Insight Bulletin: A Multidisciplinary Interlink International Research Journal
Peer Reviewed International, Open Access Journal.
ISSN : 3065-7857 / Website: https://ibrj.us / Volume-3, Issue-5 / May - 2026

Original Article

Enhancing Iot Big Data Analytics in Edge-Cloud Architectures Using Deep Learning Models

Gunnala Soumya[1], M. Jagadeeshwar[2]
[1,2]Chaitanya deemed to be University, Himayatnagar, Hyderabad

Manuscript ID:
IBMIIRJ -2026-030533

Submitted: 15 Apr. 2026
Revised: 25 Apr. 2026
Accepted: 12 May 2026
Published: 31 May 2026

ISSN: 3065-7857
Volume-3
Issue-5
Pp. 168-172
May 2026

Correspondence Address:
Gunnala Soumya
Chaitanya deemed to be University, Himayatnagar, Hyderabad
Email: soumyagunnala.cdu@gmail.com

OPEN ACCESS

Quick Response Code:

Web. https://ibrj.us

DOI: 10.5281/zenodo.21698802

DOI Link:
https://doi.org/10.5281/zenodo.21698802

Abstract

In this study, the authors' deep learning methods can be used to optimize an IoT-based big data analytics architecture in an edge-cloud based computing environment, particularly in the context of anomaly detection. The Internet of Things (IoT) creates a vast amount of data, which poses issues of real-time decision making, congestion, and security. The traditional methods are inadequate because of latency, bandwidth restrictions, and lack of security measures. Using deep learning models, it captures temporal dependency, spatial pattern, and improves classification accuracy thus, detecting anomalies and network attacks in real-time. Moreover, the implementation of edge computing further minimizes the network traffic and processing latency by bringing computation closer to the data points, which enhance efficiency and privacy. The deep learning-based approach not only improves the ability to detect anomalies but also optimizes resource usage, lowers latency, and lowers energy consumption, making it a scalable and secure solution for big data analytics in IoT applications, including smart cities and industrial automation.

Keywords: *IoT, bigdata, anomaly detection, edge computing, security and vulnerabilities.*

Introduction

Internet of Things (IoT) has changed the way things communicate and interact. Through IoT, smart devices can communicate with other devices and the Internet, and be organized, managed and controlled remotely, using unique digital identifiers [2]. This has inspired the development of creative, innovative and intelligent applications like automated health care, self-driving cars, intelligent agriculture, crowd management, and crowdsourcing [3-5]. Moreover, edge computing has emerged as a strategy to move processing towards the edge of the network and the data sources [6]. It enables IoT devices to collect environmental data and facilitates crucial data analysis for implementing smart systems [7], as shown in Figure 1. By bringing computation to the edge of the network, edge computing plays a key role in cutting down on network traffic and latency [8].

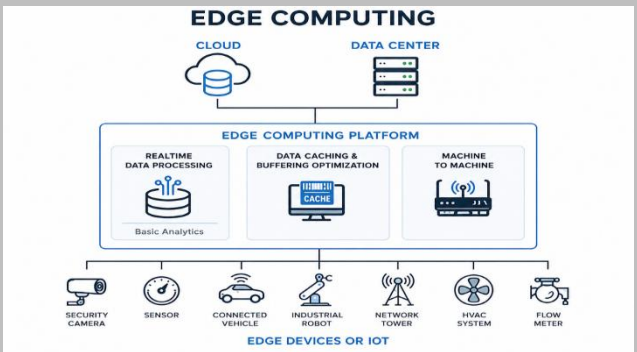

Figure 1. Edge Computing Architecture for IoT devices

How to cite this article:
Soumya, G.& Jagadeeshwar, M. (2026). Enhancing Iot Big Data Analytics in Edge-Cloud Architectures Using Deep Learning Models. Insight Bulletin: A Multidisciplinary Interlink International Research Journal, 3(5), 168–172. https://doi.org/10.5281/zenodo.21698802

Creative Commons

Although these developments are commendable, there are still a number of challenges with IoT-enabled big data analytics, especially regarding edgecloud architectures. These include slow reaction time, high bandwidth costs, high energy costs and poor security [10]. Despite this progress, there are challenges to overcome to implement IoT-based big data analytics, especially in edgecloud computing architectures, due to privacy concerns. These encompass slow reaction times, high bandwidth costs, high energy use and insufficient security [10]. Another privacy issue is that of data being uploaded to the cloud, Solutions that have been adopted to solve these problems include the use of cloud and edge computing. Cloud computing provides a scalable, available and storage option that's perfect for data analytics and Artificial Intelligence (AI) training. But it is high latency and has to be constantly maintained. The scalability and redundancy which cloud systems offer, on the other hand, are lacking in edge computing, which is constrained in processing power and offers less privacy protection [12]. These methods may vary depending on individual use cases and needs. Therefore, the study is focused on incorporating IoT with big data analytics in the edgecloud systems, and proposing the deep learning-based techniques for anomaly detection. Deep Learning is more and more useful for big data analysis due to its capacity to analyse labelled and unlabeled data [13]. It can construct hierarchical representations from lower-level inputs, which allows it to analyze different types of data, such as text, images and videos, effectively [14]. The proposed method would attempt to deal with a large amount of real time data, the problems of many real data sources. The research uses deep learning methods to identify patterns and representations in an IoT Botnet Dataset that is cleaned, aiming to enhance the ability of network attacks and anomaly detection. This study is centered on creating a framework to enhance the utilization of big data analytics through the application of deep learning while taking into account security mechanisms in order to ensure the secure and real-time transmission and processing of data in distributed edge-cloud architectures. Plus, it seeks to reduce latency and energy usage in hybrid cloud and edge setups.

Therefore, the aim of this study is to address the limitations of these conventional approaches and enhance the performance of the IoT big data analytics in edge-cloud system, specifically for the anomaly detection problem using the power of deep learning.

Related Works

With the advent of the Internet of Things (IoT), the possibilities are endless as our society and industrial sectors become smarter and more connected through intelligent IoT technology and automation, as well as real-time data exchange. Initial research work had mainly been centered on smart environments like healthcare, industrial automation, social networking, supply chain management etc., inclusion of IoT technologies in these environments. Evtodieva et al. explored how IoT can enhance intelligent supply chain management, focusing on automation and operational efficiency with connected devices and informed decision-making. Likewise, Baker et al. studied smart healthcare systems based on IoT, which enabled more convenient access to healthcare services and patient management, thanks to the use of wearable sensors and remote monitoring capabilities. These research works highlighted the significance of IoT in the development of intelligent systems, but they also showed that it is difficult to scale up, connect to and communicate with a large number of different devices. As more and more data was generated, researchers started to seek ways to incorporate a big data analytics and machine learning approach to support intelligent decision making and predictive analysis. Piccialli and Jung examined the diffusion of customer experience through big data analytics on social networking services and L'heureux et al. explored the difficulties of machine learning in big data environments. These works highlighted the importance of having advanced analytics tools and methodologies that can handle large and complex datasets coming from IoT systems. Furthermore, Tannahill et al.'s work on the use of big data analytics for system-of-systems engineering highlighted the increasing role of data-driven architectures in large scale distributed systems. While these studies offered valuable insights into the use of intelligent analytics, challenges like high computational complexity, data heterogeneity, and real-time processing limitations persisted. Edge Computing and Fog Computing architectures emerged as efficient alternatives to the centralized cloud computing approach to solve latency and bandwidth limitations issues in IoT systems. The vision and challenges of edge computing were introduced by Shi et al., who pointed out that edge computing has the ability to process data near the end devices for a low-latency application. Ghosh and Grolinger followed this idea by also combining edge-cloud computing with deep learning approaches to IoT data analytics. Roman et al. also carried out an extensive survey of the security threats and challenges in edge and fog computing environments. Overall, the studies have shown that edge computing can help to enhance real-time analytics, alleviate network congestion, and facilitate intelligent IoT applications. But resource limitations, task scheduling, security risks, and effective orchestration of distributed edge nodes remain a challenge in research. MWith the surge in IoT-connected devices and new cyber threats like botnets, anomalies, and distributed denial-of-service (DDoS) attacks, cybersecurity has emerged as one of the most critical concerns in IoT ecosystems. Many researchers suggested anomaly and botnet detection methods with the machine learning and deep learning techniques in IoT networks. Hasan et al. and Ahmad et al. proposed machine learning and deep neural network-based anomaly detection approaches to detect malicious activities in IoT architectures. To detect bots Akash et al. used random forest classifiers along with independent component analysis and Haq, Khan proposed the deep neural network-based botnet classification framework, DNNBoT. Moreover, Kim et al. used recurrent neural networks (RNN) and long short-term memory (LSTM) models for analyzing the features of the IoT botnets, while Ur Rehman et al. proposed the use of GRU based approaches for DDoS attack detection. Many of these techniques had high computational demands, required large training sets and were poor at adapting to changing attack patterns, but some showed good detection accuracy. The research on developing lightweight, intelligent and adaptive security frameworks for resource constrained IoT and edge environment has been an increasing focus recently. Xin et al. suggested deep autoencoder based anomaly detection techniques for IoT traffic classification and Bajao and Sarucam discussed hybrid deep learning, which uses CNN, LSTM and GRU for IoT threat detection. Pektaş and Acarman highlighted the importance of using proper feature selection methods in network flow-based botnet detection for efficient classification performance and minimizing false positive rates. While these sophisticated methods have enhanced the precision of IoT security solutions, there are still numerous challenges, including model explainability, energy efficiency, real-time deployment and scalability. Thus, existing research trends have shown the need for an integrated edge-based intelligent security framework that can provide low latency, adaptive and low energy consumption threat detection in dynamic IoT environments.

Problem Statement

Insufficient exploration regarding the incorporation of state-of-the-art feature selection methodologies to improve the feature engineering phase for IoT botnets detection [15]. Lack of research efforts on developing a hybrid deep learning classifier model for IoT botnets detection to improve the robustness of the system [18]. Lack of comprehensive metrics to evaluate the performance of deep learning models used for IoT botnets detection apart from accuracy [17].

Research Objectives

To design a robust IoT botnet detection framework based on a hybrid deep learning classification algorithm under the edge-cloud computing paradigm. To improve the feature selection phase for botnet detection through PCA and RFE approaches to ensure that only the most important features are selected for analysis.

Methodology

This section outlines the dataset and techniques used in developing a robust IoT botnet detection system using a hybrid deep learning model.

1. **Dataset Description**

The analysis was carried out using the "IoT Botnet Dataset" that has been made public, which consists of rich internet transaction data with multiple features for each transaction. The features consist of unique identification numbers, time stamps, flow state, protocol, source IP and ports, destination IP and ports, number of packets, number of bytes, transaction states, and timing information. In addition, statistics concerning the number of connections by IPs are provided, average rates for each protocol and IP, traffic categories, and classification feature as well as the target variable known as Attack, where 0 means non-malicious and 1 indicates malicious. This comprehensive dataset is mainly applied for training and testing deep learning models to detect intrusions in IoT botnets [20][21].

2. **Technique used**

The techniques employed in the current study in relation to feature extraction, feature selection, and classification are outlined below. These techniques have been selected due to their scalability for handling huge Internet of Things (IoT) botnet datasets and capturing time-series features.

(i) PCA

It is a technique used to transform high-dimensional datasets into fewer dimensions that consist of independent variables. This transformation process maintains much of the variability present in the dataset, capturing its inherent structure. PCA is chosen as a technique for feature selection since it simplifies the IoT botnet dataset by considering only the important features, thus increasing model efficiency and accuracy [22].

(ii) RFE

It is employed for selecting features so that the feature set derived from the PCA is further refined. The backward elimination method removes the least important features repeatedly until the final model uses only the essential features. It ensures that the final model is efficient and effective through RFE as it minimizes overfitting and retains only the impactful features for detecting botnets [23].

(iii) Long Short-Term Memory (LSTM)

The purpose of the LSTM model is to incorporate long-term dependencies into the model since it avoids the issue of the vanishing gradient. The model works because the IoT traffic has dependencies over time, and also the behavior of botnets changes over time. LSTM allows the model to detect these dependencies that enable it to detect attacks [24].

(iv) Gated Recurrent Unit (GRU)

The application of GRU is because it can detect the dependencies that exist over time in the form of sequences within IoT traffic. Botnets normally conduct attacks at different times, and the GRU network can identify the sequence over the various time steps in detecting botnet attacks [25].

(v) CNN

The application of this machine learning method improves the classification process by identifying the spatial patterns and localized features within the input dataset. The use of CNN is especially helpful since it excels in the identification of complicated patterns within the given dataset and hence becomes instrumental in the identification of botnet activities in the internet of things environment [26]. In addition to the advantages offered by the use of LSTM and GRU techniques, CNN provides further strength in terms of extracting the features from the input data. The use of these techniques is justified due to their efficiency in handling the problems associated with IoT botnet detection processes.

Implementations

The methodology begins with the collection of an IoT botnet dataset, which is subjected to a thorough data preprocessing phase. This involves data cleaning to remove any corrupt or irrelevant entries and normalization to scale the features, ensuring that no individual feature dominates the learning process due to its magnitude. Furthermore, missing values are carefully handled, either by imputation or removal, to ensure a complete and consistent dataset for further analysis. After preprocessing, feature extraction is performed using PCA, it ensures that the most informative features are extracted, enhancing the model's ability to learn from the data without being overwhelmed by irrelevant or redundant features. Once feature extraction is complete, the dataset undergoes further feature selection using RFE. It refines the feature set, ensuring that only the highly relevant features are retained for classification. After feature extraction and selection, the dataset is divided into training and testing sets. The classification model used is a hybrid approach combining three powerful Deep Learning methods: LSTM, GRU, and CNN. LSTM is used to handle the classification task, effectively capturing long-term dependencies and patterns within the IoT traffic data. The GRU component is incorporated to capture the temporal dependencies in the IoT traffic data, which is important because botnet behaviour often evolves. The CNN component is utilized to extract spatial patterns and local features from the network traffic data, helping to identify intricate patterns or anomalies within the data that are indicative of botnet activities. Finally, the performance of the employed model is evaluated using appropriate performance analysis metrics to validate

its ability to detect IoT botnet attacks effectively. The combination of these methods ensures a powerful, accurate, and robust botnet detection system that leverages both sequential and spatial data features for enhanced detection accuracy.

Conclusion And Future Scope

This research validates that deep learning can assist in building an effective big data analytics architecture using IoT devices operating in an Edge-Cloud environment, using anomaly detection methods as an example. IoT systems create large amounts of data which results in several problems when it comes to real time processing, network congestion, and security of the data generated. In general, traditional methods are unable to overcome these difficulties caused by latency, limited bandwidth, and/or lack of security. Through the use of various deep learning models, we are able to build a framework that captures temporal dependencies, detects spatial relationships, and improves the accuracy of anomaly classifications, allowing us to detect anomalies and/or network attacks in real time. The addition of using edge computing in this framework will reduce the amount of network traffic and help to reduce the time it takes to process all of the data being generated by moving computation closer to the actual point of data generation, thus increasing overall efficiency and privacy for the systems. Furthermore, applying this deep learning-based framework leads to improvements in detecting anomalies and optimising resource allocation, reducing latency, and decreasing energy consumption, making it a scalable and secure approach for developing big data analytics processes using IoT devices in multiple contexts including smart cities and industrial automation. Future studies may include expanding this framework to larger and more complex IoT networks, updating the types of Neural Networks used on the networks to include advanced architectures such as transformers in order to improve anomaly detection accuracy. Finally, by exploring the use of Federated Learning, more distributed and privacy preserving capabilities will be developed for detecting anomalies within IoT networks. Lastly, optimizing the system for deployment on low-power IoT devices would help make this solution more scalable and energy-efficient for real-world implementations in various industries.

Acknowledgment

The authors sincerely express their gratitude to the management and faculty of Chaitanya Deemed to be University, Hyderabad, for their continuous support, encouragement, and the academic environment that made this research possible. We are thankful to our colleagues and mentors for their valuable suggestions and constructive feedback throughout the course of this work.

Financial support and sponsorship

Nil.

Conflicts of interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. Evtodieva, T. E., D. V. Chernova, N. V. Ivanova, and J. Wirth. "The internet of things: possibilities of application in intelligent supply chain management." Digital transformation of the economy: Challenges, trends and new opportunities (2019): 395-403.
2. Piccialli, Francesco, and Jai E. Jung. "Understanding customer experience diffusion on social networking services by big data analytics." Mobile Networks and Applications 22 (2017): 605-612.
3. Baker, Stephanie B., Wei Xiang, and Ian Atkinson. "Internet of things for smart healthcare: Technologies, challenges, and opportunities." Ieee Access 5 (2017): 26521-26544.
4. Babar, Muhammad, Fazlullah Khan, Waseem Iqbal, Abid Yahya, Fahim Arif, Zhiyuan Tan, and Joseph M. Chuma. "A secured data management scheme for smart societies in industrial internet of things environment." IEEE Access 6 (2018): 43088-43099.
5. Lashkari, Bahareh, Javad Rezazadeh, Reza Farahbakhsh, and Kumbesan Sandrasegaran. "Crowdsourcing and sensing for indoor localization in IoT: A review." IEEE Sensors Journal 19, no. 7 (2018): 2408-2434.
6. Ghosh, Ananda Mohon, and Katarina Grolinger. "Edge-cloud computing for Internet of Things data analytics: Embedding intelligence in the edge with deep learning." IEEE Transactions on Industrial Informatics 17, no. 3 (2020): 2191-2200.
7. L'heureux, Alexandra, Katarina Grolinger, Hany F. Elyamany, and Miriam AM Capretz. "Machine learning with big data: Challenges and approaches." Ieee Access 5 (2017): 7776-7797. [8] Roman, Rodrigo, Javier Lopez, and Masahiro Mambo. "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges." Future Generation Computer Systems 78 (2018): 680-698.
8. https://www.spiceworks.com/tech/cloud/articles/edge-vs-cloud-computing/
9. Mitra, Anuran, Soumita Biswas, Tinku Adhikari, Arindam Ghosh, Soumalya De, and Raja Karmakar. "Emergence of edge computing: An advancement over cloud and fog." In 2020 11th International Conference on Computing, Communication and Networking Technologies (ICT), pp. 1-7. IEEE, 2020
10. Satyanarayanan, Mahadev, Guenter Klas, Marco Silva, and Simone Mangiante. "The seminal role of edge-native applications." In 2019 IEEE International Conference on Edge Computing (EDGE), pp. 33- 40. IEEE, 2019.
11. Shi, Weisong, Jie Cao, Quan Zhang, Youhuizi Li, and Lanyu Xu. "Edge computing: Vision and challenges." IEEE internet of things journal 3, no. 5 (2016): 637-646.
12. Ravi, Daniele, Charence Wong, Benny Lo, and Guang-Zhong Yang. "A deep learning approach to onnode sensor data analytics for mobile or wearable devices."
13. Tannahill, Barnabas K., Chris E. Maute, Yunus Yetis, Maryam N. Ezell, Aldo Jaimes, Roberto Rosas, Azima Motaghi, Halid Kaplan, and Mo Jamshidi. "Modeling of system of systems via data analytics— Case for "Big Data" in SoS." In 2013 8th International Conference on System of Systems Engineering, pp. 177-183. IEEE, 2013.
14. Xin, Qi, Zeqiu Xu, Linfeng Guo, Fanyi Zhao, and Binbin Wu. "IoT traffic classification and anomaly detection method based on deep autoencoders." (2024).

15. Akash, Nazmus Sakib, Shakir Rouf, Sigma Jahan, Amlan Chowdhury, and Jia Uddin. "Botnet detection in IoT devices using random forest classifier with independent component analysis." Journal of Information and Communication Technology 21, no. 2 (2022): 201-232. [17] Ahmad, Zeeshan, Adnan Shahid Khan, Kashif Nisar, Iram Haider, Rosilah Hassan, Muhammad Reazul Haque, Seleviawati Tarmizi, and Joel JPC Rodrigues. "Anomaly detection using deep neural network for IoT architecture." Applied Sciences 11, no. 15 (2021): 7050.
16. Hussain, Faisal, Syed Ghazanfar Abbas, Ubaid U. Fayyaz, Ghalib A. Shah, Abdullah Toqeer, and Ahmad Ali. "Towards universal features set for IoT botnet attacks detection." In 2020 IEEE 23rd international multitopic conference (INMIC), pp. 1-6. IEEE, 2020.
17. Hasan, Mahmudul, Md Milon Islam, Md Ishrak Islam Zarif, and M. M. A. Hashem. "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches." Internet of Things 7 (2019): 100059.
18. Ullah, Imtiaz, and Qusay H. Mahmoud. "A technique for generating a botnet dataset for anomalous activity detection in IoT networks." In 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 134-140. IEEE, 2020. [
19. https://sites.google.com/view/iotbotnetdatset/home
20. Haq, Mohd Anul, and Mohd Abdul Rahim Khan. "DNNBoT: Deep neural network-based botnet detection and classification." Computers, Materials & Continua 71, no. 1 (2022).
21. Pektaş, Abdurrahman, and T. Acarman. "Effective feature selection for botnet detection based on network flow analysis." In International Conference Automatics and Informatics, pp. 1-4. 2017.
22. Kim, Jiyeon, Hyerin Won, Minsun Shim, Seungah Hong, and Eunjung Choi. "Feature analysis of iot botnet attacks based on RNN and LSTM." Int J Eng Trends Technol 68, no. 4 (2020): 43-47.
23. Ur Rehman, Saif, Mubashir Khaliq, Syed Ibrahim Imtiaz, Aamir Rasool, Muhammad Shafiq, Abdul Rehman Javed, Zunera Jalil, and Ali Kashif Bashir. "DIDDOS: An approach for detection and identification of Distributed Denial of Service (DDoS) cyberattacks using Gated Recurrent Units (GRU)." Future Generation Computer Systems 118 (2021): 453-466.
24. Bajao, Naomi A., and Jae-an Sarucam. "Threats Detection in the Internet of Things Using Convolutional neural networks, long short-term memory, and gated recurrent units." Mesopotamian journal of cybersecurity 2023 (2023): 22-29.