

Utilizing Deep Learning for Intrusion Detection in IoT-Enabled Smart Networks

Rahul Palaria^{1*}, Shivam Pujari²

¹Assistant Professor, Amrapali University.

²Assistant Professor, BIAS Bhimtal.

*Corresponding Author

Rahul Palaria

Assistant Professor,
Amrapali University.

Article History

Received: 14.04.2025

Accepted: 28.05.2025

Published: 22.06.2025

Abstract: The rapid growth of IoT-based smart environments has created a multitude of considerable security vulnerabilities due to heterogeneous devices and constantly changing network conditions. Traditional intrusion detection systems (IDS) often lack the sophistication necessary to effectively detect new attacks, requiring innovative, dynamic methods. In this paper we propose a unique intrusion detection framework that utilizes a Hierarchical Bi-directional Long Short Term Memory (Bi-LSTM) model optimized with a Multi-Objective Bat Algorithm (MOBA). The Bi-LSTM model learns from future, and past data sequences to improve intrusion detection performance by enhancing accuracy when learning temporal patterns. The MOBA model optimizes the Bi-LSTM model by learning to select the best features for a supervised classifier, optimizing the model concurrently with optimizing the parameter tuning. Experimental verification of the proposed framework utilizing benchmark datasets confirms the proposed IDS framework is generally superior to the other methodologies for detection accuracy, total cost of false alarms, and total time to execute the IDS framework. The proposed IDS also shows a distinctive balance of balance feature selection and optimizing parameters, and great opportunity of performance without sacrificing execution times, potentially enabling the deployment of the IDS in resource-limited IOT environments and the ability to create an intelligent and scalable response to changing cyber-threats.

Keywords: Intrusion Detection, Internet of Things (IoT), Deep Learning, Bi-LSTM & Network Security.

Cite this article:

Palaria, R., Pujari, S., (2025). Utilizing Deep Learning for Intrusion Detection in IoT-Enabled Smart Networks. *ISAR Journal of Science and Technology*, 3(6), 40-44.

1. Introduction

Internet of Things (IoT) can be defined as a network of numerous devices that interconnects smart sensors, applications & related technologies to establish reliable communication between physical devices over the internet (Hamzei & Navimipour, 2018) [1]. IoT is applied extensively in the construction of smart cities, smart transportation, smart healthcare & smart industrial control systems (Seth et al., 2021) having transformed the operation of conventional network systems. [2] IoT architecture can be tailored to fit application needs. Although IoT design is not agreed upon everywhere, a three-layered architecture fit for different uses is usually acknowledged. There is a physical resource layer, a network layer, and a data application layer at least in the basic system architecture. as displayed in picture 1.1.

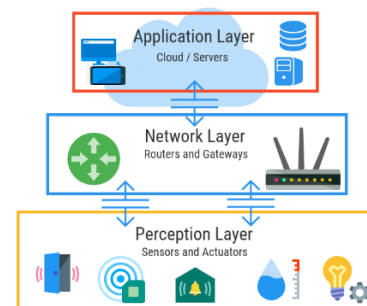


Figure 1.1: IoT architecture shown schematically

We review the three layers as follows:

The perception layer gathers real-time data from several communication devices by including physical resources including sensors and actuators.

The network layer makes use of several networking protocols to create safe connection between network devices. This layer guarantees network security and quality of service by means of safe device-to-communication.

Delivering applications tailored to a given level of responsibility falls to the application layer. This is a layer of great importance that can be attacked in several ways securitywise. Using a deep learning method at this level improves IoT network dependability and security.

IoT based smart environments raise major issues regarding security of network infrastructure. The smart environment is becoming quite vulnerable to network attacks or illegal incursions as IoT systems get more and more of importance. Among the main needs of modern times are security of IoT systems (Atlam & Wills, 2020). [3]. Three fundamental qualities define a safe system: availability, integrity, and confidentiality (Chanal & Kakkasageri, 2020). [4]. These elements play a great part in protecting smart environments against numerous assaults including distributed DOS attacks (DDoS), spoofing attacks, data modification, malicious node injection, eavesdropping etc. The great popularity of IoT based smart applications has raised security of these systems' related issues (Mrabet et al., 2020). [five] Extensive study in this area has been conducted in past ten years; several researchers have suggested numerous approaches like cryptography (Dhanda et al., 2020) [6], access control (Qio et al., 2020) [7], intrusion detection (Hajiheidari et al., 2019) [8] etc. to guard IoT systems from cyberattacks. These methods have a narrow horizon in reducing the cyberattacks and dangers, though. The IoT security suffers from several unidentified undetectable intrusions. Different publications have proposed the use of intrusion detection systems for spotting such intrusions which were not discovered by traditional methods (Sugi & Ratna, 2020) [9].

Generally speaking, IDS come in two flavors: anomaly-based and signature-based ones. Based on preset policies or attack signatures, the Signature-based IDS detects illegal access (Soe et al., 2019). [10]. To find the risks and attacks in the network, anomaly-based IDSs track real-time network traffic in comparison to previously learnt network traffic patterns (Otoum & Nayak, 2021). [11] Signature based IDS miss new attacks even if they produce superior results. High false positive rates of the anomaly based techniques influence the accuracy and dependability of the attack detection process (Aljawarneh et al., 2018) [12]. This is mostly related to the great volume of data in which these methods cannot detect the intrusion behavior in big scale network systems. An efficient Intrusion Detection System (IDS) should be able to quickly scan significant volumes of network traffic data in order to properly identify and prevent harmful assaults in their early phases. Thus, it is imperative to create a very strong IDS that transcends the limits of present systems.

Several papers have developed IDS (Liang et al., 2019) using intelligent and computationally efficient methods grounded on artificial intelligence, machine learning, and deep learning. [13] ([Thamilarasu & Chawla, 2019) [14] (Zhong et al., 2021). [15][

These techniques can detect real time attacks in network data traffic in smart environments. Conventional techniques such as rule based methods require predefined strategies, labeled data and feature sets for training. This restricts their adaptability in identifying novel or unknown attacks in dynamic environments such as IoT. ML and DL algorithms can be considered as a potential solution to overcome the drawback of rule based techniques. The autonomous operation of ML and DL algorithms continuously monitor the network traffic and does not require any predefined strategies and feature sets for attack detection (Chesney et al., 2020) [16]. These techniques exhibit superior potential in monitoring the network traffic along with classification and prediction of network attacks. However, ML algorithms depend on the availability of malicious data for identifying the threats. Therefore, it becomes prominent to upgrade the attack detection model using a dataset which contains new threats. Several literary works have validated the effectiveness of DL algorithms in detecting security threats (Samy et al., 2020) [17] (Pecori et al., 2020) [18]. DL algorithms are capable of identifying and categorizing different types of heterogeneous network traffic.

To help them to handle challenging and high level security issues, DL models include an unsupervised learning mechanism to provide hierarchical representation of the data. Better accuracy over current shallow models is achieved by DL models using a stacked neural network layer design. Given the benefits of DL methods, this work suggests using a DL model to identify unidentified intrusions in heterogeneous IoT based smart systems. Further parts address a quick summary of the suggested research approach.

2. Related Works

Intrusion Detection Systems (IDS) have been developed using somewhat extensive application of ML and DL techniques. Numerous research have validated the effectiveness of these algorithms in reaching enhanced accuracy in intrusion detection (Diro & Chilamkurti, 2018) [19], (Sriram et al., 2020) [20], (Tian et al., 2019) [21]. For example, a 2020 Ferrag et al. [22] survey looked at how DL algorithms were used to identify unexpected intrusions and assessed their performance using real-time network traffic datasets including the CSE-CIC-IDS 2018 and Bot-IoT datasets.

In a 2020 Mebawondu et al. [23] [23] lightweight IDS based on the Multi-layer Perceptron (MLP) and information gain technique was developed. The method added data mining methods to improve intrusion detection accuracy. With an accuracy of 76.96%, experimental data revealed a positive correlation and possibility for real-time intrusion detection. The suggested work did not, however, assess the efficacy of the model using varying attribute counts.

Using a deep neural network (DNN) for IoT intrusion detection was another strategy Alladi et al. (2021) [24] followed. DNN provides an output depending on its learning capacity by use of nonlinear transformation approaches to evaluate inputs. However, DNN may encounter vanishing gradient problems in lower layers of the network.

Liang et al. (2020) [25] and Miao et al. (2021) [26] explored the implementation of a Deep Reinforcement Learning (DRL) method for detecting attacks and intrusions. The DRL algorithm utilizes efficient Q-learning mechanisms to enable automated decision-

making without prior knowledge of the environment. However, the performance of the DRL algorithm can be impacted by sampling efficiency issues.

3. Problem Statement

The IoT Environment is highly dynamic in nature and with its wide distribution and heterogeneous nature of resources is vulnerable to security threats. IoT is now widely used in various applications such as Industrial Process and Operations, Sensors, Health Care, Automobiles manufacturing, Environmental monitoring and health safety, etc. The Wireless Nature of IoT Environment makes it a easier target for attackers. Developing an IoT infrastructure to detect vulnerability from unknown threads and attacks is the need of the day. Intrusion detection has become an important process in any network communications due to the advances happening in the recent years in IT industries. Threats are rising day by day with increased use of the internet and cloud environments. In recent years, numerous methods have been developed to identify and mitigate network attacks. Researchers have explored the application of machine learning (ML) and deep learning (DL) techniques to detect intrusions.

Majority of the DL methods used for dealing with intrusion detection do not perform well with varying patterns of attacks. Since the attack features/attributes are not specifically considered, detection accuracy shall be less in such cases. In addition, there are certain limitations associated with existing deep learning approaches used for IDS, which needs to be resolved in order to enhance the accuracy of IDS in IoT systems.

- With the increase in the number of layers of the deep network the computational complexity of the network increases. This problem also results in the latency problem.
- Existing works do not focus on resource consumption while developing IDS for constrained systems such as big data systems. This factor should be considered while designing IDS.
- Existing approaches for enhancing the security of the network based on attack detection depend on sophisticated and complex computations. Besides, providing security to IoT networks with resource-constrained devices and performing complex computations is challenging

Despite the availability of several techniques, there is a great scope of research in this field since these models do not consider the varying data patterns and features for encrypted networks, which can have a negative impact on their classification accuracy. Therefore, there is a significant need for a highly efficient model that can deliver precise detection performance.

4. Research Objectives

The aim of the research is the development of an efficient IDS using a deep learning approach for enhancing security in IoT based smart environments. The research objectives to achieve the above mentioned aim are as follows:

- To monitor the network traffic continuously and identify suspicious activities with the traffic at early stages of the attack.

- To extract only relevant and appropriate features for attack detection in order to make the proposed approach compact and fast.
- To achieve a high accuracy in detecting different attack with a low false positive rate.
- To optimize DL algorithms using a multi-objective optimization technique to improve the learning rate and execution process.
- To validate the performance of the proposed approach by comparing the results with other existing IDS detection models.

5. Proposed Research Methodology

This research proposes an optimized DL framework for developing an efficient IDS for securing IoT based smart systems from adversarial attacks. The study proposes a Hierarchical Bi-directional Long Short Term Memory (Hierarchical Bi-LSTM) algorithm for detecting intrusions in the IoT environment. The Hierarchical Bi-LSTM will be optimized using a multi-objective BAT algorithm (MOBA). As inferred from the existing works, most of the IDS models do not consider varying data patterns for detecting attacks and this reduces the detection accuracy since most of the novel security attacks are not detected. In order to address this constraint, the present research aims to overcome the limitation by incorporating diverse data patterns and training the model to learn from previous instances, rather than relying solely on predefined rules or strategies. Since, LSTM models use only the previous and current data instances for training, their capacity is limited. Hence this study proposes the implementation of a hierarchical Bi-LSTM model that uses future data instances for future predictions along with the previous and current timestep. In addition, the hierarchical Bi-LSTM combines two or more Bi-LSTMs and has the capability to learn complex contextual and temporal features from highly nonlinear IoT data. The study also proposes an optimization algorithm known as MOBA. The study evaluates the effectiveness of the DL algorithms considering various attack patterns. The proposed intrusion detection system will be evaluated with various performance metrics and compared with existing techniques to prove the efficacy.

5.1 Overview of the proposed approach

The Hierarchical Bidirectional LSTM is an enhanced version of conventional LSTMs that improves the performance of system architecture in sequence classification tasks. It effectively tackles the challenge of utilizing all time steps within the input sequence to enhance performance. This model trains two LSTMs instead of one LSTM on the input sequence, resulting in enhanced capabilities. Bi-LSTM overcomes the limitation of conventional RNN approach of storing the long length sequences. The proposed approach involves utilizing a hierarchical Bi-LSTM to extract contextual features from historical and future data instances. These features are then combined within the hierarchical Bi-LSTM to generate the output.

On the other hand, the BAT optimization algorithm will be used for finding optimal parameters for the Bi-LSTM model in order to enhance its performance and to assist the Bi-LSTM model to achieve an optimal solution with reduced number of iterations. In the optimization process, the parameters of the Bi-LSTM model will be tuned in order to increase the flexibility and robustness of

the intrusion detection process. Since, the parameters of the DL algorithms affect the efficiency of the intrusion detection process it is essential to determine the optimal parameters for improving the efficiency. Here, the is used as a multi-objective algorithm since it simultaneously performs feature selection and optimization of Bi-LSTM algorithm. A novel feature selection based approach for intrusion detection in IoT systems is proposed in this research. The optimal collection of features for the hierarchical Bi-LSTM model to identify IoT intrusions will be discovered using the MOBA technique.

5.2 Proposed Workflow

The suggested method's process consists in several phases including:

Different intrusion detection datasets like TON_IoT datasets, UNSW-NB15, NSL-KDD dataset etc. will be obtained at this round of data collecting.

Preprocessing helps to filter pointless data and uncertainty like missing data, null values from the input data. An vital part of the intrusion detection process, preprocessing greatly helps to raise the detection accuracy.

The pertinent and important features from the data will be chosen in the step of feature selection. Just the pertinent features from the processed data are chosen throughout this procedure to lower computational complexity and increase execution speed.

(d) Recognition of Intrusion Hierarchical Bi-LSTM model will help to identify security intrusion or threats. The MOVA approach will help to maximize the Bi-LSTM model.

Several criteria including accuracy, precision, recall, F-measure, and false alarm rate (FAR) will be used in the performance assessment of the suggested approach.

5.3 Tools and Software Platforms

We shall apply the experimental analysis with Python. Both benign and malicious samples will be taken under consideration for the experimental analysis in this work. While twenty percent will be utilized for testing, eighty percent will be used for instruction. TensorFlow will be the backend of Kera's library while DL classifiers will be constructed from Kera's library.

6. Expected Outcome

The paper suggests a DL based attack detection method for smart IoT environment. Combining a swarm intelligence based MOVA for feature selection with deep learning based hierarchical Bi-LSTM for intrusion detection, the approach is a feature selection and optimization based one. The intended intrusion detection method will be made to achieve very low false detection rate and great detection accuracy. The proposed model is predicted to be a lightweight system having great execution time and accompanied with reduced number of resources using a computationally light swarm intelligence algorithm. Furthermore projected to be able to address data dimensionality problems and increase IoT scalability, throughput, and dependability is the suggested solution.

References

1. Hamzei, M., & Navimipour, N. J. (2018). Toward efficient service composition techniques in the internet of things. *IEEE Internet of Things Journal*, 5(5), 3774-3787.
2. Seth, I., Panda, S. N., & Guleria, K. (2021, October). IoT based smart applications and recent research trends. In *2021 6th International Conference on Signal Processing, Computing and Control (ISPCC)* (pp. 407-412). IEEE.
3. Atlam, H. F., & Wills, G. B. (2020). IoT security, privacy, safety and ethics. In *Digital twin technologies and smart cities* (pp. 123-149). Springer, Cham.
4. Chanal, P. M., & Kakkasageri, M. S. (2020). Security and privacy in IOT: a survey. *Wireless Personal Communications*, 115(2), 1667-1693.
5. Mrabet, H., Belguith, S., Alhomoud, A., & Jemai, A. (2020). A survey of IoT security based on a layered architecture of sensing and data analysis. *Sensors*, 20(13), 3625.
6. Dhanda, S. S., Singh, B., & Jindal, P. (2020). Lightweight cryptography: a solution to secure IoT. *Wireless Personal Communications*, 112(3), 1947-1980.
7. Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S., & Fang, B. (2020). A survey on access control in the age of internet of things. *IEEE Internet of Things Journal*, 7(6), 4682-4696.
8. Hajiheidari, S., Wakil, K., Badri, M., & Navimipour, N. J. (2019). Intrusion detection systems in the Internet of things: A comprehensive investigation. *Computer Networks*, 160, 165-191.
9. Sugi, S. S. S., & Ratna, S. R. (2020, December). Investigation of machine learning techniques in intrusion detection system for IoT network. In *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)* (pp. 1164-1167). IEEE.
10. Soe, Y. N., Feng, Y., Santosa, P. I., Hartanto, R., & Sakurai, K. (2019). Rule generation for signature based detection systems of cyber attacks in iot environments. *Bulletin of Networking, Computing, Systems, and Software*, 8(2), 93-97.
11. Otoum, Y., & Nayak, A. (2021). As-ids: Anomaly and signature based ids for the internet of things. *Journal of Network and Systems Management*, 29(3), 1-26.
12. Aljawarneh, S., Aldwairi, M., & Yassein, M. B. (2018). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *Journal of Computational Science*, 25, 152-160.
13. Liang, C., Shanmugam, B., Azam, S., Jonkman, M., De Boer, F., & Narayansamy, G. (2019, March). Intrusion detection system for Internet of Things based on a machine learning approach. In *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)* (pp. 1-6). IEEE.
14. Thamilarasu, G., & Chawla, S. (2019). Towards deep-learning-driven intrusion detection for the internet of things. *Sensors*, 19(9), 1977.

15. Zhong, M., Zhou, Y., & Chen, G. (2021). Sequential model based intrusion detection system for IoT servers using deep learning methods. *Sensors*, 21(4), 1113.
16. Chesney, S., Roy, K., & Khorsandroo, S. (2020, September). Machine learning algorithms for preventing IoT cybersecurity attacks. In *Proceedings of SAI Intelligent Systems Conference* (pp. 679-686). Springer, Cham.
17. Samy, A., Yu, H., & Zhang, H. (2020). Fog-based attack detection framework for internet of things using deep learning. *IEEE Access*, 8, 74571-74585.
18. Pecori, R., Tayebi, A., Vannucci, A., & Veltri, L. (2020, July). IoT Attack detection with deep learning analysis. In *2020 International Joint Conference on Neural Networks (IJCNN)* (pp. 1-8). IEEE.
19. Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems*, 82, 761-768.
20. Sriram, S., Vinayakumar, R., Alazab, M., & Soman, K. P. (2020, July). Network flow based IoT botnet attack detection using deep learning. In *IEEE INFOCOM 2020-IEEE conference on computer communications workshops (INFOCOM WKSHPS)* (pp. 189-194). IEEE.
21. Tian, Z., Luo, C., Qiu, J., Du, X., & Guizani, M. (2019). A distributed deep learning system for web attack detection on edge devices. *IEEE Transactions on Industrial Informatics*, 16(3), 1963-1971.
22. Ferrag, M. A., Maglaras, L., Moschogiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50, 102419.
23. Mebawondu, J. O., Alowolodu, O. D., Mebawondu, J. O., & Adetunmbi, A. O. (2020). Network intrusion detection system using supervised learning paradigm. *Scientific African*, 9, e00497.
24. Alladi, T., Agrawal, A., Gera, B., Chamola, V., Sikdar, B., & Guizani, M. (2021, June). Deep neural networks for securing IoT enabled vehicular ad-hoc networks. In *ICC 2021-IEEE International Conference on Communications* (pp. 1-6). IEEE.
25. Liang, W., Huang, W., Long, J., Zhang, K., Li, K. C., & Zhang, D. (2020). Deep reinforcement learning for resource protection and real-time detection in IoT environment. *IEEE Internet of Things Journal*, 7(7), 6392-6401.
26. Miao, Q., Lin, H., Wang, X., & Hassan, M. M. (2021). Federated deep reinforcement learning based secure data sharing for Internet of Things. *Computer Networks*, 197, 108327.