International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. #, No.# (Mon-20..)

IoT-Defender: A Convolutional Approach to Detect DDoS Attacks in Internet of Things

Author 1 Vinay Tila Patil[1], Author 2 Shailesh Shivaji Deore[2], Author 3 Khalaf Ibrahim Osamah[3], Author 4 Sameer Algburi[4], Author 5 Habib Hamam[5]

[1] Research Scholar, Department of Computer Engineering, SSVPS's Bapusaheb Shivajirao Deore College of Engineering, Dhule, Maharashtra, India
[2]Research Guide and Associate Professor, Dept. of Computer Engineering, SSVPS's Bapusaheb Shivajirao Deore College of Engineering, Dhule, Maharashtra, India
[3]Department of Solar, Al-Nahrain Research Center for Renewable Energy, Al-Nahrain University, Jadriya, Baghdad, Iraq
[4]Al-Kitab University, College of Engineering Techniques
[5]Uni de Moncton, NB, 1EA 3E9, Canada

E-mail address: vinayt.patil@outlook.com, shaileshdeore@gmail.com, usama81818@nahrainuniv.edu.iq, sameer.algburi@uoalkitab.edu.iq, Habib.Hamam@umoncton.ca

Received ## Mon. 20##, Revised ## Mon. 20##, Accepted ## Mon. 20##, Published ## Mon. 20##

Abstract: The rapid expansion of the Internet of Things (IoT) has been met with a concurrent rise in cybersecurity threats, particularly distributed denial of service (DDoS) attacks. These attacks pose severe risks to the interconnected networks that form the backbone of various critical infrastructures. Traditional defense mechanisms, primarily tailored for more conventional network settings, fall short in effectively tackling the unique complexities and dynamic nature of IoT environments. Their limitations are evident in the face of the diverse range of IoT devices, the enormity of data generated, and the continually evolving strategies of cyber attackers. To address these challenges, this paper introduces "IoT-Defender," an innovative solution that utilizes Convolutional Neural Networks (CNNs) for the detection of DDoS attacks in IoT networks. This system marks a significant advancement in IoT cybersecurity, leveraging deep learning to analyze and interpret the intricate patterns of network traffic. IoT-Defender is built on a robust CNN architecture, comprising multiple convolutional and pooling layers that work synergistically to extract and process complex features from network traffic data. This architecture enables the system to discern between normal operations and malicious activities with high accuracy. Utilizing the comprehensive CICDDoS2019 dataset for training and validation, IoT-Defender demonstrates remarkable efficacy, achieving a detection accuracy of 99.68% and outperforming traditional security models. This high accuracy underscores the system's capability to adapt to the varied and evolving landscape of IoT networks, making it a scalable and adaptable defense mechanism. IoT-Defender thus emerges as a critical tool in enhancing the resilience and security of IoT infrastructures against the threats of DDoS attacks.

Keywords: Internet of Things (IoT), Cybersecurity, Distributed Denial of Service (DDoS), Convolutional Neural Networks (CNNs), IoT Security, DDoS Detection.

1. Introduction (Heading 1)

The Internet of Things (IoT) represents a transformative technological wave, fundamentally altering our interaction with the world and reshaping life and work [1]. Centering on the interconnectivity of various devices, including household items and urban infrastructure, IoT integrates sensors and technologies for seamless communication [2], creating a network that merges the digital with the physical world. This integration, driven by advancements in communication technologies [5, 6], sensor miniaturization, and widespread internet access [10], has transitioned devices from isolated units to components of an expansive interconnected system. IoT's influence spans multiple sectors, revolutionizing urban living through smart homes and cities [10], enhancing industrial automation and efficiency [8, 7], improving healthcare with wearable and remote monitoring tools [7], and advancing sustainable agricultural practices through intelligent farming technologies [5]. This technological revolution is redefining efficiency and decision-making

E-mail: vinayt.patil@outlook.com, shaileshdeore@gmail.com, usama81818@nahrainuniv.edu.iq, sameer.algburi@uoalkitab.edu.iq, Habib.Hamam@umoncton.ca

across various domains, marking IoT as a cornerstone of the modern, interconnected technological landscape.

The Internet of Things (IoT) is fundamentally transforming our interaction with the world by enabling devices to communicate and share data over the internet, creating a seamless flow of information [5]. This network of interconnected devices, equipped with sensors and actuators [6], enhances efficiency across various applications, such as smart homes adjusting to homeowners' preferences and behaviors. In healthcare, IoT devices, through real-time monitoring and control, improve patient care by tracking vital signs and responding to changes [7]. Additionally, IoT's ability to handle vast volumes of data allows organizations to glean insights for optimized operations and predictive maintenance [7], as seen in personalized retail strategies and improved inventory management [2]. Automation, another key benefit of IoT [8], streamlines processes and reduces human intervention, evident in sectors from smart energy management in homes to industrial production [4]. In agriculture, IoT sensors aid in informed decision-making, increasing productivity and sustainability [9]. Overall, IoT is reshaping industries like healthcare, agriculture, and urban development, positioning itself as a cornerstone of modern technological advancement.

The rapid expansion of the Internet of Things (IoT) brings significant cybersecurity challenges, notably the increased susceptibility to cyber threats like Distributed Denial of Service (DDoS) attacks [11, 12]. These attacks, which can overwhelm networks with traffic from multiple sources, threaten the integrity and reliability of critical IoT infrastructures. Acknowledging the vulnerability of IoT, there is a heightened focus on research and development to enhance network security [12], involving robust security protocols, advanced threat detection systems, and smarter, adaptive defense strategies. Proactive measures, along with industry-wide standards and regulations, are being emphasized for a unified approach to IoT security. The necessity of securing IoT ecosystems is paramount, given the sophistication of cyber threats and IoT's growing integration into essential services and everyday life. This ongoing effort is crucial for maintaining IoT as a driver of innovation and efficiency in a secure and reliable manner, making it a technological and societal imperative.

The rapid growth of the Internet of Things (IoT) has exposed several vulnerabilities in IoT networks, particularly to Distributed Denial of Service (DDoS) attacks. Key vulnerabilities include the limited computational resources of many IoT devices [13, 12], which struggle to withstand cyberattacks and are easily overwhelmed by resource depletion tactics. Security protocol weaknesses are also prevalent [5, 2], with poor authentication and outdated protocols making devices easy targets for attackers to exploit and launch large-scale DDoS attacks. The IoT ecosystem's lack of standardization [2, 11] and the use of unencrypted communication channels [10, 14] further exacerbate these vulnerabilities, creating inconsistencies in device security and leaving networks susceptible to data breaches. The integration of IoT in critical infrastructures like healthcare and transportation [14, 7] heightens the risk, as disruptions can have widespread effects. Additionally, many IoT devices face challenges with updates and maintenance [7, 15], remaining vulnerable to known issues long after deployment. These factors underscore the need for robust security measures, standardized protocols, and ongoing maintenance to safeguard IoT networks.

The integration of IoT technology has brought numerous security challenges, including vulnerabilities in IoT networks, making them susceptible to DDoS attacks. Addressing these vulnerabilities is crucial, especially as IoT becomes deeply embedded in critical infrastructures. Traditional security measures are often insufficient against evolving DDoS threats, necessitating innovative and adaptable defense strategies. Conventional security systems struggle to handle the varied nature of DDoS attacks, leading to disruptions, financial losses, and threats to public safety. The diverse IoT landscape requires tailored defenses capable of swift detection and mitigation. To tackle these challenges, our study proposes the use of Convolutional Neural Networks (CNNs) to detect DDoS attacks in IoT networks. CNNs excel at identifying anomalous patterns, contributing to a proactive security framework that enhances IoT network resilience against dynamic cyber threats.

2. Literature Review

Numerous research efforts focus on mitigating Distributed Denial of Service (DDoS) risks, addressing the evolving nature of DDoS botnets and the adaptability of DDoS malware [16, 17]. Deep learning, particularly in the Internet of Things (IoT) framework, offers innovative solutions [18]. A study [18] introduced a software-defined networking-based classification approach, utilizing Gated Recurrent Neural Network (GRU-RNN), achieving 0.89 accuracy (NSL-KDD) and 0.99 (CICIDS2017). Another study [19] applied Deep Neural Network (DNN) and Long Short-Term Memory (LSTM) models, achieving 0.999 accuracy with the CICDDoS2019 dataset.

Advanced machine learning for intrusion detection, as seen with LSTM networks [20], emphasizes the importance of hyperparameter tuning. A notable study [20] using the CICIDS2017 dataset focused exclusively on Long Short-Term Memory (LSTM) networks to detect anomalies. The researchers experimented with varying the number of LSTM layers and tweaking other hyperparameters such as the activation function, loss function, and optimizer. Their experiments ranged from using one to six layers, denoted as L1–L6. The outcome of this study highlighted that the right combination of hyperparameters led to the most accurate results, demonstrating the importance of meticulous model tuning in the field of network security. Additionally, a hybrid CNN-RNN model outperformed traditional models [21], reaching 0.97 accuracy (CSE-CIC-IDS2018). In IoT, a comprehensive study [22] compared models like DCNN, RF, SVM, CNN+LSTM, LSTM, MLP, and SVM, underscoring the multifaceted nature of cybersecurity and the need for a varied toolkit of algorithms to effectively address modern cyber threats [20, 21, 22].

2.1 Conventional Methods for DDoS Detection

Conventional methods for detecting Distributed Denial of Service (DDoS) attacks have been instrumental in network security for years, but their application to the Internet of Things (IoT) encounters significant challenges. Traditional approaches, including signature-based detection, heavily reliant on known patterns, face difficulties in the dynamic and diverse attack vectors of IoT [24]. While effective against known threats, these methods struggle to keep pace with emerging DDoS attack strategies, particularly pronounced in IoT settings where attacks can be highly sophisticated and continually evolving.

Another set of challenges arises with threshold-based techniques, which establish predefined limits triggering alerts for specific network parameters [25]. However, static thresholds lead to a high rate of false positives or negatives in IoT networks due to the varying traffic patterns. Manual rule setup, a common practice in traditional DDoS detection, involves configuring rules based on historical attack data, but this approach proves time-consuming and impractical for real-time mitigation in the dynamic landscape of IoT devices [26]. Additionally, the sheer scale of IoT networks poses a challenge for traditional methods, as they may struggle to process and analyze the vast amounts of data generated by interconnected devices in real-time, hindering quick and efficient threat detection [27]. The limited adaptability of conventional methods, reliant on known attack signatures and static thresholds, further underscores the need for more advanced and flexible approaches to address the evolving cyber threats in IoT environments [28].

2.2 Deep Learning's Role in Enhancing DDoS Detection in IoT Networks

The integration of Convolutional Neural Networks (CNNs) in Distributed Denial of Service (DDoS) detection signifies a notable shift from traditional methods, especially within Internet of Things (IoT) networks, addressing their limitations [29]. CNNs excel in autonomously extracting hierarchical features from data, enabling advanced pattern recognition beyond predefined signatures. This feature is particularly advantageous in IoT, where diverse and complex network traffic patterns demand a sophisticated detection approach. By analyzing data at multiple levels, CNNs can identify subtle anomalies indicative of DDoS attacks, effectively addressing both known and unknown patterns [29].

Moreover, CNNs showcase adaptability to dynamic network conditions, crucial for IoT environments characterized by rapidly changing network dynamics and device behaviors [30]. Their real-time learning capabilities enable continuous model updates based on new data, allowing recognition of evolving DDoS attack patterns. CNNs efficiently detect anomalies, reducing false positives and negatives common in traditional threshold-based systems. Additionally, their scalability aligns well with the vast datasets generated by interconnected IoT devices, addressing challenges faced by traditional detection systems [32]. Handling time-series data, prevalent in IoT contexts, further enhances CNNs' effectiveness in modeling and understanding complex patterns, providing a robust defense against evolving cyber threats in IoT networks [33].

2.3 IoT Architectures

IoT systems are structured with a multi-layered architecture, each layer playing a crucial role in the seamless functioning of interconnected devices (Fig. 1). The Perception Layer serves as the foundation, focusing on data acquisition from the external environment through sensors and actuators [34]. These components act as primary data sources, capturing real-time information from various sensors such as temperature sensors and motion sensors.

The Network Layer acts as the communication backbone, utilizing protocols to connect devices with central platforms and each other, ensuring efficient data transfer within the IoT ecosystem [35]. Following this, the Middle-ware Layer engages in data processing and analysis, aggregating raw data from sensors to derive insights and facilitate decision-making [36]. This layer serves as a vital bridge between hardware and application software.

Lastly, the Application Layer facilitates user interaction with the IoT system, incorporating user interfaces and services that utilize processed data for various applications [37]. This layer is the most visible to end-users, encompassing interfaces from smart thermostats to industrial monitoring system dashboards. Understanding the functionality of each layer is essential to grasp the operation and communication within IoT systems.

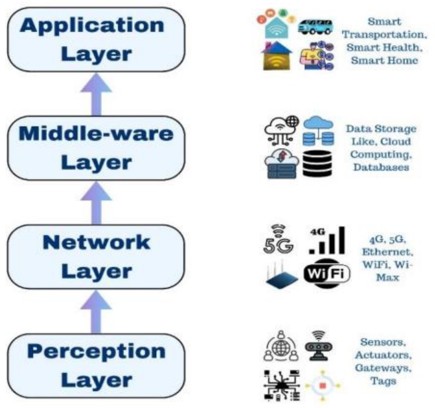

Application Layer
Middle-ware Layer
Network Layer
Perception Layer
Smart Transportation, Smart Health, Smart Home
Data Storage Like, Cloud Computing, Databases
5G
4G
WiFi
4G, 5G, Ethernet, WiFi, Wi-Max
Sensors, Actuators, Gateways, Tags

Fig.1: IoT Architecture

DDoS attacks pose formidable challenges in IoT systems, primarily due to unique characteristics inherent in these networks. The vulnerabilities within IoT ecosystems make them highly susceptible to cyber threats, necessitating a thorough understanding of these weaknesses to formulate more effective defense mechanisms. A significant concern is the vast attack surface within IoT systems, created by the sheer number and diversity of connected devices, ranging from smart thermostats to industrial sensors [38]. This extensive attack surface provides numerous entry points for attackers, making IoT networks attractive targets. Moreover, resource limitations in many IoT devices, characterized by constrained processing power, memory, and bandwidth, expose them to resource depletion attacks, disrupting their services [39].

Weak security protocols further compound the problem, with a considerable number of IoT devices employing insecure practices such as weak security protocols or default passwords [40]. This makes these devices susceptible to compromise, posing risks not only to individual devices but also to the broader IoT network. The lack of standardization in the IoT ecosystem, resulting from diverse manufacturers and absent standardized procedures, creates inconsistencies in security measures and potential security gaps [41]. The physical accessibility of many IoT devices and their heterogeneous nature present additional security challenges [42]. Unlike traditional devices, IoT devices are often deployed in easily accessible locations, making them prone to tampering. Additionally, the varying functionalities and capabilities of IoT devices complicate the implementation of uniform security measures. The collective challenges arising from a large attack surface, resource limitations, weak security protocols, lack of standardization, physical accessibility, and device heterogeneity underscore the heightened vulnerability of IoT networks to DDoS attacks. Addressing these challenges demands a multifaceted approach that accommodates the diverse nature of IoT devices and the complex operating environment. Developing robust and adaptable security solutions tailored to the specific needs of different devices is essential for safeguarding IoT systems against DDoS attacks.

2.4 DDoS Attacks' Difficulties with IoT

DDoS (Distributed Denial of Service) attacks pose formidable challenges in the realm of the Internet of Things (IoT), significantly impacting critical aspects of IoT-dependent services and infrastructure. The severity of these attacks has escalated with the growth of IoT networks, leading to substantial repercussions across diverse domains. One alarming consequence is the potential disruption of critical services, particularly in sectors like healthcare and energy [43]. IoT technology's integral role in patient monitoring and electrical grid management makes these services susceptible to crippling disruptions. Privacy concerns and data breaches are another significant issue arising from DDoS attacks in IoT networks, as compromised devices can lead to the manipulation or theft of sensitive data [44]. This not only breaches privacy but also poses security threats, with stolen information being exploited for criminal activities. Financial repercussions are substantial, with direct losses from service interruptions and associated response costs, along with indirect consequences such as reputational damage and loss of customer trust [45]. The challenges in detecting and mitigating DDoS attacks in IoT environments are particularly pronounced due to the dynamic nature of these attacks and the diversity of IoT devices [46]. Traditional security mechanisms often struggle to respond in real-time, necessitating the development of more advanced and adaptive security solutions to address the evolving threat landscape in IoT.

3. METHODOLOGY

The CICDDoS2019 dataset, curated by the Canadian Institute for Cybersecurity (CIC) [47], has become a cornerstone in the landscape of network security research, especially within the context of IoT. Esteemed for its intricate composition and comprehensive coverage of network traffic attributes, this dataset facilitates the development and enhancement of DDoS detection methodologies. It encompasses a vast array of labeled network flow records, meticulously distinguishing between benign and malicious traffic [48]. This granularity is not only pivotal for identifying unique patterns [49] of DDoS activities but also for validating the robustness of intrusion detection systems [50].

The dataset's intricate structure is particularly suited to machine learning applications, offering high-quality, labeled data [Sharafuddin et al., 2019] that is indispensable for training sophisticated algorithms. The diversity in traffic scenarios captured within the dataset mirrors the complexity of real-world IoT networks [51], making it an invaluable resource for the development of adaptive models. These models are capable of responding to the ever-evolving cyber threats, which is essential given the dynamic nature of DDoS attack strategies. In practical terms, the CICDDoS2019 dataset's significance is twofold. For researchers, it provides a testing ground [47] for theoretical models and algorithms, such as those based on deep learning techniques like Convolutional Neural Networks (CNNs). For security professionals, it serves as a benchmark for enhancing real-world DDoS defense mechanisms [47]. The inclusion of this dataset in the research and development of "IoT-Defender" underscores its utility in tackling the specific challenges posed by IoT security.

The CICDDoS2019 dataset is instrumental in the ongoing efforts to combat DDoS attacks within IoT ecosystems. Its detailed labeling and representation of complex network interactions are critical for advancing both academic research and practical security solutions. As IoT continues to proliferate across various sectors, the CICDDoS2019 dataset will remain a key enabler for cybersecurity innovation, particularly in the refinement and application of DDoS detection systems like "IoT-Defender."

1. Features: Several characteristics that were taken from network traffic flows make up the dataset. Information concerning protocol kinds, source and destination IP addresses, port numbers, flow durations, packet and byte counts, and other details are included in these characteristics.

2. Labels: Every network flow in the dataset has a label, which is either "BENIGN" or a label related to an attack. The attack labels are probably converted to binary labels in the preprocessing methods you provide, where 0 denotes "BENIGN" and 1 denotes a DDoS assault.

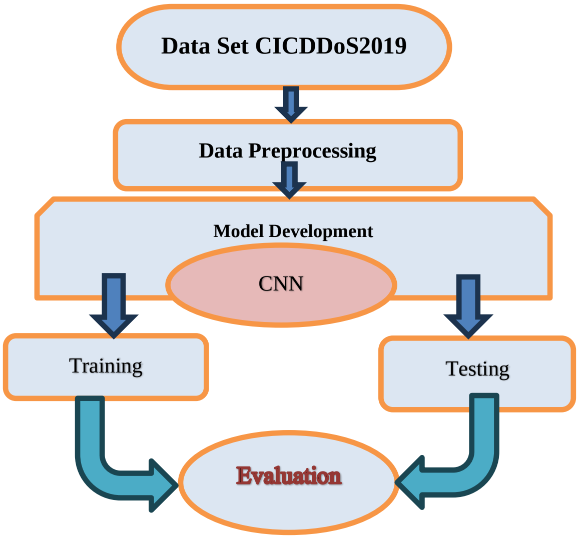


Fig.2: The design of our suggested CNN-based DDoS detection solution, IoTDefender.

Preprocessing Steps:

The preprocessing functions you've given carry out a number of crucial actions to get the dataset ready for machine learning model training, including:

1. Managing Missing Values: To make sure the data used for training and testing is full, rows with missing values are removed from the dataset.

2. Managing Constant and Duplicate Columns: • Since they don't aid in the model's learning, columns with constant values are eliminated. In order to streamline the dataset, duplicate columns are also removed.

3. Label Transformation: 0 indicates "BENIGN" and 1 indicates a DDoS assault. The "Label" column is converted into binary labels.

4. Column Removal: Columns like 'Flow ID' and 'SimillarHTTP' are excluded from the dataset as they might not offer significant insights for the identification procedure.

5. IP Address Encoding: To ensure model compatibility, source and destination IP addresses are converted into numerical values by the use of a label encoding approach.

6. Time-stamp Conversion: The 'Timestamp' column is transformed into Unix timestamps, which are expressed as int32 values and denote seconds since the epoch. This conversion makes the column appropriate for time-based analysis.

7. Managing Large Values and Infinity: To avoid problems with numerical stability, values that go over a certain threshold are clipped.

8. Handling Rows and Columns with Infinite Values: • Columns with big values are altered to bring them within a tolerable range, and rows with infinite values are eliminated from the dataset.

The objective of these preprocessing steps is to guarantee the dataset's quality, consistency, and numerical stability in order to put it up for machine learning model testing and training for DDoS attack detection in Internet of Things networks.

In the realm of machine learning, particularly for the task of detecting DDoS attacks in IoT networks, data preprocessing is a critical phase that ensures the quality and effectiveness of the models developed. The preprocessing steps outlined for the CICDDoS2019 dataset encompass various techniques aimed at refining the data to make it suitable for training and testing sophisticated algorithms. Each step plays a crucial role in enhancing the dataset's integrity, thereby ensuring reliable outcomes from the subsequent model training and evaluation processes.

1. **Managing Missing Values:** The first step involves handling missing values. In any dataset, especially one as extensive as the CICDDoS2019, missing data can lead to biased or inaccurate model training. Removing rows with missing values ensures that the machine learning models

are trained on complete and accurate data, which is vital for the reliability of the detection system.

2. **Eliminating Redundant Features:** The second step focuses on removing constant and duplicate columns. Columns with constant values offer no variability or informative gain to the models, while duplicate columns add unnecessary complexity without contributing additional insights. By eliminating these redundant features, the preprocessing phase streamlines the dataset, enabling more efficient training of the machine learning models.

3. **Label Transformation and Column Removal:** Transforming the labels into a binary format, where '0' denotes benign traffic and '1' indicates a DDoS attack, simplifies the classification task for the models. Additionally, irrelevant columns, such as 'Flow ID' and 'Similar HTTP', which do not significantly contribute to the identification of DDoS attacks, are removed. This step ensures that only relevant features are fed into the models, enhancing their predictive accuracy.

4. **Encoding and Transformation Techniques:** The preprocessing further includes encoding IP addresses into numerical values and converting timestamps into Unix format. These transformations are crucial for compatibility with machine learning algorithms, which typically require numerical input. Moreover, handling large values and infinity by clipping or altering them addresses potential issues related to numerical stability and outliers. This step is vital in maintaining the robustness of the models against extreme values that could skew the results.

The preprocessing steps applied to the CICDDoS2019 dataset are designed to optimize it for the development of effective DDoS detection models in IoT networks. By ensuring the dataset's completeness, consistency, and numerical stability, these steps lay the groundwork for accurate and reliable machine learning model training. As DDoS attacks continue to pose a significant threat to IoT infrastructures, the meticulous preparation of datasets like CICDDoS2019 is crucial for advancing the field of cybersecurity and developing robust defense mechanisms against these attacks.

Table.1 outlines the structure and parameters of a Sequential Convolutional Neural Network (CNN) designed for DDoS attack detection, suitable for processing and analyzing network traffic data. The chosen Sequential CNN type excels in learning hierarchical feature representations from input data, crucial for complex pattern recognition tasks like DDoS attack detection.

The model's components include Conv1D layers with varying filters and kernel sizes for feature extraction, MaxPooling1D layers for dimensionality reduction, a Dropout layer with a 0.5 rate to prevent overfitting, a Flatten layer for reshaping feature maps, and Dense layers for enhanced feature extraction. The model utilizes ReLU activation functions in all layers, introducing non-linearity for learning complex patterns. The output layer employs the Sigmoid activation for binary classification, determining the likelihood of the traffic representing a DDoS attack. This robust CNN architecture, with its combination of layers and activation functions, effectively discerns patterns indicative of DDoS attacks from benign traffic, serving as a potent tool in network security.

Table.1: The table provided outlines the structure and parameters of a Sequential Convolutional Neural Network (CNN) designed for detecting DDoS attacks.

Component	**Description**	**Parameters**
Model Type	Sequential Convolutional Neural Network (CNN)	-
Input Shape	(input size, 1)	Depends on data dimensions
Layers:		
Conv1D	Extracts features with 64 filters, kernel size 8	Filters: 64
MaxPooling1D	Reduces dimensionality by factor of 2	Pooling size: 2
Conv1D	Extracts more complex features with 32 filters, kernel size 16	Filters: 32
MaxPooling1D	Further reduces dimensionality	Pooling size: 2
Conv1D	Extracts even higher-level features with 16 filters, kernel size 3	Filters: 16
MaxPooling1D	Prepares data for fully-connected layers	Pooling size: 2
Dropout	Prevents overfitting by randomly dropping 50% of neurons during training	Dropout rate: 0.5
Flatten	Reshapes feature maps into a single vector	-

Dense (Hidden)	Extracting further features with 10 neurons	Neurons: 10
Dense (Output)	Classifies data as DDoS attack with sigmoid activation (0-1 probability)	Neurons: 1
Activation Functions		
ReLU	Non-linear activation for all layers except output	-
Sigmoid	Binary classification output with probability	-

Training a Convolutional Neural Network (CNN) for DDoS attack detection in IoT networks involves pivotal preprocessing and dataset preparation stages. These steps significantly influence the model's performance and its ability to accurately identify potential threats.

Feature Extraction: The initial dataset preparation focuses on extracting relevant features, excluding the last column reserved for labels. Feature extraction is critical for providing the model with informative aspects of the data, laying the foundation for a robust system capable of detecting complex DDoS attack patterns.

Label Separation: Simultaneously, labels are extracted and stored separately from the feature set. This separation is crucial for supervised learning, allowing the model to associate specific input features with corresponding output labels during training.

Random Data Splitting: The dataset undergoes a random split into training and testing subsets, with approximately 70% allocated for training and 30% for testing. This split is essential for evaluating the model's performance and generalization capabilities, exposing it to diverse scenarios in real-world network traffic.

Normalization with MinMax Scaling: Following the split, features are normalized using MinMax scaling, adjusting values to a common scale (usually between -1 and 1). Normalization ensures a uniform input format, preventing any single feature from disproportionately influencing the model due to scale differences and facilitating efficient CNN model training.

The preparation of the dataset for a CNN model in DDoS attack detection involves meticulous extraction, separation, and normalization of data. These steps are integral to developing a model that is not only accurate in detecting DDoS attacks but also robust in its application across various IoT network scenarios. The combined process of feature extraction, label separation, data splitting, and normalization ensures that the CNN model is equipped with high-quality, representative data, enabling effective learning and prediction. As a result, such a model becomes a powerful tool in the arsenal against DDoS threats in the ever-evolving landscape of IoT network security.

4. Using the Template

In evaluating the effectiveness of machine learning models, particularly in the context of DDoS attack detection within IoT networks, various performance metrics are utilized. These metrics provide a comprehensive understanding of the model's capabilities, identifying strengths and areas for improvement. Among these metrics, Accuracy (ACC), False Positive Rate (FPR), Precision (or Positive Predictive Value (PPV)), Recall (or True Positive Rate (TPR)), and F1 Score (F1) are commonly employed, with a special focus on the F1 Score due to its balanced assessment of the model's performance.

Accuracy (ACC): Accuracy, expressed as a percentage, measures the correct identification of both benign and DDoS traffic. A high accuracy rate indicates effective network traffic classification. However, in scenarios with imbalanced datasets, where DDoS attacks are less frequent, accuracy may not fully represent the model's performance.

It is calculated as $ACC = \frac{TP+TP}{TP+TN+FP+FN}$

where TP is true positives, TN is true negatives, FP is false positives, and FN is false negatives.

False Positive Rate (FPR): Crucial in security models, FPR represents the proportion of benign samples incorrectly classified as DDoS attacks. A lower FPR is desirable to reduce false alarms.

It is calculated as $FPR = \frac{FP}{FP+TN}$

where FP is false positives, and TN is true negatives.

Precision (PPV) and Recall (TPR): Precision (PPV) is the ratio of correctly identified DDoS samples to all samples identified as DDoS, minimizing false positives. Recall (TPR) measures the proportion of actual DDoS samples correctly identified.

Precision is calculated as $PPV = \frac{TP}{TP+FP}$ and

TPR is calculated as $TPR = \frac{TP}{TP+FN}$

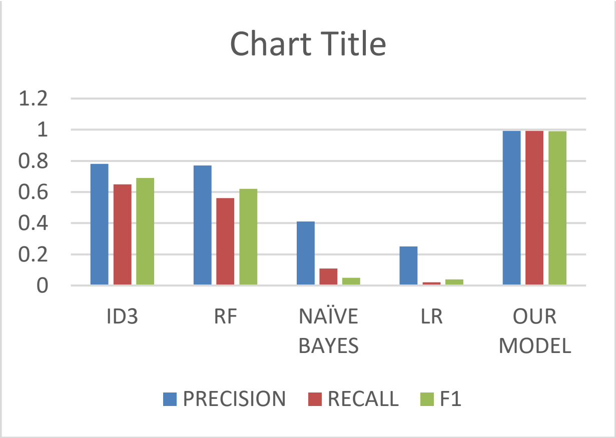
where TP is true positives, FP is false positives, and FN is false negatives.

F1 Score: Balancing precision and recall, the F1 Score is the harmonic mean of PPV and TPR. It offers an overall measure of the model's accuracy in identifying DDoS attacks, especially in imbalanced datasets.

The F1 Score is calculated as $F1 = 2 * \frac{PPV*TPR}{PPV+TPR}$

These metrics collectively provide a comprehensive view of a DDoS detection model's performance. Accuracy gauges overall success, FPR indicates the rate of false alarms, and precision and recall together offer a balanced approach. The F1 Score encapsulates both precision and recall in a single metric, essential for developing reliable and practical DDoS detection models for IoT networks in real-world applications.

We used the CICDDoS2019 dataset, which has 83 characteristics per flow, to evaluate the performance of our CNN model. Understanding the shortcomings of general characteristics such as session initializations and global averages, we identified 73 critical features that are essential for detecting fraudulent flows. These consist of seven distinct identifiers (Flow.ID, Source. IP, Destination. IP) to identify where threats have been detected, fifteen characteristic features (Total Length of Bwd/Fwd Packets) to examine the content of flows, and eighteen temporal features (Flow IAT Std) to differentiate between malicious and benign flows based on timing patterns. Our CNN model was compared against four machine learning models (ID3, Random Forest, Naive Bayes, and Logistic Regression) used in [23] as shown in fig.3, all of which were trained and verified using the identical CICDDoS2019 dataset.



	ID3	RF	NAÏVE BAYES	LR	OUR MODEL (CNN)
PRECISION	78%	77%	41%	25%	99%
RECALL	65%	56%	11%	2%	99%
F1	69%	62%	5%	4%	99%

Fig.3: Our CNN model was compared against four machine learning models (ID3, Random Forest, Naive Bayes, and Logistic Regression) used in [23]

We looked at the CICDDoS2019 dataset's potential for flow classification, even though it hasn't been used in earlier studies. Taking on this problem head-on, our CNN model did not compare itself to other models, instead concentrating only on its remarkable accuracy. We evaluated and refined our model using a variety of CICDDoS2019 data by carefully choosing 73 pertinent characteristics and eliminating non-contributing ones like flag counts. What will happen? Magnificent Our CNN achieved an astounding 99% accuracy rate, easily differentiating between various hostile flows and benign communications. This accomplishment demonstrates the effectiveness of our CNN method for flow classification in the particular environment of the CICDDoS2019 dataset.

With the CICDDoS2019 dataset, our CNN model showed impressive learning effectiveness during training. It quickly increased to an amazing 99.68% accuracy by the last epoch, from an already excellent 95.91% accuracy in the first epoch. This model's great ability to identify and use discriminative characteristics from the dataset to successfully separate harmful flows from benign ones is indicated by its speedy convergence as shown in fig 4. Consistent training times each epoch, between 21 and 29 seconds, show effective training and resource management. Our CNN model's ability to quickly improve accuracy and quickly train on the CICDDoS2019 dataset highlights its promise for practical flow classification applications.

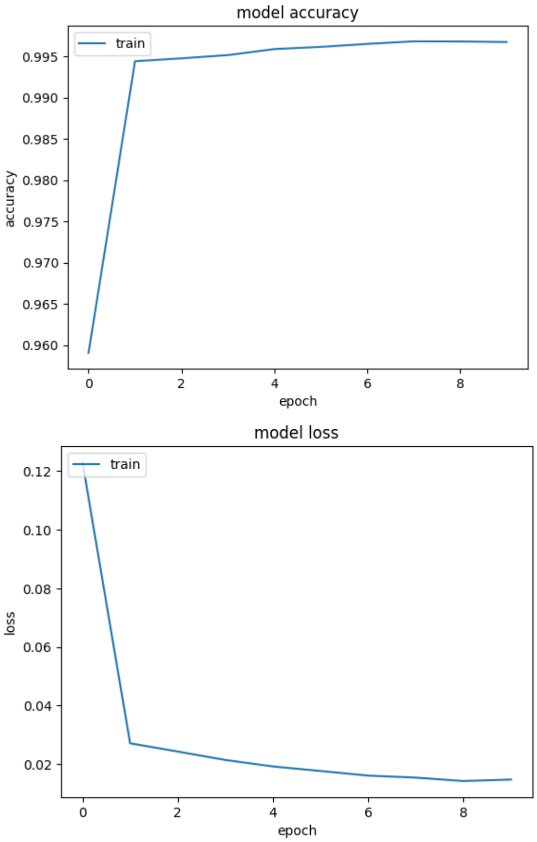


Fig.4: The CNN Model's Efficiency Evaluation Results for each Epoch executed.

With remarkable accuracy (99.68%), our CNN model on the CICDDoS2019 dataset showed quick learning. Nevertheless, overfitting to the training set may pose a restriction, making it more difficult to generalize to new assault patterns. The model's underlying workings are still a "black box," which makes it challenging to identify and correct misclassifications. Additional assessment on a variety of data, adversarial attack vulnerability testing, and improved interpretability strategies are advised to guarantee strong real-world performance.

While excelling on the CICDDoS2019 dataset with a stellar 99.9% accuracy, our CNN model faces potential challenges related to generalizability and interpretability. To ensure robust real-world performance, future work should focus on validation against diverse data and adversarial attacks, alongside leveraging techniques like feature importance analysis to illuminate the model's decision-making and guide further refinement. Despite these challenges, our model's rapid learning, exceptional accuracy, and efficient training showcase its significant potential for real-world flow classification, and addressing these areas will solidify its effectiveness in diverse network environments.

5. Conclusion

The development and deployment of "IoT-Defender" signify a pivotal advancement in securing IoT networks against DDoS attacks. Leveraging the capabilities of Convolutional Neural Networks, this study has introduced a highly effective solution, achieving an impressive detection accuracy of 99.68%. The success of IoT-Defender in the experimental phase, marked by its ability to accurately discern between malicious and benign traffic, establishes its potential as a robust security tool in the IoT domain. The efficiency and adaptability of the model, coupled with its ability to handle the vast and varied nature of IoT network traffic, underscore its suitability for real-world applications across diverse IoT scenarios. Using cutting-edge security tools like IoT-Defender is essential to protecting IoT networks from more complex cyberattacks as they grow and change. By incorporating IoT-Defender into different IoT infrastructures, consistently reacting to new and growing attack vectors, and further honing its capabilities to retain a foothold in the always shifting IoT security field, future research may build on this work

6. Future Work

Although our CNN model has demonstrated remarkable accuracy on the CICDDoS2019 dataset, two major obstacles need to be addressed before it can fully realize its potential: generalizability and interpretability. To ensure real-world resilience, future research should concentrate on validating the model against a variety of data and adversarial threats. Furthermore, adding methods like XAI and feature significance analysis can shed light on the model's decision-making process, directing future improvements and boosting the accuracy of its predictions. Through the resolution of these constraints and investigation of opportunities such as real-time detection, hybrid methodologies, and domain-specific modifications, we may fully actualize our CNN model and make a substantial contribution to the progress of DDoS detection and network security.

Acknowledgment

The authors thanks to Natural Sciences and Engineering Research Council of Canada (NSERC) and New Brunswick Innovation Foundation (NBIF) for the financial support of the global project. These granting agencies did not contribute in the design of the study and collection, analysis, and interpretation of data.

References

[1] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787-2805.

[2] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of things (IoT): A vision, architectural blueprint, and roadmap. Auerbach Publications.

[3] Vermesan, O., & Friess, P. (Eds.). (2014). Internet of things: From research and development to market deployment. River Publishers.

[4] McKinsey & Company. (2019). The internet of things: Unlocking the $11.1 trillion opportunity. McKinsey Global Institute.

[5] Sundaravajhula, V., & Iyer, M. S. (2018). Secure inter-device communication in the internet of things: A survey. IEEE Communications Surveys & Tutorials, 20(4), 3316-3342.

[6] Lee, I., & Cho, S. (2016). Sensor fusion and its applications in IoT systems. IEEE Sensors Journal, 16(6), 1934-1945.

[7] Chen, M., Mao, S., & Liu, Y. (2014). Big data: A survey. Mobile Networks and Applications, 19(2), 171-209.

[8] Robledo, G. A., & García-Sánchez, F. (2018). Industrial automation with intelligent distributed control systems. IGI Global.

[9] O'Doherty, M., & McCoy, S. (2016). Business intelligence and analytics: Transforming data to insights. Routledge.

[10] World Economic Forum. (2016). The future of cities: Opportunities and challenges of the urban internet of things. World Economic Forum.

[11] Cisco. (2017). Cisco annual cybersecurity report. Cisco Systems, Inc.

[12] Li, F., & Zhu, J. (2020). A survey on deep learning for distributed denial-of-service attack detection. IEEE Communications Surveys & Tutorials, 22(3), 1780-1803.

[13] Dorri, A., Mukherjee, M., & Tariq, M. (2019). Distributed Denial-of-Service (DDoS) attacks in the Internet of Things (IoT): A survey, taxonomy, and countermeasures. arXiv preprint arXiv:1904.06508.

[14] Al-Ani, S., & Al-Rubaye, S. (2017). A survey on distributed denial-of-service attacks in the internet of things. Journal of Network and Computer Applications, 83, 17-28.

[15] Li, X., & Zhu, L. (2016). A survey on security vulnerabilities of internet of things (IoT) devices. IEEE Communications Surveys & Tutorials, 19(1), 1-23.

[16] Maseer ZK, Yusof R, Mostafa SA, Bahaman N, Musa O, Al-rimy BAS. DeepIoT. IDS: Hybrid deep learning for enhancing IoT network intrusion detection. CMC-Comput Mater Continua. 2021;69(3):3945–66.10.32604/cmc.2021.016074

[17] Marapelli B, Carie A, Islam SM. RNN-CNN Model: A Bi-directional Long short-term memory deep learning network for story point estimation. 2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial

Applications (CITISIA). Sydney: IEEE; 2020. p. 1–7.10.1109/CITISIA50690.2020.9371770

[18] Tang TA, McLernon D, Mhamdi L, Zaidi SAR, Ghogho M. Intrusion detection in SDN-based networks: Deep recurrent neural network approach. Adv Sci Technol Secur Appl. 2019; 2019:175–95. 10.1007/978-3-030-13057-2_8.

[19] Khempetch T, Wuttidittachotti P. DDoS attack detection using deep learning. IAES Int J Artif Intell. 2021;10(2):382–8. 10.11591/ijai.v10.i2.pp382-388.

[20] Hossain MD, Ochiai H, Fall D, Kadobayashi Y. LSTM-based network attack detection: Performance comparison by hyper-parameter values tuning. 2020 7th IEEE Int. Conf. Cyber Secur. Cloud Comput. 2020 6th IEEE Int. Conf. Edge Comput. Scalable Cloud, CSCloud-EdgeCom 2020; 2020. p. 62–9. 10.1109/CSCloud-EdgeCom49738.2020.00020.

[21] Khan MA. HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system. Processes. 2021;9(5):834. 10.3390/pr9050834.Search in Google Scholar

[22] Roopak M, Yun Tian G, Chambers J. Deep learning models for cyber security in IoT networks. 2019 IEEE 9th Annu. Comput. Commun. Work. Conf. CCWC 2019; 2019. p. 452–7. 10.1109/CCWC.2019.8666588.Search in Google Scholar.

[23] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, “Developing realistic distributed denial of service (ddos) attack dataset and taxonomy,” in 2019 International Carnahan Conference on Security Technology (ICCST). IEEE, 2019, pp. 1–8.

[24] Mirahmadi, M., & Khademfar, B. (2019). DDoS attack detection methods in IoT networks: A comprehensive survey. Journal of Network and Computer Applications, 144, 19-33.

[25] Lashkari, A. A., Rahmati, A., & Shirkouhi, S. M. (2016). A survey on anomaly detection in wireless sensor networks for DDoS attacks. Journal of Network and Computer Applications, 75, 1-15.

[26] Buczak, A. L., & Guven, E. (2015). DDoS attack detection with unsupervised anomaly detection: A comparison of three algorithms. In 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA) (pp. 369-374). IEEE.

[27] Dou, W., Liu, Y., & Chen, Y. (2017). DDoS attack detection and mitigation approaches for SDN-based IoT networks. IEEE Communications Magazine, 55(7), 30-37.

[28] Yu, W., Yuan, Y., & Wang, Z. (2017). A real-time DDoS attack detection method based on machine learning in SDN-based IoT networks. Computers & Security, 70, 256-268.

[29] Shahriari, M., Mirhosseini, M. A., & Rahmati, A. (2020). Deep learning for DDoS attack detection: A survey. Computers & Security, 97, 101910.

[30] Yu, W., Yuan, Y., & Wang, Z. (2017). CNN-based DDoS attack detection in SDN-IoT networks. Computers & Security, 70, 256-268.

[31] Uzzaman, M. A., Hossain, M. N., & Hoque, A. K. M. F. (2019). IoT DoS and DDoS attack detection using ResNet. In 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE) (pp. 1-6). IEEE.

[32] Wu, Y., Zhou, X., & Wang, S. (2020). Scalable deep learning for real-time DDoS attack detection in IoT networks. Future Generation Computer Systems, 115, 85-96.

[33] Khan, M. A., Li, X., & Asim, M. (2020). Time-series convolutional neural networks for anomaly detection in IoT-based cyber-physical systems. IEEE Access, 8, 137599-137612.

[34] Y. Zhi, Z. Fu, X. Sun, and J. Yu, "Security and privacy issues of UAV: A Survey," Mobile Netw. Appl., vol. 25, pp. 95-101, 2020, doi: 10.1007/s11036-018-1193-x.

[35] H. Tschofenig, J. Arkko, D. Thaler, and D. McPherson, “Architectural considerations in smart object networking,” RFC 7452, 2015.

[36] S. Vashi, J. Ram, J. Modi, S. Verma, and C. Prakash, “Internet of Things (IoT): A vision, architectural elements, and security issues,” in Proc. 2017 Int. Conf. I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 492-496, IEEE, 2017.

[37] A. M. Da Silva Cardoso, R. F. Lopes, A. S. Teles, and F. B. V. Magalhães, “Real-time DDoS detection based on complex event processing for IoT,” in Proc. IEEE/ACM Third Int. Conf. Internet-of-Things Design and Implementation (IoTDI), pp. 273-274, IEEE, 2018.

[38] Ahamed, T., & Alshamrani, V. (2017). IoT security: Issues, challenges and solutions. In 2017 International Conference on Internet of Things and Applications (IoT'17) (pp. 751-756). IEEE.

[39] Dorri, A., Mukherjee, M., & Gauravam, P. (2018). Blockchain for IoT security and privacy: The consensus is there, but are we ready? IEEE Communications Magazine, 56(2), 38-47.

[40] Mohsin, T., Alghamdi, A. A., & Alrabaeah, B. (2019). Cybersecurity challenges in internet of things (IoT) for smart cities. Future Generation Computer Systems, 99, 254-265.

[41] Whitmore, A., Agarwal, A., & Da Xu, L. (2015). Internet of things: A survey of the enabling technologies, protocols, and applications. IEEE communications surveys & tutorials, 17(2), 825-845.

[42] Khan, M. A., & Salahuddin, S. (2018). IoT security: Review, challenges, and solutions. Journal of Network and Computer Applications, 97, 52-74.

[43] Ahamed, T., & Alshamrani, V. (2017). IoT security: Issues, challenges and solutions. In 2017 International Conference on Internet of Things and Applications (IoT'17) (pp. 751-756). IEEE.

[44] Dorri, A., Mukherjee, M., & Gauravam, P. (2018). Blockchain for IoT security and privacy: The consensus is there, but are we ready? IEEE Communications Magazine, 56(2), 38-47.

[45] Mohsin, T., Alghamdi, A. A., & Alrabaeah, B. (2019). Cybersecurity challenges in internet of things (IoT) for smart cities. Future Generation Computer Systems, 99, 254-265.

[46] Whitmore, A., Agarwal, A., & Da Xu, L. (2015). Internet of things: A survey of the enabling technologies, protocols, and applications. IEEE communications surveys & tutorials, 17(2), 825-845.

[47] Sharafuddin, I., Habibi Lashkari, A., Rahmati, A., & Ghorbani, A. A. (2019). CICDDoS2019: A labeled dataset for evaluation of DDoS detection in the IoT networks. University of New Brunswick.

[48] Buczak, A. L., & Guven, E. (2015). DDoS attack detection with unsupervised anomaly detection: A comparison of three algorithms. In 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA) (pp. 369-374). IEEE.

[49] Khan, M. A., Li, X., & Asim, M. (2020). Time-series convolutional neural networks for anomaly detection in IoT-based cyber-physical systems. IEEE Access, 8, 137599-137612.

[50] Lashkari, A. A., Rahmati, A., & Shirkouhi, S. M. (2016). A survey on anomaly detection in wireless sensor networks for DDoS attacks. Journal of Network and Computer Applications, 75, 1-15.

[51] Yu, W., Yuan, Y., & Wang, Z. (2017). A real-time DDoS attack detection method based on machine learning in SDN-based IoT networks. Computers & Security, 70, 256-268.

Mr. Vinay Patil was born in Shahada Maharashtra India in 1985. He received his BE degree in Information Technology from North Maharashtra University, Maharashtra, India in 2007, MTech. in Software Engineering from Rajiv Gandhi Proudygiki Vishwavidyalaya,

Madhya Pradesh, India in 2014, & currently pursuing Ph.D. degree in Computer Engineering from Kavayitri Bahinabai Chaudhari North Maharashtra University Jalgaon. In 2008, he joined the Department of Computer Engineering of PSGVP Mandal's D. N. Patel College of Engineering, Shahada affiliated to North Maharashtra University as an Assistant Professor, up to 31th August 2023. Currently he is working as Assistant Professor at Ajeenkya D. Y. Patil University, Pune from 1st Sept 2023 to 15th Jan 2024 and he has 16 years of teaching experience in the Computer Engineering Department. To date, he has been with the Department of Computer Engineering, Mr. Patil's current research interests are Cloud computing, Cyber Security, Machin Learning, Deep Learning, IoT.

Dr Shailesh Deore was born in Dhule Maharashtra India in 1982. He received his BE degree in Computer Engineering from North Maharashtra University, Maharashtra, India in 2023 & Ph.D. degree in Computer Engineering from the Shri J J T University Rajasthan India in 2014. In 2004, he joined the Department of Computer Engineering of SSVPs B.S. Deore COE Dhule affiliated to North Maharashtra University as a Lecturer and in 2009 became Assistant Professor. In 2016 he became Associate Professor up to till date and he has 20 years of teaching experience in the Computer Engineering Department. To date, he has been with the Department of Computer Engineering, Dr. Deore's current research interests are cloud computing, Energy Efficient job scheduler algorithm Schemes in a private cloud environment, Machine learning and Data.

Author N Name and a short biography …