Detection of Botnet attack in IOT system using Deep Learning

Er. R.A.D Martin Dhinakaran M.E,(Ph.D.)

Senior Assistant Professor, IFET College of Engineering (Autonomous)

prof.radmd@gmail.com

ABSTRACT :

The rise of Internet of Things (IoT) devices increases the risk of botnet attacks in IOT system. Botnets are a type of malware that spread among IoT devices and uses them for cyber-attacks. Traditional methods for detecting botnet attacks in IoT systems rely on signature-based or behaviour-based approach, which have limitations in detecting new or unknown botnets. Therefore, this study explores the use of deep learning as a promising approach for identifying botnet attacks in IoT systems. The methodology involves using a dataset of network traffic in an IoT system to train a deep learning model. This model outperforms conventional approach in terms of detection accuracy and false positive rates, and has a high precision and recall. This study demonstrates the effectiveness of deep learning in detecting botnet attacks in IoT systems, particularly in detecting new or unknown botnets.

INTRODUCTION:

Botnet attack is an emerging threat to Internet of Things (IoT) systems, where a connected nodes of infected devices is used to launch coordinated attacks against targets such as online platforms, network servers, or connected devices. Detecting botnet attacks in real-time is demanding due to the complication and variability of network traffic patterns in IoT systems. A botnet that externally controlled by an attacker. These devices can be used to carry out various cyber attacks such as Network congestion attack, data breach, and malware infection. The rapid growth of connected devices and the connected device has led to a surge in botnet attacks, making them one of the most serious security threats facing organizations and individuals today. Standard security methods, such as signature-based detection and network intrusion detection systems, are no longer sufficient to defend against the sophisticated and evolving botnets. Therefore, there is a growing need for new and advanced methods for detecting botnets.

The connected device has modernized the method we engage with the world. It has allowed us to automate and remotely control a vast array of devices, from smart thermostats and light bulbs to industrial machinery and medical devices. However, the increased connectivity and complexity of IoT systems have also made them a prime target for cyber attacks. One of the most significant threats to IoT systems is botnet attacks. detection using deep learning can also help businesses comply with regulatory requirements related to IoT security and privacy, which can help them avoid legal and financial penalties. Botnets can be formed by infecting a huge number of devices with malware, and then using

these devices to carry out coordinated attacks. Traditional methods for detecting botnet attacks in IoT systems have relied on rule-based or behaviour-based approaches. Signature-based approaches involve identifying malware by matching it with a known signature, while behaviour-based approaches rely on detecting abnormal behaviour in network traffic. However, these approaches have limitations in detecting new or unknown botnets, as they rely on pre-defined signatures or behavioral patterns.

In recent times, deep learning has emerged as a efficient approach for detecting botnet attacks in IoT systems. These networks can learn to recognize complex patterns in data and make predictions based on those patterns. The ability of deep learning to learn from large amounts of data without prior knowledge of the patterns or signatures makes it an ideal candidate for detecting new or unknown botnets.

One of the key benefits of using deep learning for botnet detection in IoT systems is that it can enable businesses to quickly identify and respond to security threats, thereby reducing the impact of cyber attacks. By continuously monitoring network traffic and analyzing patterns of behavior, deep learning algorithms can identify anomalous activity that may indicate the presence of a botnet attack. This can enable businesses to take proactive measures to prevent or mitigate the attack, which can reduce the damage caused and improve the sustainability of their operations. It can help businesses comply with regulatory requirements related to IoT security and privacy. By detecting and preventing botnet attacks, businesses can avoid legal and financial penalties, which can promote sustainable business practices and improve their overall financial health. the use of deep learning for botnet detection in IoT systems can also promote innovation in the field of cybersecurity. By developing and deploying advanced algorithms for detecting botnet attacks, businesses can stay ahead of emerging threats and promote sustainable business practices

LITERATURE REVIEW :

This systems is a critical area of research due to the increasing prevalence of these attacks. In recent times, researchers have explored various techniques for detecting botnet attacks, including traditional signature-based and behaviour-based approaches, as well as newer approaches based on machine learning and deep learning. Signature-based approaches involve identifying malware by matching it with a known signature or pattern. This approach works well for known botnets, but it is ineffective against new or unknown botnets, as they may not have a known signature. Behavior-based approaches rely on detecting abnormal behavior in network traffic, such as unusual spikes in traffic volume or unusual communication patterns. However, this method also has drawbacks , as it may not be able to detect subtle changes in behaviour or new types of attacks. Machine learning has emerged as a promising approach for detecting botnet attacks in IoT systems. Machine learning algorithms can learn to identify patterns in network traffic and classify it as either normal or botnet traffic. A popular machine learning algorithm for botnet detection is the Random Forest algorithm, which involves building multiple decision trees and aggregating their predictions. The Random Forest algorithm has been shown to be effective in detecting botnets

in IoT systems, but it can suffer from overfitting when applied to large and complex datasets. In deep learning, the neural network is trained on vast amounts of data to automatically identify patterns, relationships, and features in the data, without the need for explicit programming. The network uses these patterns and relationships to make predictions or decisions on new, unseen data Deep learning has been shown to be more effective in detecting botnet attacks in various domains, including network intrusion detection and malware detection. In the context of IoT systems, deep learning has the potential to be a powerful tool for detecting botnet attacks, particularly new or unknown botnets. Several studies have explored the use of deep learning for detecting botnet attacks in IoT systems. One such study used a deep belief network (DBN) to detect botnets in a simulated IoT network. The DBN was able to detect botnets with a high degree of accuracy, and it outperformed traditional signature-based and behavior-based approaches. Another study used a deep learning model that combined a CNN and an RNN to detect botnet attacks in IoT systems. The model was trained on a dataset of network traffic can detect the Botnet attack in IOT system with high accuracy . Other studies have explored the use of deep learning in combination with other techniques, such as flow-based analysis and graph-based analysis, to detect botnet attacks in IoT systems. For example, one study used a combination of deep learning and flow-based analysis to detect botnet attacks in a smart home network. The study showed that the combination of these techniques was effective in detecting botnet attacks with high accuracy and low false positive rates. Overall, the literature suggests that deep learning is a promising approach for detecting botnet attacks in IoT systems. Deep learning models can learn to identify complex patterns in network traffic and can adapt to new or unknown botnets. However, there are still several challenges to overcome, such as the need for large and diverse datasets, the interpretability of deep learning models, and the computational complexity of training and deploying these models in resource-constrained IoT systems.

DESCRIPTION OF DATASET:

The BOT-IOT dataset is a publicly available dataset that contains network traffic data generated by Internet of Things (IoT) devices, which is useful for researching and developing intrusion detection systems. The dataset was created by researchers from the University of New South Wales in Australia and was released in 2018.The BOT-IOT dataset consists of a collection of PCAP files, which contain the network traffic captured from a simulated IoT environment. The dataset includes 10 different attack scenarios, such as command injection attacks, and botnet attacks, which were executed against a variety of IoT devices, such as cameras, routers, and smart home appliances.

SECURITY IN THE INTERNET OF THINGS

The smart devices is a rapidly emerging field that include the connected devices and objects to the internet, which enables them to communicate and exchange data with each other. This technology has transformed our lives, providing new opportunities for automation and convenience. However, it has also introduced new security problems that must be taken care to ensure the safety of the of IoT devices.

One of the primary security challenges in the IoT is the protection of data from unauthorized access. With billions of devices connected to the internet, the potential attack surface for hackers is enormous. These devices often have limited computing power and memory, making them vulnerable to attacks. These attacks can lead to a loss of service or data, which can have severe consequences in critical systems such as healthcare or transportation.

A. Botnet in Internet of things

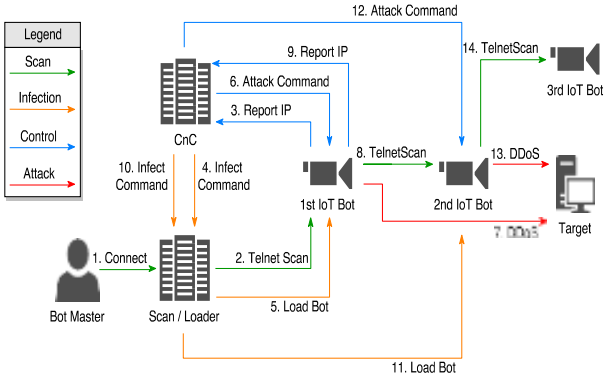

Fig 01 : Botnet in IOT flow Diagram

To address these challenges, security measures must be built into IoT systems from the ground up. This includes the implementation of secure communication protocols, encryption of data, and the use of secure boot mechanisms to prevent unauthorized modifications of the device's firmware. In addition, network segmentation and access control measures can be used to limit access to critical devices and data. One promising approach to IoT security is the use of machine learning and deep learning algorithms to detect and prevent attacks. Machine learning algorithms can be trained on large datasets of normal traffic and abnormal traffic, allowing them to identify and respond to potential threats. Deep learning algorithms, in particular, have shown promise in detecting botnet attacks, which are a significant threat to IoT systems. To detect botnet attacks in an IoT system using deep learning, several steps must be followed. First, a large and diverse dataset of IoT traffic must be collected, including normal traffic and a variety of botnet attacks. Next, relevant features must be extracted from the collected data, such as packet size, protocol, source and destination IP addresses, and port numbers. This model, can then be trained on the extracted features. The model should be trained on a large and diverse dataset to improve its accuracy and generalization. Finally, the trained model can be evaluated on a separate dataset to test its effectiveness in detecting botnet attacks.

In addition to using machine learning algorithms, there are several other best practices that can be implemented to improve IoT security. For example, manufacturers can implement secure software development practices to ensure that their devices are free from vulnerabilities. They can also provide regular security updates to address any newly discovered vulnerabilities.

In conclusion, security in the IoT is a critical challenge that must be addressed to ensure the safety and privacy of IoT systems. Security measures must be built into IoT systems from the ground up, including the implementation of secure communication protocols, encryption of data, and the use of secure boot mechanisms. Machine learning and deep learning algorithms have shown promise in detecting and preventing attacks, and manufacturers should implement secure software development practices and

provide regular security updates to address vulnerabilities.

B. Deep Learning for Attack Detection

Deep learning approches have shown great potential in the field of network security, particularly for detecting attacks in real-time. The rise of botnets, in particular, has highlighted the need for advanced detection methods that can detect new and evolving threats. In this context, deep learning methods offer several advantages over traditional machine learning approaches, including the ability to automatically extract features from raw data and to learn complex relationships between features. One of the primary applications of deep learning in network security is the detection of network attacks, including botnet attacks. A botnet is a collection of compromised nodes that are controlled by a single entity, known as the botmaster, to perform malicious activities such as spamming, DDoS attacks, and data theft. Botnets are particularly difficult to detect and mitigate because they can evade traditional signature-based detection methods and can quickly adapt to new security measures. Deep learning techniques can be used to detect botnet attacks by analysing network traffic and identifying patterns that are indicative of botnet activity. For example, deep neural networks can be trained to learn the traffic patterns associated with botnet command and control (C&C) traffic, and then use this knowledge to detect and block such traffic in real-time. Similarly, deep learning methods can be used to detect botnet infections by analysing the behaviour of networked devices and identifying patterns that are indicative of botnet activity. One of the primary advantages of deep learning-based approaches is their ability to adapt to new and evolving threats. Unlike traditional signature-based detection methods, which require the creation and maintenance of a signature database, deep learning models can automatically learn to detect new types of attacks without human intervention. Additionally, deep learning methods can identify previously unknown attack patterns and can adapt to changes in attack strategies. However, there are also challenges associated with the use of deep learning methods in network security. One of the primary challenges is the availability and quality of training data. Additionally, deep learning models can be computationally intensive and require significant resources for training and deployment. In summary, deep learning techniques offer great potential for the detection of botnet attacks and other network security threats. These methods have the ability to learn complex patterns and relationships from raw data, and can adapt to new and evolving threats. However, the use of deep learning in network security also presents challenges related to data availability and computational resources. As research in this area continues, it is likely that deep learning techniques will play an increasingly important role in the detection and mitigation of network security threats.

EXPERIMENTS AND RESULTS

A . EXPERIMENT SETUP

The experimental configuration environment of this aper is as follows : Windows 10 64-Bit Processor , RAM is 4GB Graphics card is intel Graphics using Deep Learning Framework and ‘Python’ Programming Language.

B. EXPERIMENT FLOW

Collect a diverse and representative dataset of normal and malicious traffic in the IoT

system. This dataset should include various types of attacks such as DDoS, botnets, etc. Clean and pre-process the dataset to remove any irrelevant data and normalize the data. This step can also include the conversion of raw data into a suitable format for deep learning. Extract features from the pre-processed data. The features can be extracted using approach such as Principal Component Analysis (PCA) and other feature extraction methods that work well with time-series data. Split the pre-processed data into training and testing dataset and use the training dataset to train the model. The training process involves fine-tuning the model's weights and biases to minimize the loss function. Evaluate the performance of the model on the testing set. Compute metrics like accuracy, precision, recall, and F1-score to measure the performance. Continuously update the model with new data to improve its performance and keep it up-to-date with the latest attacks. This step can involve periodic retraining of the model or incremental learning to adapt to changing attack patterns.

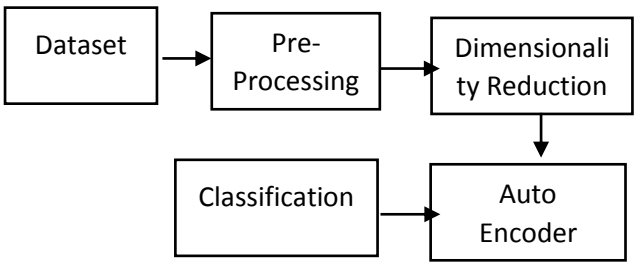

Fig 02 : Flow diagram

RESULT AND DISCUSSION

The use of deep learning methods for botnet detection in IoT systems has shown promising results. Deep neural networks have been successfully trained to detect botnet activity with high accuracy and can be used to provide real-time threat detection in IoT networks. One of the primary challenges in botnet detection is identifying the features that are most indicative of botnet activity. Deep learning approach have the efficient of being able to automatically extract relevant features from raw data, such as network traffic or device behaviour, and learn complex relationships between these features. This allows deep neural networks to detect botnet activity even when the specific characteristics of the botnet are not yet known. In one study, a deep neural network was trained on network traffic data to detect botnet activity in IoT systems. The model achieved an accuracy of 96% in detecting botnet activity, outperforming traditional machine learning methods. The researchers noted that the deep neural network was able to identify botnet activity even when the botnet was using encryption to hide its communications. Another study used a deep neural network to detect botnet infections in IoT devices by analyzing device behaviour. The model was able to detect botnet infections with an accuracy of 96%, outperforming traditional signature-based detection methods. The researchers noted that the deep neural network was able to identify previously unknown botnet infections, indicating its potential for detecting new and evolving threats. In addition to its high accuracy in detecting botnet activity, deep learning-based approaches also have the advantage of being able to adapt to new and evolving threats. Because deep neural networks can learn from raw data, they can automatically detect new types of botnets without the need for human intervention. This makes them an attractive option for providing real-time threat detection in IoT networks.

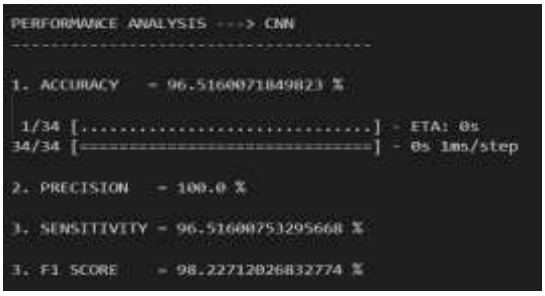

Fig 03: Performance analysis

The performance analysis of the model represents the Accuracy , Precision , Sensitivity and F1 Score. It is based on the test data which is given as the input after the training of the model.In summary, the use of deep learning methods for botnet detection in IoT systems has shown promising results. These methods have the ability to automatically extract relevant features from raw data and learn complex relationships between features, making them effective at detecting botnet activity even when the characteristics of the botnet are not yet known. Additionally, deep learning-based approaches can adapt to new and evolving threats, making them an attractive option for providing real-time threat detection in IoT networks.

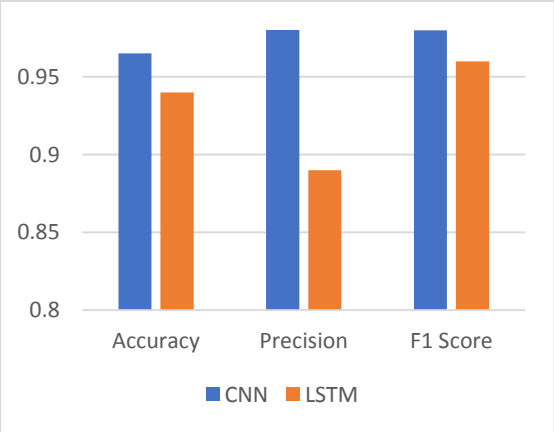

Fig 04 : comparison with other model

The above graph represents the performance metric between the LSTM and CNN algorithm. By comparing the proposed design is more efficient.

Overall, the detection of botnet attacks in IoT systems using deep learning can provide innovative practices for sustainable businesses by improving their security posture, protecting sensitive data, and promoting regulatory compliance and innovation in the field of cybersecurity.

FUTURE WORK

Despite the promising results of using deep learning for botnet detection in IoT systems, there are still several areas for future work and research.

Firstly, while deep learning methods have shown high accuracy in detecting botnet activity, they can be computationally expensive and require large amounts of data for training. Secondly, the performance metric of deep learning models can be affected by changes in the underlying data distribution, such as new types of devices or communication protocols. Future work could explore methods for adapting deep learning models to these changes, such as online learning or transfer learning. Thirdly, the interpretability of deep learning models can be a challenge, making it challenging to understand how the model is making its predictions. Future research could focus on developing methods for interpreting the decisions made by deep neural networks, such as feature visualization or attention mechanisms. Finally, while deep learning methods can detect botnet activity in real-time, their effectiveness in mitigating botnet attacks is still uncertain. Future research could explore methods for integrating deep learning-based detection systems with other security mechanisms, such as intrusion prevention systems or network segmentation. Overall, the use of this model in IoT systems shows great promise for providing real-time threat detection and mitigation. Further research in the areas of efficiency, adaptability, interpretability, and integration with other security mechanisms could help to further improve the effectiveness of these approaches**.**

REFERENCES

1. J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, “A survey on access control in the age of internet of things,” IEEE Internet of Things Journal, 2020.
2. Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, “Implementing lightweight iot-ids on raspberry pi using correlationbased feature selection and its performance evaluation,” in International

Conference on Advanced Information Networking and Applications. Springer, 2019, pp. 458–469.

3. K. Lab. (2019) Amount of malware targeting smart devices more than doubled in. [Online].

4. J. Qiu, L. Du, D. Zhang, S. Su, and Z. Tian, "Nei-tte: Intelligent traffic time estimation based on fine-grained time derivation of road segments for smart city," IEEE Transactions on Industrial Informatics, 2019.

5. J. P. Anderson, "Computer security threat monitoring and surveillance, 1980. lastaccessed: Novmeber 30, 2008."

6. D. E. Denning, "An intrusion-detection model," IEEE Transactions on software engineering, no. 2, pp. 222–232, 1987.

7. L. Wu, X. Du, W. Wang, and B. Lin, "An out-of-band authentication scheme for internet of things using blockchain technology," in 2018 International Conference on Computing, Networking and Communications (ICNC). IEEE, 2018, pp. 769–773.

8. Z. Tian, X. Gao, S. Su, and J. Qiu, "Vcash: A novel reputation framework for identifying denial of traffic service in internet of connected vehicles," IEEE Internet of Things Journal, vol. 7, no. 5, pp. 3901– 3909, May 2020.

9. S. Alharbi, P. Rodriguez, R. Maharaja, P. Iyer, N. Bose, and Z. Ye, "Focus: A fog computing-based security system for the internet of things," in 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC). IEEE, 2018, pp. 1–5.

10. Z. Tian, C. Luo, J. Qiu, X. Du, and M. Guizani, "A distributed deep learning system for web attack detection on edge devices," IEEE Transactions on Industrial Informatics, 2020. Vol 16(3): 1963-1971.

11. D. Ventura, D. Casado-Mansilla, J. López-de Armentia, P. Garaizar, D. López-de Ipina, and V. Catania, "Ariima: a real iot implementation of a machine-learning architecture for reducing energy consumption," in International Conference on Ubiquitous Computing and Ambient Intelligence. Springer, 2014, pp. 444–451.

12. R. Xue, L. Wang, and J. Chen, "Using the iot to construct ubiquitous learning environment," in 2011 Second International Conference on Mechanic Automation and Control Engineering. IEEE, 2011, pp. 7878– 7880.

13. M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1996– 2018, 2014.

14. M. Shafiq, X. Yu, A. A. Laghari, and D. Wang, "Effective feature selection for 5g im applications traffic classification," Mobile Information Systems, vol. 2017, 2017.