International Journal of Advance Research in Science and Engineering
Volume No. 13, Issue No. 03, March 2024
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Securing IOT Networks with Dynamic Learning and LSTM-Based Attack Detection

Mrs. Nilofar S. Hunnargi[1], Dr. Ajay D. Jadhav[2]

[1]*Electronics Engineering Department, Shivaji University Kolhapur*

[2] *Principal Dnyanshree Institute of Engineering & Technology [DIET], Satara, India.*

Abstract:

The Internet of Things (IoT) has revolutionized the way we interact with technology, connecting a myriad of devices to create smart and interconnected ecosystems. However, the rapid proliferation of IoT devices has also introduced unprecedented security challenges, making IoT networks prime targets for cyber-attacks. Securing these networks requires innovative approaches that can adapt to evolving threats, and one such approach is the integration of dynamic learning and Long Short-Term Memory (LSTM)-based attack detection mechanisms.

Keywords: DDOS Attack, Intrusion Detection Systems, IOT Networks, Machine Learning.

I. Introduction

Dynamic learning algorithms empower IoT networks to learn from their environments, constantly updating their defense strategies to counter new and emerging threats. This adaptability is crucial in the dynamic and heterogeneous IoT landscape, where traditional static security measures often fall short. By incorporating dynamic learning capabilities, IoT devices and networks can proactively identify and mitigate potential security breaches, enhancing overall resilience and reliability.

This work aims to explore the fusion of dynamic learning and LSTM-based attack detection specifically tailored for IoT networks. By developing and implementing these advanced security measures, we strive to create a robust framework that safeguards IoT ecosystems from malicious activities, ensuring the privacy, integrity, and availability of IoT-enabled services and applications.

II. Literature Survey

The literature survey is focused on various security algorithms, developed for making the system secure against Distributed Denial of Service (DDoS) attacks. Most of the algorithms are based on deep learning approaches.

In [1] Deep learning-based DDoS attack detection approach called DeepDefense is used and DDoS attacks, countermeasures, statistical methods, and machine learning approaches are Discussed. Shallow representation models limit conventional machine learning techniques. Statistical methods in DDoS detection need feature selection improvements. In [2], authors introduce a deep-learning classifier for

low-power radios, utilizing an LSTM framework sensitive to persistent signal imperfections. Experimental results show high resilience to software radio adversaries, achieving 99.58% accuracy with a 2-layer LSTM mod In [3], the authors introduce a deep-learning-based classifier focused on learning hardware imperfections in low-power radios that are difficult for high-power adversaries to emulate. They use an LSTM framework sensitive to signal imperfections over long durations, achieving 99.58% accuracy in classifying devices. The study also presents a wireless device identification platform using deep learning (DNN, CNN, RNN) to enhance IoT security, demonstrated with RF data from ZigBee devices across various SNR levels. The models serve as an intrusion detection system, detecting impersonation attacks and improving network security, accessibility, authentication, and integrity. Experimental results show the effectiveness of deep learning in wireless device identification for enhancing IoT security. In [4], the authors propose a blockchain-enabled data collection and sharing scheme using Ethereum blockchain and deep reinforcement learning (DRL) to ensure reliability and security. DRL optimizes data collection, while blockchain guarantees secure data sharing. Simulations show superior security and resistance to attacks compared to traditional database-based schemes across various attack types. In [5], the authors propose a distributed deep learning approach for cyber-attack detection in fog-to-things computing. They argue that traditional methods lack accuracy and scalability in IoT settings. By leveraging deep learning and hardware advancements, they demonstrate improved detection accuracy, lower false alarms, and scalability in edge networks, making fog-to-things computing ideal for attack detection due to its data richness and deep learning's capabilities.

In [6], the authors have presented the architecture of cloud-assisted IoT applications for smart cities, telemedicine, and intelligent transportation system. Authors have considered current security threat obstacles to the adoption of IoT technology in many areas. Authors investigate the security threats and attacks due to unauthorized access and misuse of information collected by IoT nodes and devices. Further, the authors describe the possible countermeasure to these security attacks. In [7], the authors introduce Deep-Feature Extraction and Selection (D-FES), combining stacked feature extraction and weighted feature selection. They demonstrate its effectiveness in reducing bias and computational complexity. Experimental results on the AWID dataset show a detection accuracy of 99.918% and a false alarm rate of 0.012%, making it the most accurate detection of impersonation attacks reported. In [8], the authors have addressed the need for an automated testing framework to help security analysts to detect errors in learning-based IoT traffic detection systems. The authors have given the method of a testing framework for learning-based IoT traffic detection systems, TLTD. With genetic algorithms, TLTD can generate opposing samples for IoT traffic detection systems and may perform a black-box test on the systems. In [9], the authors collaborate with consumers and security experts to develop a Consumer Security Index (CSI) for IoT devices. They use a methodology involving focus groups, online

surveys, and natural language processing to identify and evaluate security features, consumer preferences, and manufacturer communication about device security. The goal is to create a user-friendly index that informs consumer decisions and encourages manufacturers to prioritize security in IoT device production. In [10], the authors review current IoT security standards and highlight three key contributions: increasing government interest in baseline security requirements, dominance of de facto standards by industry associations, and challenges in setting universal security baselines and monitoring standards adoption. The paper aims to improve understanding of IoT security standards evolution and proposes a more coordinated approach to standards development and deployment. In [11], the authors introduce an IoT-enabled smart security system for homes. The system captures images of intruders and sends them to authorized emails via SMTP, enhancing home security. It also automates home appliances using IoT, reducing human effort. The system is controlled by a Raspberry Pi3 microcontroller, interfaced with various sensors and a camera for effective monitoring and control.

In [12], the authors propose a PUF-based authentication protocol for IoT devices, leveraging unique analog/RF properties during transmission for secure identification. They utilize a deep neural network-based framework called RF-PUF to extract entropy information from inherent process variations in wireless transmitters, achieving robust identification without additional circuitry. Simulation results demonstrate the framework's ability to distinguish up to 10,000 transmitters with a low false detection probability. In [13], the authors introduce a scalable and efficient homologous binary search scheme (IHB) for IoT firmware security analysis. They leverage readable strings in binaries and employ string filtering and MinHash techniques to achieve accuracy and efficiency. Testing on a real dataset shows significant improvements in efficiency, true positive rate (92.88%), and false-positive rate (2.83%) compared to existing methods. The authors also provide their tools and datasets for open science and future enhancements. In [14], the authors found the functional requirements within the IoT information security sharing system to verify the functions to be performed between the individuals within the reference model of the IoT information security sharing system. IoT is being applied to varied industries, and market activation is fully swinging in the home- appliance, medical, and transportation fields closely associated with life. Authors have addressed current security vulnerabilities of assorted industries, reported in various fields, but only security requirements exist, but there's no technical countermeasure, and policy issues and security matters are discussed only within the field of standardization. Authors also deduce that to address the widespread infringement accidents, an information security sharing system within the IoT environment which will be applied directly within the field is required.

In [15], the authors present basic elements of IoT models and supply situation assessment for IoT applications. Authors have highlighted the protection enhancement measures for the IoT

applications supported by the three domains (local, transfer, and data storage) of the IoT model. The author has addressed challenges in IoT systems in terms of the confidentiality, authenticity, and integrity of the info sensed, collected, and exchanged by the IoT objects. These challenges make IoT deployments extremely liable to differing kinds of security attacks, leading to insecure IoT environments.

In [16], the authors have given the on-demand security configuration technique that can be configured for required security functions and reorganized them without recreating the device image. For a massive number of devices in IoT, with the help of this approach, if there is a change in this security service, the author's technique can substitute the old modules for new ones without regenerating the device image. In [17], authors introduce a secure multi-hop routing protocol for IoT devices, combining authentication and routing processes efficiently. The protocol uses multi-layer parameters for enhanced security without significant overheads, making it suitable for IoT communication. In [18], the author explores circuit designs of emerging memory devices for nonvolatile logic, security circuits, and CIM for DNNs, showcasing silicon-verified examples of these circuits. In [19], the author discusses the use of deep learning in security systems, focusing on collaborative deployment and energy-efficient security enhancements using game theory. In [20], authors analyze IoT security from Perception, Transportation, and Application levels, highlighting challenges and opportunities for creating a "trust ecosystem" in SIoT.

In [21], the author presents a certification methodology for IoT security assessment, based on ISO 31000 and ETSI's Risk-based Security Assessment, to empower testers in evaluating security solutions for large-scale IoT deployments.

III Methodology:

A Dynamic Learning-Based Algorithm (DLBA) analyses network behavior and detect attack. This algorithm is designed to monitor and analyze network traffic, identify anomalous patterns, and detect potential attacks in a networked environment. The work integrates various functionalities essential for network management and security. It includes components for message broadcasting, route discovery, timers, metric computation, and packet queue operations. These functionalities collectively contribute to the efficient operation of the DLBA algorithm in monitoring and managing network resources. One crucial aspect of the work is its utilization of machine learning techniques, specifically deep learning methods such as Long Short-Term Memory (LSTM) networks. LSTM networks are a type of recurrent neural network (RNN) capable of learning long-term dependencies and temporal patterns in sequential data, making them well-suited for time-series analysis tasks like network traffic monitoring.

The work incorporates attack detection mechanisms using LSTM model. This model is trained on a dataset comprising network traffic features and attack labels, enabling them to learn the characteristics of normal network behavior and detect deviations indicative of potential attacks.

Overall, the work provides a comprehensive framework for dynamic learning-based network analysis and attack detection, leveraging machine learning techniques to enhance network security and performance. An LSTM-based method is implemented for attack detection in network traffic. LSTM is a type of recurrent neural network (RNN) that is well-suited for processing sequential data, making it ideal for tasks such as time-series analysis, natural language processing, and in this case, analyzing network traffic patterns. The LSTM network is trained using a dataset that includes features extracted from network traffic, such as packet timings, sizes, headers, source/destination addresses, and other relevant information.

Feature Extraction:

Before inputting data into the LSTM network, feature extraction is performed to convert raw network traffic data into meaningful numerical representations. Features may include statistical measures, frequency domain analysis results, time-based features, and other engineered attributes that capture the underlying patterns in the data.

Model Training:

a training phase where the LSTM network learns from the labelled dataset, which contains instances of normal network behaviour and various types of attacks. During training, the LSTM network adjusts its internal parameters (weights and biases) to minimize a predefined loss function, optimizing its ability to differentiate between normal and attack patterns.

Prediction and Detection:

After training, the LSTM network is capable of making predictions on new, unseen data. In the context of attack detection, the network analyzes incoming network traffic patterns and classifies them as normal or potentially malicious based on the learned patterns. Detection decisions are typically based on thresholds or confidence levels determined during training and validation phases.

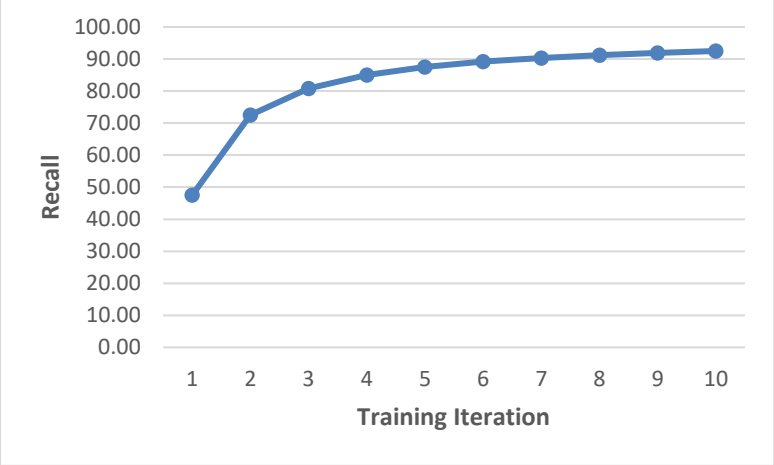
Evaluation:

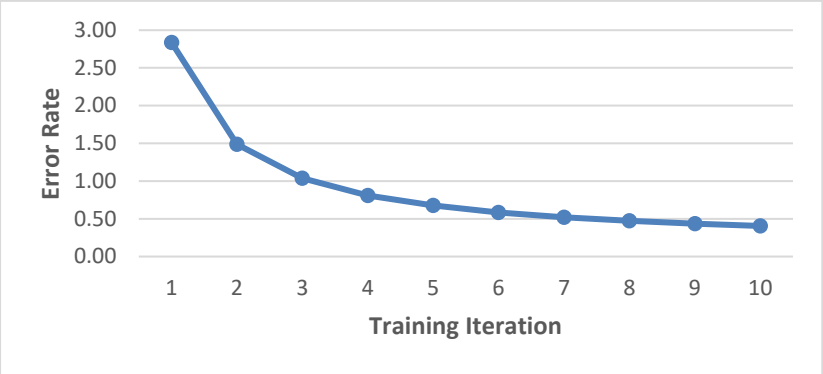
The performance of the LSTM-based attack detection method is evaluated using metrics such as accuracy, precision, recall, error rate.LSTM to develop an effective and robust system for detecting and responding to network attacks based on observed traffic patterns.

Simulation environment: The number of nodes set to 150 nodes.An energy model is specified along with the initial energy of 100 Joules. Various parameters like channel thresholds, data rates, topology, tracing, and node configurations are set. Nodes are configured as Base Stations, Access Points, Gateways, Internet nodes, and attackers like DDos, Injection, Zero-day, and Man-in-the-Middle attackers. Attackers are placed strategically based on the network size.CBR (Constant Bit Rate) traffic

is generated between nodes, simulating communication patterns. Various events like frequency updates and result collection are scheduled during the simulation. Overall, this environment simulates a network with multiple nodes, energy constraints, routing protocols, and various types of attackers, allowing for the analysis of network behavior under different conditions and attack scenarios.

IV Results:





The graph for Accuracy, Precision and Recall shows an upward trend, indicating that as the model undergoes more iterations, its value improves. At iteration 10 final accuracy reaching is 99.59, precision 99.58 and recall 92.5%.The graph for Error rate shows a downward trend, indicating that as the model undergoes more iterations, its error rate reduces, at iteration 10 error rate is 0.40.

As accuracy increases, the error rate decreases. However, achieving very high accuracy might lead to overfitting, where the model learns the training data too well but fails to generalize to new, unseen data. Conversely, reducing the error rate might require simplifying the model, potentially sacrificing accuracy.

Increasing precision often leads to a decrease in recall and vice versa. This trade-off is known as the precision-recall trade-off. A high precision means the model is conservative in its predictions, avoiding false positives, but it might miss some positive instances, leading to lower recall. Conversely, a high recall means the model captures more positive instances but might include more false positives, reducing precision. These trade-offs highlight the importance of evaluating machine learning models based on multiple metrics and understanding the balance between different performance measures to ensure the model's effectiveness and generalization capability.

Conclusion

Securing IoT networks with dynamic learning and LSTM-based attack detection represents a proactive and intelligent approach to mitigating the ever-evolving cybersecurity challenges faced by IoT ecosystems. By combining dynamic learning algorithms that enable networks to adapt and learn from their environments with LSTM-based models that excel in detecting complex patterns and anomalies, we can create a resilient defense mechanism against a wide range of cyber threats.

The synergy between dynamic learning and LSTM-based attack detection is instrumental in safeguarding IoT networks, enabling them to fulfill their potential as transformative technologies while mitigating the associated security risks effectively. Through ongoing research and innovation in this field, we can continue to enhance the security and resilience of IoT ecosystems, fostering trust and confidence in the adoption of IoT technologies across various domains and industries.

References:

[1] Xiao yong Yuan et al. “Deep Defense: Identifying DDoS Attack via Deep Learning”2017 IEEE International Conference on Smart Computing (SMARTCOMP).

[2] R. Das, A. Gadre, S. Zhang, S. Kumar, and J. M. F. Moura, "A Deep Learning Approach to IoT Authentication," *2018 IEEE International Conference on Communications (ICC)*, Kansas City, MO, 2018, pp. 1-6. DOI: 10.1109/ICC.2018.8422832

[3] H. Jafari, O. Omotere, D. Adesina, H. Wu and L. Qian, "IoT Devices Fingerprinting Using Deep Learning," *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, Los Angeles, CA, USA, 2018, pp. 1-9. DOI: 10.1109/MILCOM.2018.8599826

[4] C. H. Liu, Q. Lin, and S. Wen, "Blockchain-enabled Data Collection and Sharing for Industrial IoT with Deep Reinforcement Learning," in *IEEE Transactions on Industrial Informatics*. DOI: 10.1109/TII.2018.2890203

[5] A. Abeshu and N. Chilamkurti, "Deep Learning: The Frontier for Distributed Attack Detection in Fog-to-Things Computing," in *IEEE Communications Magazine*, vol. 56, no. 2, pp. 169-175, Feb. 2018. DOI: 10.1109/MCOM.2018.1700332

[6] Alsaidi and F. Kausar, "Security Attacks and Countermeasures on Cloud Assisted IoT Applications," *2018 IEEE International Conference on Smart Cloud (SmartCloud)*, New York, NY, 2018, pp. 213-217. DOI: 10.1109/SmartCloud.2018.00043

[7] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo and K. Kim, "Deep Abstraction and Weighted Feature Selection for Wi-Fi Impersonation Detection," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp. 621-636, March 2018.
DOI: 10.1109/TIFS.2017.2762828

[8] Xiaolei Liu, Xiaosong Zhang, Nadra Guizani, Jiazhong Lu, Qingxin Zhu, Xiaojiang Du, “TLTD: A Testing Framework for Learning-Based IoT Traffic Detection Systems”, Sensors 2018, 18, 2630; doi:10.3390/s18082630

[9] J. M. Blythe and S. D. Johnson, "The consumer security index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices," Living in the Internet of Things: Cybersecurity of the IoT - 2018, London, 2018, pp. 1-7. DOI: 10.1049/cp.2018.0004

[10] I. Brass, L. Tanczer, M. Carr, M. Elsden and J. Blackstock, "Standardising a moving target: The development and evolution of IoT security standards," Living in the Internet of Things: Cybersecurity of the IoT - 2018, London, 2018, pp. 1-9. DOI: 10.1049/cp.2018.0024

[11] M. L. R. Chandra, B. V. Kumar, and B. SureshBabu, "IoT enabled home with smart security," 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, 2017, pp. 1193-1197. DOI: 10.1109/ICECDS.2017.8389630

[12] B. Chatterjee, D. Das and S. Sen, "RF-PUF: IoT security enhancement through authentication of wireless nodes using in-situ machine learning," 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, DC, 2018, pp. 205-208. DOI: 10.1109/HST.2018.8383916

[13] Y. Chen, H. Li, W. Zhao, L. Zhang, Z. Liu, and Z. Shi, "IHB: A scalable and efficient scheme to identify homologous binaries in IoT firmware," 2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC), San Diego, CA, 2017, pp. 1-8. DOI: 10.1109/PCCC.2017.8280478

[14] J. Choi, Y. Shin, and S. Cho, "Study on information security sharing system among the industrial IoT service and product provider," 2018 International Conference on Information Networking (ICOIN), Chiang Mai, 2018, pp. 551-555. DOI: 10.1109/ICOIN.2018.8343179

[15] P. K. Chouhan, S. McClean, and M. Shackleton, "Situation Assessment to Secure IoT Applications," 2018 Fifth International Conference on Internet of Things: Systems, Management, and Security, Valencia, 2018, pp. 70-77. DOI: 10.1109/IoTSMS.2018.8554802

[16] B. Chung, J. Kim and Y. Jeon, "On-demand security configuration for IoT devices," 2016 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2016, pp. 1082-1084. DOI: 10.1109/ICTC.2016.7763373

[17] P. L. R. Chze and K. S. Leong, "A secure multi-hop routing for IoT communication," 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, 2014, pp. 428-432. DOI: 10.1109/WF-IoT.2014.6803204

[18] C. Dou et al., "Challenges of emerging memory and memristor-based circuits: Nonvolatile logics, IoT security, deep learning, and neuromorphic computing," 2017 IEEE 12th International Conference on ASIC (ASICON), Guiyang, 2017, pp. 140-143. DOI: 10.1109/ASICON.2017.8252431

[19] C. Esposito, X. Su, S. A. Aljawarneh and C. Choi, "Securing Collaborative Deep Learning in Industrial Applications Within Adversarial Scenarios," in IEEE Transactions on Industrial Informatics, vol. 14, no. 11, pp. 4972-4981, Nov. 2018. DOI: 10.1109/TII.2018.2853676

[20] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges," in IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2483-2495, Aug. 2018. DOI: 10.1109/JIOT.2017.2767291

[21] S. N. M. García, J. L. Hernández-Ramos and A. F. Skarmeta, "Test-based risk assessment and security certification proposal for the Internet of Things," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 641-646. DOI: 10.1109/WF-IoT.2018.8355193