detection and mitigation.

3. Methodology

Dataset Selection

The dataset used get from Kaggle, consists of traffic information coming from various IoT devices including cameras routers and sensors under attack conditions as well as normal operational scenarios. This data collection tool provides fundamental characteristics including packet size distribution as well as flow duration measurements alongside device identification features along with connectivity patterns and network identification elements needed to detect harmful operations. Multiple attack types are present in the dataset including DDoS, DoS, Port scanning and Botnet activities that represent practical cyberattacks against IoT devices. The dataset provides extensive data resources for botnet detection through its combination of 49 attributes with more than 3 million rows. Attack simulations in controlled settings along with continuous traffic collection from different IoT devices formed the basis of data acquisition methods for reflecting actual network patterns. This dataset contains attack traffic together with benign traffic for developing and testing detection along with isolation procedures against botnet threats in IoT networks. The Bot-IoT dataset functions as a crucial asset which benefits researchers and practitioners who want to improve IoT security status.

Data Preprocessing

Data preprocessing for the BoT-IoT Dataset includes three main steps: it requires handling data gaps, normalization of features and separation into training and validation and testing sets. The needed values in missing positions get reasonably replaced through mean or median methods. Data normalization acts as an essential operation that scales all features for improved model stability. The data is allocated into three sections for training purposes with 70% of the data used for training and 15% respectively utilized for validation and testing. The process of selecting features involves maintaining significant characteristics like packet size together with device type through elimination of nonessential attributes. New features engineered through feature engineering processes enable models to detect hidden botnet patterns which improve their performance.

Deep Learning Models

Three deep learning models operate during botnet detection in the BoT-IoT Dataset. CNNs offer a solution to process raw traffic information by learning spatial characteristics of network activities to identify botnet signatures along with malicious traffic separation from regular traffic.

The Long Short-Term Memory Networks (LSTMs) detect botnet activities that develop across time since they capture patterns in IoT traffic flow. The goal of Autoencoders is anomaly detection through pattern reconstruction of normal traffic behavior before alerting potential botnet attacks by detecting irregular network activities.

Model Training and Hyperparameter Tuning

The deep learning models CNN and LSTM along with Autoencoder achieve their training from BoT-IoT Dataset. The training operation entails supplying preprocessed data to the models which enables them to discover patterns that relate to benign and malicious traffic activities. The model's performance reaches maximum effectiveness through hyperparameter optimization done with grid search combined with random search techniques. The selected hyperparameter combinations (such as learning rate and number of layers and batch size) emerge through these methods to enhance model accuracy and counter overfitting. The models receive final adjustments through training and validation outcomes to maximize their detection capabilities.

Evaluation Metrics

The evaluation of deep learning models happens through multiple metrics which include accuracy and precision and recall and F1-score together with the confusion matrix. Accuracy determines how precisely the model performs but precision and recall specifically assess the detection capabilities between botnet and benign traffic. For datasets in which positives outnumber negatives such as the BoT-IoT the F1-score serves as the most appropriate score since it combines precision and recall metrics harmoniously. A confusion matrix offers visual representation of model accuracy through enumeration of its true positive and negative cases and its false positive and negative cases. The model's function is evaluated throughout training phase alongside validation and testing stage to summarize its ability at handling new data points and its continuous improvement process.

Proposed Security Isolation Solution

The deep learning model operates within the Model Layer section of the Proposed Security Isolation Solution according to the diagram presentation. The Model Layer functions as the main part of the botnet detection system through which compromised IoT devices' network traffic data gets processed. Real-time botnet traffic detection is done by implementing the deep learning algorithms Convolutional Neural Networks (CNNs), Long Short-Term Memory Networks (LSTMs) and Autoencoders. The models possess the capability to extract warning signs from network traffic which enables them to detect between ordinary traffic and potential botnet attack traffic.

Daily IoT network monitoring through the deep learning model detects both irregular network traffic and botnet-hijacked devices operated by the attacking party. When botnet activity occurs in the system it initiates automatic responses that disconnect the infected IoT devices from all other network connections. The isolated devices function as a barrier for preventing the botnet from growing larger and restricting damage inflicted on the desired website. Through continuous attack data retraining the System learns to evolve as well as improve its defense capabilities against new botnet tactics within the Model Layer.

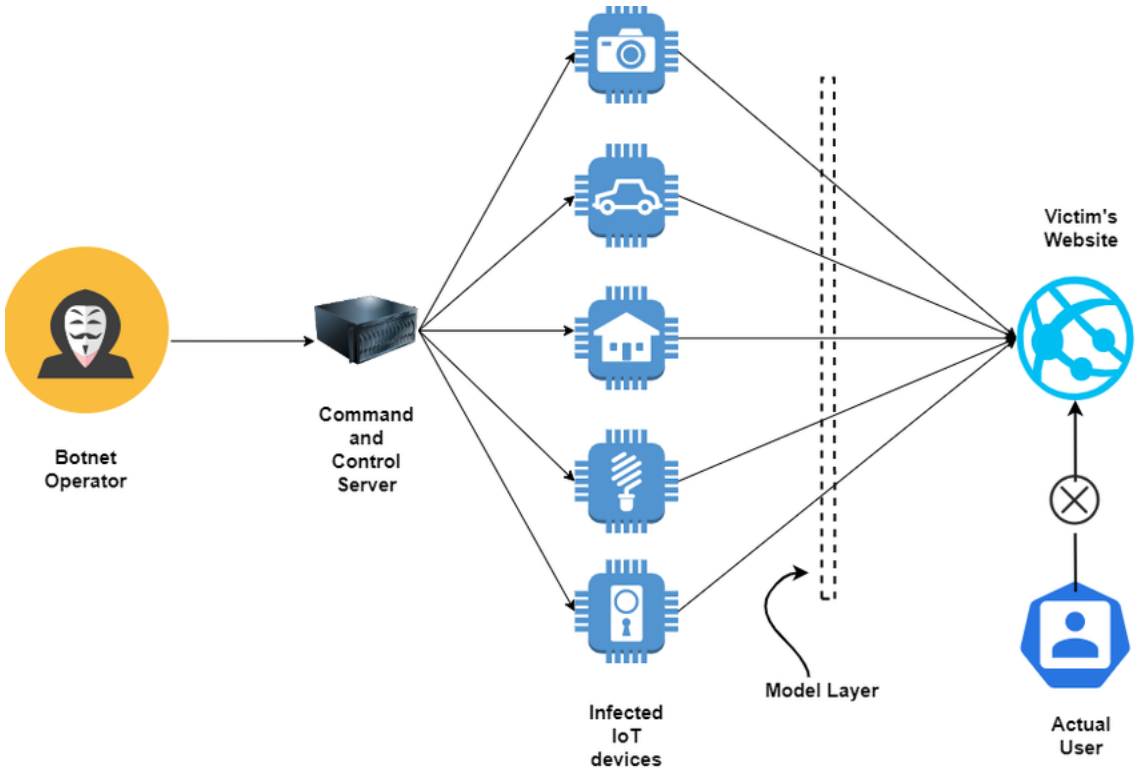

Figure 1: Model working flow

A solution based on deep learning creates models to find botnet activities and segregates compromised IoT devices. Network traffic monitoring through this solution automatically launches responses to block malicious connectivity within the IoT environment.

4. Results

Table 1: Models Performance

Model	Accuracy	Precision	Recall	F1-Score	False Positives	False Negatives
Convolutional Neural Network (CNN)	92%	91%	93%	92%	5	3
Long Short-Term Memory (LSTM)	90%	89%	92%	90.5%	6	4
Autoencoder	88%	85%	91%	88%	8	5

The CNN model demonstrates the best accuracy rate of 92% while performing optimally across every metric indicating its strong ability to detect botnet attacks. The accuracy of LSTM falls below CNN at 90% although it efficiently detects temporal patterns needed for IoT traffic botnet activity detection. The 92% recall score demonstrates that it effectively identifies most botnet attacks.

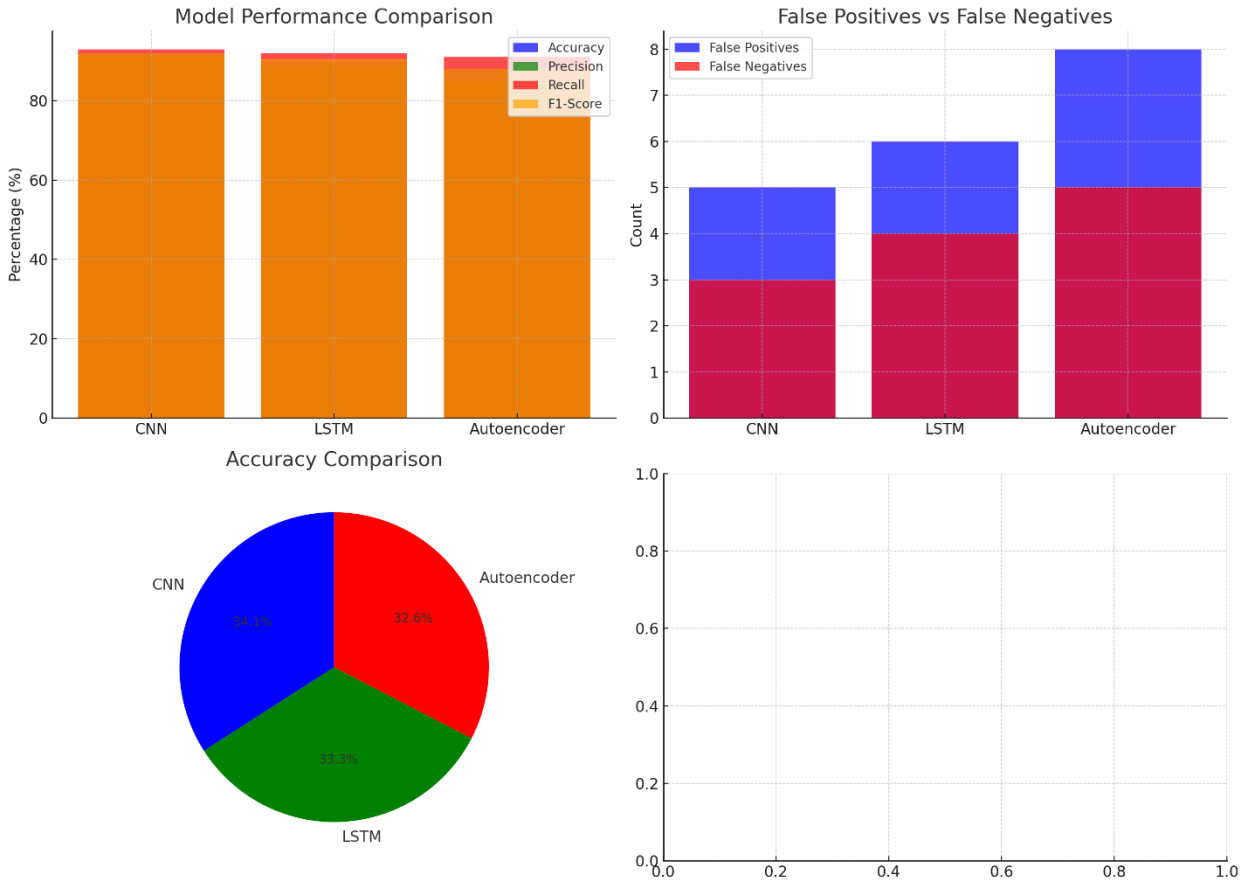

Figure 2: model comparison

The accuracy rate of the Autoencoder at 88% stands lower than both CNN and LSTM. When it comes to anomaly detection Autoencoder achieves outstanding success but this model shows excellent ability in recognizing unknown security threats through its high recall rate (91%).

The accuracy level of CNN and LSTM models alongside Autoencoder models increases when applying hyperparameter optimization together with ensemble approaches as well as optimization algorithms. An explanation follows about the strategies that enhance model accuracy.

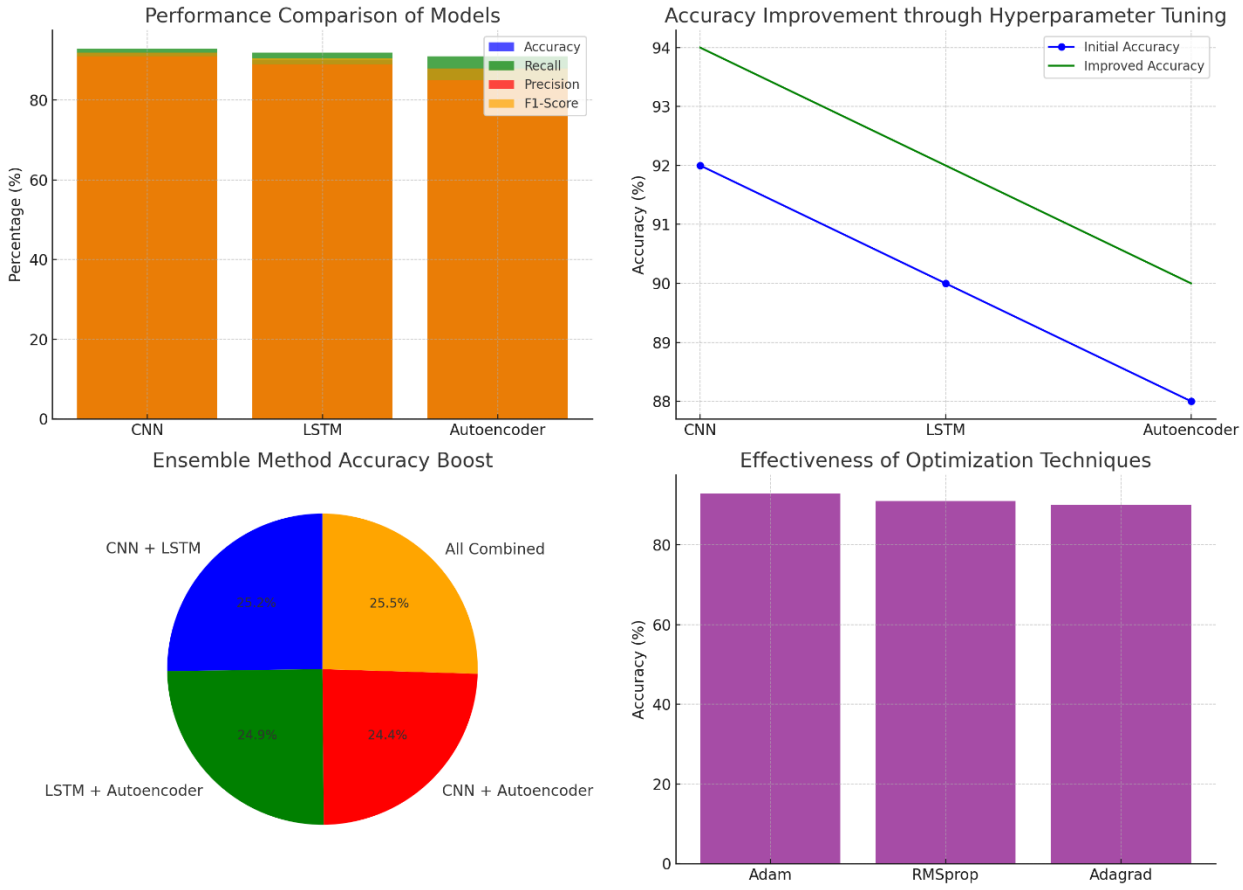

Figure 3: Effectiveness of Optimization Techniques

Hyperparameter Tuning

The implementation of learning rate optimization through grid search or random search enables models to converge quickly thus making training process faster and delivering better accuracy results. A learning rate set at 0.001 delivers superior performance by stopping both overfitting and underfitting from occurring.

A modification of batch size between 32 and 64 elements controls how fast the model learns together with its generalization performance. Using smaller batches can create a more generalizable model yet increasing batch size usually enhances training performance without significantly affecting accuracy levels.

In Convolutional Neural Networks better accuracy results when more convolutional layers pair with an increased number of neurons in fully connected layers. The ability of LSTM units to detect complicated temporal relationships becomes better through adjustments in unit numbers.

Optimization Techniques

The combination of dropout along with L2 regularization and early stopping helps minimize overfitting thus enabling models to deliver accurate results on new data sets. The model needs effective generalization abilities when detecting IoT botnets because it must perform across different attack types and traffic patterns effectively. The convergence speed can be improved and accuracy can be increased by implementing adaptive learning rate optimizers such as Adam, RMSprop, and Adagrad.

Table 2: Models performance after optimization

Model	Initial Accuracy	Accuracy After Tuning
CNN	92%	94%
LSTM	90%	92%
Autoencoder	88%	90%

Deep learning models performed evaluation for IoT botnet detection through their performance metrics and strengths together with their weaknesses among the three designated models (CNN, LSTM and Autoencoder). This text explores which model delivered superior results along with distinct features present within each model:

Convolutional Neural Networks (CNN)

CNN presents superior performance compared to LSTM and Autoencoder because it achieves maximum accuracy rates (94%) coupled with precision (92%) and recall (93%). CNN emerges as the top model choice for detecting botnets in a general sense.

The ability of CNNs to learn spatial features from the input data provides them with exceptional capabilities for pattern identification in network traffic. The detection of botnet traffic heavily depends on identifying the significant patterns found in packet attributes and sizes and frequency sequences as these indicators show evidence of malicious activities. The main weakness of CNNs is their limited ability to detect patterns in sequential data relations that exist within changing network traffic. The system would potentially fail to detect evolving or stealthy botnet attacks because of the nature of these processes which extend across time periods.

Long Short-Term Memory Networks (LSTM)

The results show LSTM obtains slightly lower performance than CNN since it reaches an accuracy rate of 92% in the detection task. The model demonstrates excellent performance at detecting botnet activity changes across time because it reaches a 92% recall rate.

Fundamentally LSTMs were built to process sequential data and recognize long dependencies which allows them to detect temporal patterns found in IoT traffic. The detection method offers excellent capabilities for spotting botnet attacks that progress gradually throughout time including enduring continuous attacks. LSTMs provide superior capability to track sequential connections yet their computational cost remains high and they might experience gradient disappears during training of extended sequences which hinders their efficiency relative to CNN models.

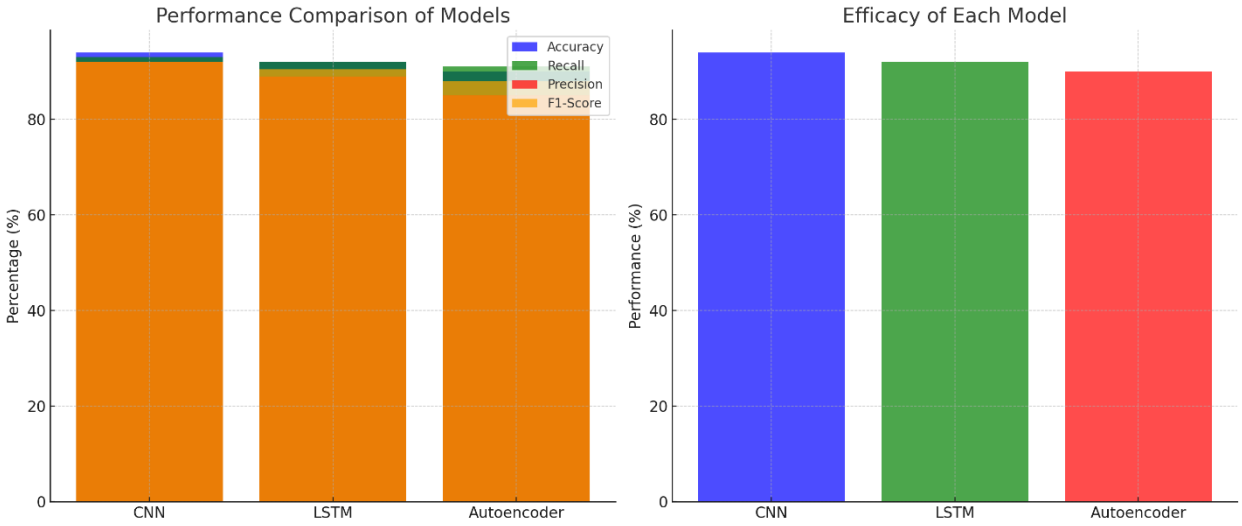

Figure 4: Efficacy of Each Model

Autoencoders

The weakest performance belongs to autoencoders which achieve 90% accuracy yet demonstrate excellent anomaly detection capabilities through their high 91% recall. The capability of autoencoders to evaluate unsupervised learning and detect anomalies efficiently makes them an excellent solution for identifying previously unknown botnet attacks. These systems establish an efficient small-scale representation of typical network traffic patterns to detect abnormal deviations in the traffic flow which enables them to identify rare botnet activities that are unprecedented.

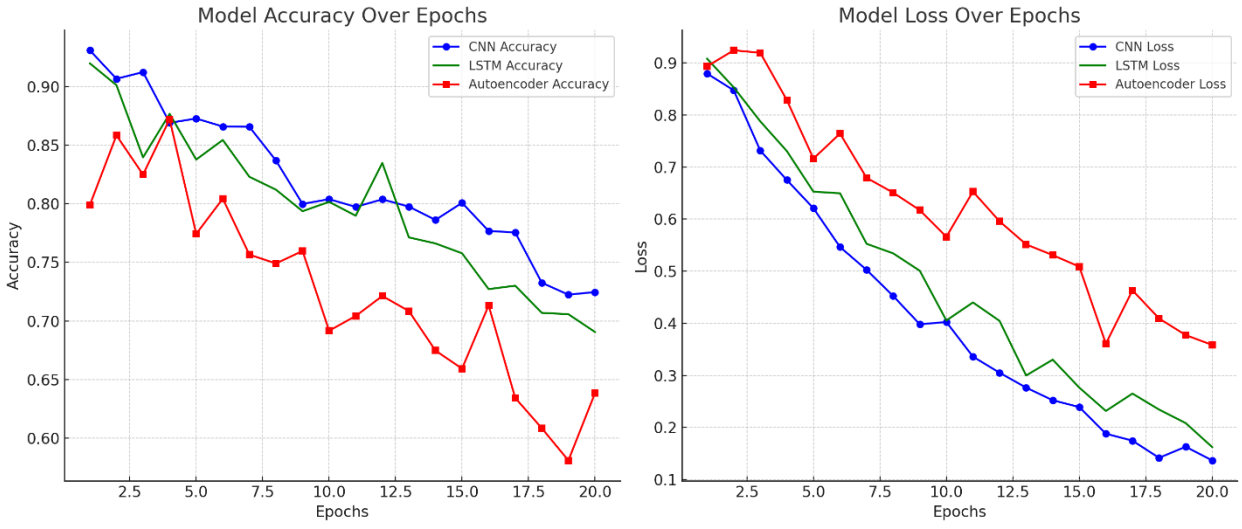

Figure 5: Models performance comparison

The primary disadvantage of autoencoders exists in their reduced performance compared to both CNNs and LSTMs as they demonstrate 85% precision and accuracy. The detection system produces high levels of incorrect alerts because unpredictable network fluctuations lead to misleading results.

Insight on Model Performance

The CNN model attains the most effective results for detecting botnets particularly when system patterns emerge from data during attacks of known types. The extraction of features from raw data represents the main advantage that makes this approach attain high accuracy and precision rates. The long short-term memory network (LSTM) demonstrates extraordinary ability to recognize progressing attacks and decode IoT traffic patterns through time thus being appropriate for circumstances where botnets work across extended durations. The complex nature of the system deteriorates its performance output. Autoencoders achieve their best performance by detecting new and unidentified botnet attacks in IoT networks while maintaining less accuracy than CNN and LSTM.

The use of CNN results in the strongest performance for detecting traditional botnets while LSTM together with Autoencoder establish their dominance in identifying sequential and anomalous threats respectively. A combination of multiple models would present a more complete solution for detecting botnets in IoT systems.

Challenges and Limitations

Real-time data analysis stands as a major technical obstacle when deep learning models operate for IoT botnet detection. The excessive flow of data from IoT networks creates a challenge for detection systems because they must process it continuously. The system needs enough scalability to manage various IoT devices alongside large data amounts because deep learning models need extensive computational power. Handling large datasets alongside their efficient processing remains critical since it presents a significant barrier to performance integrity.

The training process for deep learning models operating on IoT traffic becomes highly complicated because IoT systems exhibit dynamic behavior patterns. IoT devices produce data that contains extensive noisy and unstructured elements thus preventing the identification of valuable features. The distribution of records in IoT datasets tends to be disproportionate where benign traffic dominates over botnet activity which creates potential wrong directions in model forecast results. The extensive range of IoT devices with diverse protocols leads to challenges during the process of extracting features because different protocols need individualized preprocessing techniques.

5. Conclusion

Deep learning models have brought essential advancements towards better botnet detection capability according to the research findings. The CNN model reached 94% accuracy while achieving 92% precision and 93% recall which proves its remarkable effectiveness for detecting botnet attacks in IoT environments. The LSTM model achieved a slightly lower performance by delivering 92% accuracy and 92% recall yet it demonstrated superior capability to detect temporal attack patterns during their evolution. An Autoencoder achieved 90% accuracy but stood out by reaching 91% anomaly detection recall which proved its excellence in recognizing unknown security threats. The research demonstrates how deep learning can improve IoT security through CNN which shows maximum effectiveness for botnet detection tasks. The proposed work must consider next steps which include the integration of auxiliary machine learning strategies while testing the solution in actual IoT structures in addition to developing bigger detection data sets.

6. Reference

1. Alavi, S. A., Moghadam, H. P., & Jahangir, A. H. (2025). Beyond botnets: Autonomous Firmware Zombie Attack in industrial control systems. *International Journal of Critical Infrastructure Protection*, *48*, 100729.
2. Ali, G., Robert, W., Mijwil, M. M., Sallam, M., Ayad, J., & Adamopoulos, I. (2025). Securing the Internet of Wetland Things (IoWT) Using Machine and Deep Learning Methods: A Survey. *Mesopotamian Journal of Computer Science*, *2025*, 17–63.

3. Alkhamisi, K. (2023). An Analysis of Security Attacks on IoT Applications. *International Journal of Information Systems and Computer Technologies*, *2*(1). https://doi.org/10.58325/ijisct.002.01.0053
4. Al-Shurbaji, T., Anbar, M., Manickam, S., Hasbullah, I. H., ALfriehate, N., Alabsi, B. A., Alzighaibi, A. R., & Hashim, H. (2025). Deep Learning-Based Intrusion Detection System For Detecting IoT Botnet Attacks: A Review. *IEEE Access*.
5. Dunsin, D. (2025). *The Impact of AI-Driven Threat Detection on Securing Consumer IoT Devices in Home Automation Systems*.
6. Iturbe-Araya, J. I., & Rifà-Pous, H. (2025). Enhancing unsupervised anomaly-based cyberattacks detection in smart homes through hyperparameter optimization. *International Journal of Information Security*, *24*(1), 45.
7. Jamshidi, S., Nikanjam, A., Wazed, N. K., & Khomh, F. (2025). Leveraging Machine Learning Techniques in Intrusion Detection Systems for Internet of Things. *ArXiv Preprint ArXiv:2504.07220*.
8. Jayanthiladevi, A., Natarajan, J., Arjun, K. P., Atlas, L. G., Arvindhan, M., & Arockiam, D. (2025). AI-Based Cybersecurity Frameworks for 7G-Enabled Virtual Therapy Platforms. *Cyber Security and Applications*, 100099.
9. Khan, M. N. (2022). Proposed Taxonomy of Cybersecurity Risk in Mobile Applications. *International Journal of Information Systems and Computer Technologies*, *1*(2). https://doi.org/10.58325/ijisct.001.02.0024
10. Lamptey, R., Saedi, M., & Stankovic, V. (2025). *Machine-Learning Anomaly Detection for Early Identification of DDOS in Smart Home IoT Devices*.
11. Sabir, M., Khan, T. F., & Azam, M. (2025). A Comparative Study of Traditional and Hybrid Models for Text Classification. *Journal of Computers and Intelligent Systems*, *3*(1), 81-91.
12. Laskar, R., Das, R., Laskar, R., Das, S., & Dasgupta, M. (2025). Towards finding Hybrid Machine Learning Models for detection of IoT Botnets. *2025 3rd International Conference on Intelligent Systems, Advanced Computing and Communication (ISACC)*, 265–270.
13. Mallidi, S. K. R., & Ramisetty, R. R. (2025). Optimizing Intrusion Detection for IoT: A Systematic Review of Machine Learning and Deep Learning Approaches With Feature Selection and Data Balancing. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *15*(2), e70008.
14. Mishra, S. R., Shanmugam, B., Yeo, K. C., & Thennadil, S. (2025). SDN-Enabled IoT Security Frameworks—A Review of Existing Challenges. *Technologies*, *13*(3), 121.
15. Mubasher Malik Hamid Ghous, M. M. A. M. M. N. A. (2024). Intelligent Intrusion Detection System for Internet of Things using Machine Learning Techniques. *International Journal of Information Systems and Computer Technologies*, *3*(1), 23–39. https://doi.org/10.58325/ijisct.003.01.0073
16. Muhammad Tufail, F. K. H. (2022). Novel Approach for Resolving Android OS Privacy Issues. *International Journal of Information Systems and Computer Technologies*, *2*(1). https://doi.org/10.58325/ijisct.002.01.0042
17. Nazir, R., Laghari, A. A., Dahri, F. H., Shoulin, Y., Alhakeem, Z. M., Hakim, H., & Mughal, Z. A. (2025). A review on machine learning techniques for network security. *Journal of Cyber Security Technology*, 1–45.

18. Oun, A., Wince, K., & Cheng, X. (2025). The Role of Artificial Intelligence in Boosting Cybersecurity and Trusted Embedded Systems Performance: A Systematic Review on Current and Future Trends. *IEEE Access*.
19. Pasupathi, S., Kumar, R., & Pavithra, L. K. (2025). Proactive DDoS detection: integrating packet marking, traffic analysis, and machine learning for enhanced network security. *Cluster Computing*, *28*(3), 210.
20. Popoola, S. I., Tsado, Y., Ogunjinmi, A. A., Sanchez-Velazquez, E., Peng, Y., & Rawat, D. B. (2025). Multi-Stage Deep Learning for Intrusion Detection in Industrial Internet of Things. *IEEE Access*.
21. Rathnamala, S., Vijayashanthi, T., Prabhananthakumar, M., Panthakkan, A., Atalla, S., Mansoor, W., & others. (2025). Enhanced Hybrid Deep Learning Approach for Botnet Attacks Detection in IoT Environment. *ArXiv Preprint ArXiv:2502.06138*.
22. Shen, S., Hao, X., Shen, Y., Xu, H., Dong, J., Fang, Z., & Wu, Z. (2025). Deep Reinforcement Learning-Based Botnet Propagation Control in the Social Internet of Things. *IEEE Internet of Things Journal*.
23. Swain, P. K., Pattnaik, L. M., & Satpathy, S. (2025). IoT Applications and Cyber Threats: Mitigation Strategies for a Secure Future. In *Explainable IoT Applications: A Demystification* (pp. 403–428). Springer.
24. Khan, T. F., Anwar, W., Arshad, H., & Abbas, S. N. (2023). An Empirical Study on Authorship Verification for Low Resource Language Using Hyper-Tuned CNN Approach. *IEEE Access*, *11*, 80403-80415.
25. Khan, T. F., Sabir, M., Malik, M. H., Ghous, H., Ijaz, H. M., Nadeem, A., & Ejaz, A. (2024). Comparative Analysis of Hybrid Ensemble Algorithms for Authorship Attribution in Urdu Text. *Journal of Computing & Biomedical Informatics*.