Journal of Information Systems Engineering and Management
2025, 10(6s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

IoT Network Security Anomaly Detection and Classification using Deep Learning

Dr. Karthik Meduri[1], Dr. Steven Brown[2], Dr. Geeta Sandeep Nadella[3*], Dr. Hari Gonaygunta[4], Dr. Snehal Satish[5], Mohan Harish Maturi[6]

[1,3,4,5,6] Independent Researcher, [2] Professor.

[1,2,3,4,5,6] Dept of Information Technology, University of the Cumberlands, Williamsburg, KY, USA.

Email: [1]karthik.meduri@ieee.org, [2]steven.brown@ucumberlands.edu, [3]geeta.s.nadella@ieee.org, [4]hari.gonaygunta@ieee.org, [5]snehal.satish@ieee.org, [6]mohan.maturi@ieee.org

Orchid Id number: [1]0009-0007-6056-7577, [2]0009-0003-9703-4177, [3]0000-0001-7126-5186, [4]0009-0003-3360-154X, [5]0009-0005-5494-8467, [6]0009-0003-3335-7516

Corresponding Author: Geeta Sandeep Nadella, email: geeta.s.nadella@ieee.org*

ARTICLE INFO

Received: 08 Oct 2024

Revised: 10 Dec 2024

Accepted: 24 Dec 2024

ABSTRACT

The Internet of Things (IoT) is an expanding network of interconnected devices exposed to growing cyber security threats. Integrating AI-powered solutions presents a promising avenue for enhancing anomaly detection and classification. This study delves into developing a comprehensive methodology leveraging machine learning and deep learning techniques. Utilizing the BoTNeTIoT-L01 dataset, meticulously curated from IoT devices, the research focuses on data gathering, preprocessing, and exploratory data analysis to unearth underlying patterns and anomalies within network traffic data. Subsequently, a suite of machine learning models, including Logistic Regression, LightGBM (Light Gradient-Boosting Machine), and Decision Tree, along with a deep learning model optimized with the Adam optimizer, is employed to detect and classify anomalies effectively. The comparative analysis underscores the superior performance of advanced models such as LightGBM and Decision Tree, showcasing their efficacy in accurately identifying security threats within IoT environments. The study also addresses pertinent technical challenges, ethical considerations, and future directions, emphasizing the imperative for responsible deployment and ongoing innovation in AI-powered IoT security solutions.

Keywords: IoT Security, Anomaly Detection, Machine Learning, Deep Learning, Light Gradient-Boosting Machine (LightGBM)

INTRODUCTION:

IoT systems play vital roles in smart homes, healthcare, manufacturing, and many other industries. Ensuring strong security mechanisms for these systems remains a critical challenge. Despite its many advantages, IoT devices' interconnected nature and large amounts of data generation are susceptible to innumerable security threats, including irregularities and malicious attacks. This research presents a solution to address these challenges by improving anomaly detection capabilities through advanced AI models [1]. By detecting entry from the expected behavior of devices connected to the Internet of Things, a system that detects disruption provides an essential line of protection from potential attacks [2]. It is essential to ensure robust safety
measures for the rapidly altering Internet Things world to protect sensitive data, critical systems, and user privacy. IoT devices are becoming increasingly networked as they span fields ranging from smart homes to automated manufacturing, generating large amounts of data. This relationship also reveals several security threats to the IoT ecosystem, including malicious attacks, unauthorized access, and data breaches [3]. AI techniques are used with more advanced methods, providing a basic level of security surveillance and complementing the capabilities of sophisticated AI-based random detection systems. As technology advances and the complexity of datasets increases, there is a growing need to expand traditional methods to more consistent and intelligent random detection methods to effectively deal with the changing landscape of security threats [4].

IoT settings are ever-changing, and diverse structures are often too firm to work with traditional security technologies, requiring more advanced and flexible solutions [5]. In the digital age, artificial intelligence (AI) is a viable way to instantly improve anomalous event detection systems with sophisticated algorithms to detect deviations from abnormal behavior in complex data samples. With AI models such as deep learning, machine learning, and reinforcement learning, we can build security systems and multi-layered systems for breach detection that can successfully mitigate security issues in IoT facilities. In order to improve the quality and resilience of IoT systems to new cyber threats, we will discuss the possible artificial technology to enhance the detection of IoT security anomalies. Current IoT security disturbance detection systems, as shown in Fig. 1, face significant challenges in effectively identifying and mitigating emerging threats within dynamic and diverse IoT environments [6]. Traditional rules-based methods lack the adaptability and scalability needed to keep up with evolving attack vectors and the activities of various IoT devices. There is a need to improve systems that detect disruptions in IoT security using advanced artificial Intelligence (AI) models [7].

To achieve the highest accuracy score, compare the models to check which model performs well. Design the proposed framework for anomaly detection systems to enhance the scalability and adaptability of IoT systems [8].

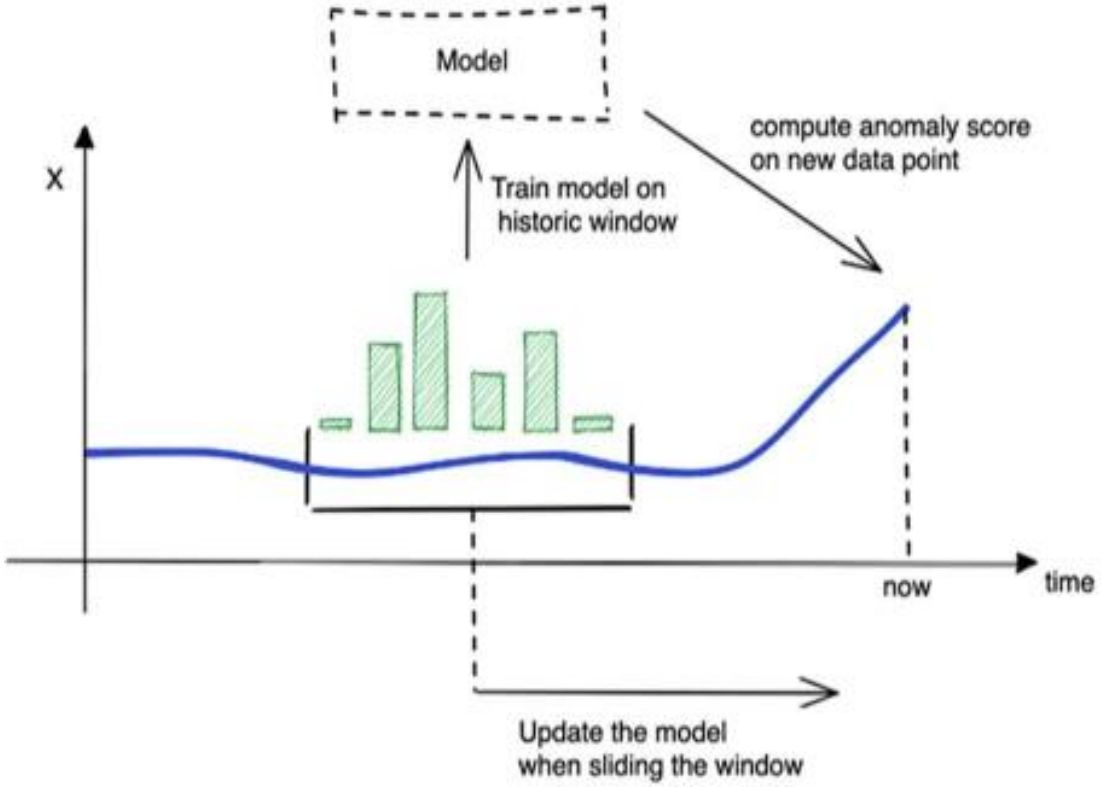

Fig. 1. AI-Based IoT Anomaly Detection with Sliding Windows [8]

Recently, studies have focused on using cutting-edge AI technologies to improve IoT abnormality detection capabilities [9]. Using technology within traditional rule-based methods often leads to difficulties in adapting to IoT settings' changing and diverse landscapes. The promise of better accuracy, continuous tracking, scalability, and agility from AI-based disturbance detection solutions will enhance the public safety image of IoT facilities [10].

An important area of study in IoT security is the detection of disruptions aimed at enhancing the resistance of IoT ecosystems to new cyberattacks [11]. There is a need to detect and reduce distortions for security devices in many fields, including industrial automation and smart homes. In addition, ongoing research efforts seek to address issues such as the flexibility of AI models to exploit the enemy and sensitivity to complex attacks [12]. In an increasingly connected world, academics are working to preserve the sanctity of critical facilities by reducing security threats, protecting vital information, and pushing the boundaries of disinformation detection methods designed specifically for IoT security [13]. Scientists discovered ways to integrate different IoT source data and obtain relevant features for unusual identification. Generating raw sensor information, selecting useful features, and integrating data from multiple sources is essential to comprehensively understanding IoT network activity [14]. Because learning

algorithms without monitoring can find trends and distortions in data that are not hierarchical, they have attracted attention to detecting irregularities in IoT security. Methods, including assemblies and automated encoders, were examined without classified training data to identify deviations from normal behavior [15].

In general, attempts to identify the disorder use analytical or rule-based techniques to find irregularities in the system's regular behavior. These methods are often applied in many areas, such as industrial monitoring, finance, and network security [16]. In order to identify observations or events that deviate from estimated limits, one of the basic techniques is to create standards or rules based on predetermined criteria, including statistical variables or expert experience. Traditional disturbance detection techniques, for example, network security, often involve tracking the flow of network traffic and finding abnormalities based on the breach from expected behavior. This may include finding unusual interactions, abnormally high data transfer rates, or strange attempts to access network resources [17,18].

Differences in factory tracking systems can be detected by comparing sensor readings with previous data or predetermined thresholds to find differences indicative of potential process malfunction or equipment failure. Statistical modeling is another standard traditional method for detecting irregularities [19]. In this method, the system's primary distribution is represented by using mathematical equations. Finding a pattern in the data and highlighting the separation from the estimated standards may involve aggregation algorithms, time series analysis, or distribution modeling. Statistical models, for example, can be used to examine business data in financial control to detect irregularities or strange spending habits that may indicate fraud [20].

Intelligent attackers can use stealing strategies to undermine rules-based error detection systems [21]. By manipulating input or using established standards or standards to hide hazardous activities, attackers can undermine the effectiveness of existing diagnostic measures. While standard rule-based practices are easy to implement, they often fail to maintain the changing and diverse nature of the IoT context. They rely on flexible standards or rules that may not adequately reflect the diversity of IoT conduct or changing opposing strategies [22]. These methods can create heavy security teams with false positive notifications that may be unrelated to actual security incidents [23,24]. The limited adoption of legacy technologies contributes to delays in recognizing system limitations and violations, especially as IoT installations grow in size and complexity [25].

2) METHODS AND METHODOLOGY:

In the methodology for advancing IoT network security detection and classification with machine learning and deep learning models, we get the secondary dataset IDS-IoT data to analyze, detect, and classify anomalies. As shown in Fig. 2, we first implement step data collection. The second is preprocessing the data and then preparing the data to employ feature selections and targets and also transform the data into training and testing to apply the machine learning models (Logistic Regression, lightGBM, Decision Tree) and in which Deep learning to use the Adam_Optimizer model to detect and classify their anomalies the proposed diagram is given below:

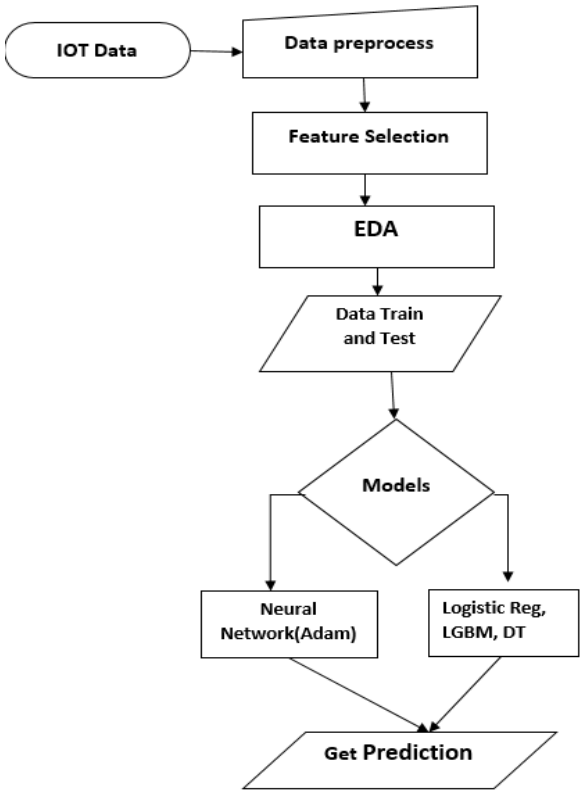

Fig. 2. Proposed Framework AI-based Models [20]

A. Data Gathering

The first step of this research analysis is data gathering. We used quantitative data from the data repertory site. The BoTNeT, IoT-L01 dataset was meticulously collected by sniffing network traffic from nine IoT devices in a local network setup using a central switch. The data capture was performed using Wireshark, focusing on two types of Botnet attacks, Mirai and Gafgyt. The dataset features were engineered statistically, with a 10-second time window and a decay factor of 0.1 to reduce redundancy. Twenty-three features were derived, including packet count, jitter, and sizes of outbound and inbound packets, calculated with mean, variance, and covariance measures. This comprehensive data collection and feature extraction process aimed to facilitate the accurate detection of IoT Botnet attacks. Many researchers use this data set to test and train the models for enhancing the efficacy of network and IOT cyber threat attacks [26].

B. Exploratory Data Analysis

Exploratory-Data-Analyses is a vital step in data analysis. We examine and visualize the dataset to uncover patterns, spot anomalies, test hypotheses, and check assumptions using summary statistics and graphical representations. In the BoTNeT, IoT-L01 data context, EDA thoroughly examines the twenty-three features derived from network traffic data, including packet count, jitter, and sizes of outbound and inbound packets. We use statistical measures such as mean, variance, and covariance to understand the distribution and relationships between these feature variables. Visualization tools such as histograms, box plots, and scatter plots help identify trends and outliers. For instance, visualizing the distribution of packet counts can reveal normal traffic patterns and deviations indicative of potential anomalies.

C. Implementation of ML and DL Models

Figure 2 represents the proposed framework of this research to detect the anomalies in the IOT system with the Artificial Intelligence model using the machine learning technique and predict the anomalies in IoT security systems [27].

1. **Logistic-Regression-Model:** remains a statistical model castoff for binary classification complications. It predicts the probability of the outcome that a given input belongs to a certain class.

Formula: The logistics-regression model relates the logistic (sigmoid) functions to the linear combinations of inputs-features:

$$\sigma(z) = \frac{1}{1 + e^{-z}}$$

Where $z = \beta_0 + \beta_1 x_1 + \cdots + \beta_n x_n$

Here:

- $\sigma(z)\sigma(z)$ is the predicted probability of the class.
- $\beta 0\beta 0$ is intercepting.
- $\beta 1,\beta 2,\ldots,\beta n\beta 1,\beta 2,\ldots,\beta n$ stay co-efficients of these features $x1,x2,\ldots,xnx1,x2,\ldots,xn$.
- In IoT network security, logistic regression can be used to classify network activities using normal and abnormal features created from network traffic data.

2. **Light-GBM** is a gradient-boost framework that uses tree-based learning procedures. It builds an ensemble of decision trees sequentially, where each tree tries to correct the errors of the previous ones.

Key Features:

- Histogram-based: LightGBM uses histograms for continuous features to speed up training.
- Leaf-wise growth**:** Trees are grown leaf-wise rather than level-wise, which can result in more complex trees and better accuracy.

Formula: The objective function minimized in LightGBM combines a loss function (e.g., mean squared error for regression) and regularization terms:

$$Obj = \Sigma^n l(y_i, \hat{y}_i) + \Omega(f)$$

Where:

- $l(yi,y\hat{}i)l(yi,y\hat{}i)$ is the loss function measuring the difference between actual and predicted values.
- $\Omega(f)\Omega(f)$ is the regularization term to prevent overfitting.

LightGBM can be used to build robust models for detecting anomalies in IoT networks by learning patterns in the data that differentiate normal behavior from anomalies [28].

3. **Decision Tree:** is a tree-like model used for classification and regression. The separation of data into sub-sets created arranged the feature values, making decisions at each node to reach a final prediction at the leaf nodes.

Formula: Decision trees use impurity measures like Gini impurity or entropy for classification tasks:

$$Gini = 1 - \sum_{i=1}^{n} p_i^2$$

$$Entropy = -\sum_{i=1}^{n} p_i \log_2(p_i)$$

Where pi is the probability of a specific class at a node.

4. **Adams-Optimizer-Model:** An approach for first-order equations gradient-based optimization of stochastic objective functions is the Adam (Adaptive Moment Estimation) optimizer [29]. The method calculates the adaptive learning rates for every parameter by merging the benefits of two additional random gradient descent expansions: AdaGrad and RMSProp.

Formulas**:** Adam updates the parameters using:

Gradient (g_t): Computed from the objective function

Exponential moving average of the gradient
(m_t): $m_t = \beta_1 m_{t-1} + (1 - \beta_1) g_t$

Exponential moving average of the squared gradient
(v_t): $v_t = \beta_2 v_{t-1} + (1-\beta_2) g_t^2$

Bias correction:
$m\hat{}_t = \frac{m_t}{1-\beta_1^t}, \qquad v_t = \frac{v_t}{1-\beta_2^t}$

Parameter update:

$$\theta_t = \theta_{t-1} - \alpha \frac{m_t}{\sqrt{v_t} + \epsilon}$$

DATA ANALYSIS AND RESULTS

The last section is based on the evaluation process of anomaly detection for security systems. This evaluation discussed and visualized the performance and effectiveness of both models used for the analysis [30]. It also displayed the metrics to identify normal and anomalies in the IoT system, to give these metrics [31]. We cover the accuracy score, precisions, recalls, and f1-scores of both models' performance and compare them to check which model gives the highest accuracy score. Further analysis and argument are given below:

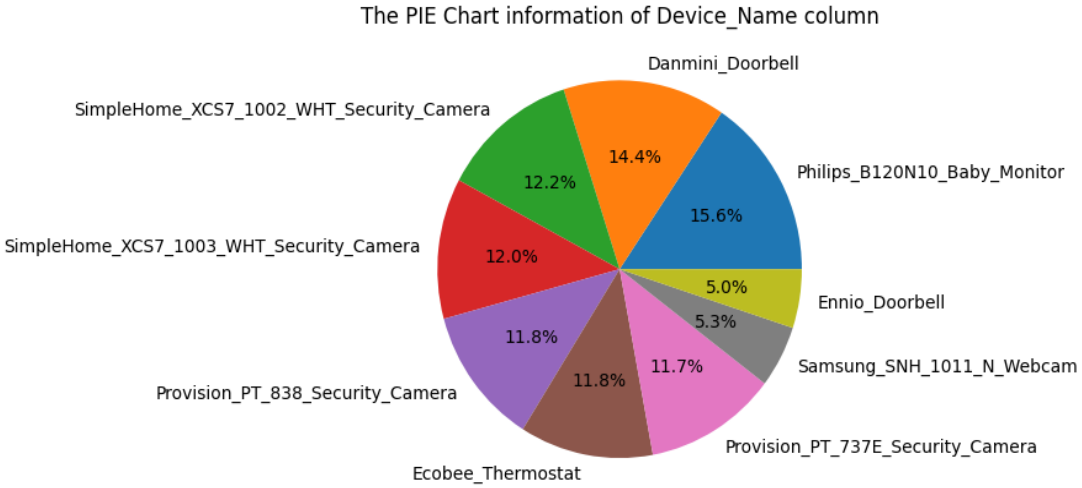

Fig. 3. IOT Devices name PIE-Chart

The above Fig. 3. shows the pie chart for darn mini doorbells 14%.6, Phillips baby monitor 15.6%, samsang webcam 5.6%, ecobee thermostate 11.8%, and provision security camera 12.0%.

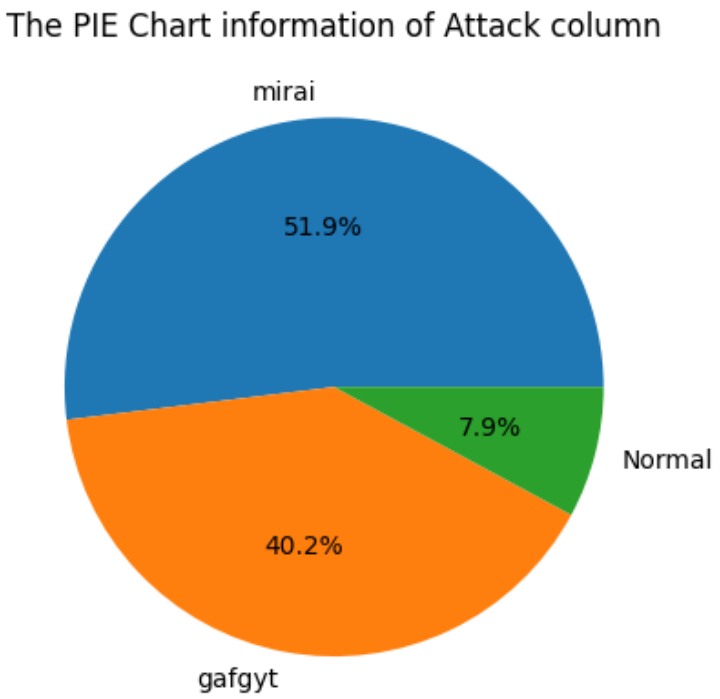

Fig. 4. Attack distribution plot

In the above Fig. 4. represents the attack columns in our dataset, which show three main types of attacks in IOT devices' security systems. The first is Mirai 51.9% Normal 7.9%, and Gafgyt 40.2% are attacks in IOT systems.

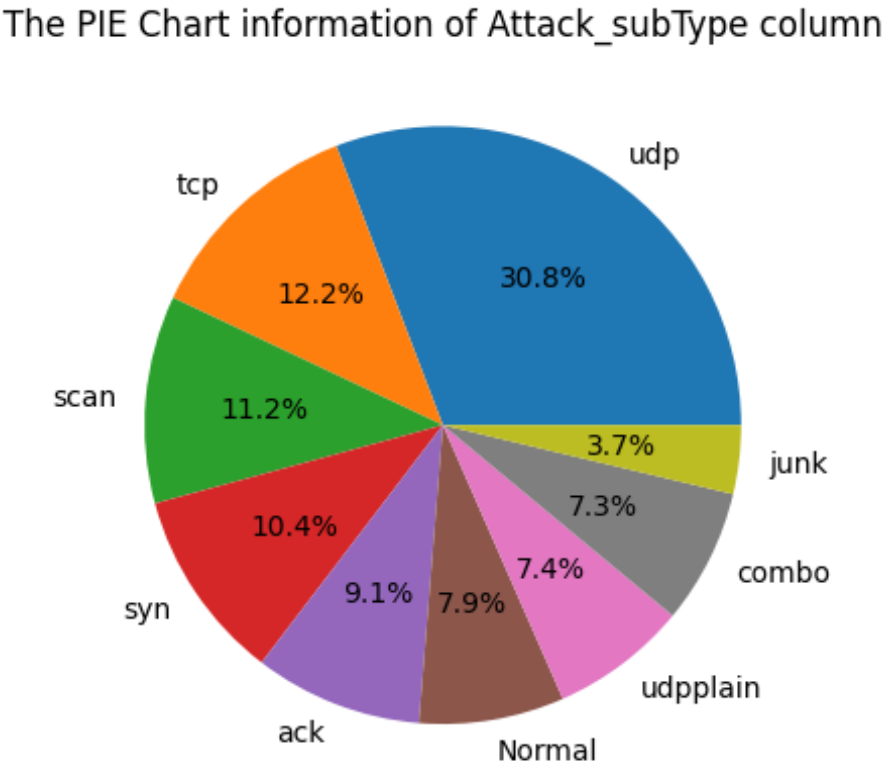

Fig. 5. Attacks sub-types distribution.

In this pie chart, as shown in Fig. 5., distributed the subtypes of attacks that have a high impact on IoT and

security networks are very harmful attacks; there are nine sub-categories in which the high ratio is UDP at 30.8%, and TCP is 12.2 scan at 11.2%, the lowest is ranges. There are some other security protocols with their detected anomalies re-classified in values given below the table 1.

Table 1 Protocol Anomalies rates

Protocol	Anomaly Rate
IPv	0.064630
LLC	0.064630
UDP	0.042208
TCP	0.016977
HTTPS	0.008872
ICMP	0.002002
HTTP	0.000777
DNS	0.000040
SSH	0.000015
ARP	0.000011
Telnet	0.000000
SMTP	0.000000
IRC	0.000000
DHCP	0.000000

MODEL RESULTS COMPARISON

The evaluation of the machine learning and deep learning models applied to the IDS-IoT dataset involved a detailed comparison of their performance in detecting and classifying anomalies within IoT network security. Key performance metrics such as accuracy, precision, recall, and F1-score were computed for each model. Logistic regression demonstrated reliable classification capabilities with good interpretability, making it suitable for straightforward anomaly detection tasks. LightGBM, with its gradient boosting framework, showed superior performance in handling complex patterns and provided higher accuracy and robustness against overfitting compared to other models. While intuitive and easy to visualize, the Decision Tree model outperformed LightGBM's accuracy and precision but provided useful insights through its hierarchical decision-making structure. The deep learning model, optimized using the Adam optimizer, excelled in learning intricate patterns from the dataset.

Table 2 Deep Learning Model Adam-optimizer

Epoch	Loss	Accuracy
1	0.5817	0.6965
5	0.1930	0.9195
10	0.1870	0.9206
15	0.4010	0.8303
20	0.0577	0.9843
25	0.0773	0.9792
30	0.5207	0.6938
35	0.2068	0.9277
40	0.2092	0.9265
45	0.2078	0.9276
50	0.2079	0.9270

Table 3 Models Accuracy Score Comparison

Model	Accuracy Score
Logistic Regression	0.728
LightGBM	0.999
Decision Tree	0.999
Deep Learning (Adam-optimizer)	0.999

The results presented in Table 2 showcase the performance of the Deep Learning model trained with the Adam optimizer over multiple epochs. Initially, the model's loss is relatively high at epoch 1, indicating its uncertainty and lack of accuracy. However, the loss and accuracy metrics significantly improve as the training progresses through subsequent epochs. By epoch 20, the loss diminishes to a minimal value. At the same time, the accuracy climbs to nearly 98.43%, indicating the model's ability to learn complex patterns and make accurate predictions. Although there are fluctuations in performance throughout training, the overall trend showcases a remarkable increase in accuracy over time [32].

Table 3 compares the accuracy scores of various models, including Logistic Regression, LightGBM, Decision Tree, and the Deep Learning model with the Adam optimizer. Logistic regression exhibits the lowest accuracy score at 0.728, while LightGBM, Decision Tree, and the Deep Learning model achieve high accuracy scores of 0.999. These results suggest that advanced machine learning models, particularly LightGBM and Decision Tree, along with the Deep Learning model trained with the Adam optimizer, excel in accurately detecting anomalies in IoT network security data, outperforming traditional logistic regression methods.

CHALLENGES AND FUTURE SCOPE

A. Technical Challenges

One of the main technical experiments in AI data-driven IoT-security falsehoods in safeguarding the quality and sufficiency of data with the intricate nature of IoT networks and the diverse range of devices involved, obtaining comprehensive and clean datasets remains a significant hurdle. The enormous amount of data produced by Internet of Things devices presents difficulties in processing, storing, and analyzing.

As AI models become increasingly sophisticated, ensuring their interpretability and transparency becomes paramount. Understanding how models arrive at their decisions is crucial for trust and accountability in IoT security. However, complex models such as deep learning algorithms often lack interpretability, posing challenges in explaining their outputs and making them less accessible to stakeholders.

B. Ethical Privacy Concerns

With the proliferation of IoT strategies for collecting massive quantities of data, anxieties surrounding information privacy and user consent have become more pronounced. Collecting, storing, and analyzing sensitive data without consent can infringe upon users' privacy rights. Ensuring compliance with data protection regulations and obtaining explicit user consent for data collection and processing is essential to address these ethical concerns.

The use of AI in IoT security raises ethical considerations regarding bias, fairness, and unintended consequences. Biased training data or algorithmic decisions can lead to discriminatory outcomes, exacerbating existing social inequalities. Moreover, deploying AI-driven security measures must consider the potential for unintended consequences, such as false positives or reliance on inaccurate predictions, which could undermine trust and result in real-world harm.

CONCLUSION

To conclude, this research in the methodology outlined for advancing IoT network security through machine learning and deep learning models presents a comprehensive approach to detecting and classifying anomalies within IoT environments. Researchers gain insights into the underlying patterns and anomalies in network traffic data through meticulous data collection, preprocessing, and exploratory data analysis. Implementing machine learning models such as Logistic Regression, LightGBM, and Decision Tree, along with the Adam optimizer in deep learning, demonstrates the effectiveness of advanced techniques in accurately identifying security threats. The comparison of model performance highlights the superior accuracy and robustness of LightGBM, Decision Tree, and the Deep Learning model, emphasizing their potential for enhancing IoT security. However, the research also identifies various challenges and ethical considerations, including data quality issues, interpretability of models, and privacy concerns, which must be identified to certify answerable besides principled deployment of AI-driven security solutions in IoT ecosystems. Future research directions should address these tasks while discovering emerging technologies and methodologies further to enhance the resilience and effectiveness of IoT security systems.

ACKNOWLEDGMENT

We would like to thank our professors at the University of the Cumberlands for guiding us in many ways. All authors contributed equally to this work and were involved in the conception and design of the study, data acquisition, analysis, and interpretation. All authors were involved in drafting and revising the manuscript and have approved the final version.

FUNDING STATEMENT

The authors received no financial support for the research, authorship and/or publication of this article.

CONFLICT OF INTEREST

The authors declared no potential conflicts of interest with respect to the research, funding, authorship and/or publication of this article.

REFERENCES

[1] Boultwood, R. Collins, M.C. Conroy, and N. Crabtree, "The UK Biobank imaging enhancement of 100,000 participants: rationale, data collection, management and future directions," Nature Communications, vol. 11, no. 1, p. 2624, 2020. doi: 10.1038/s41467- 020-16474-y

[2] Castiglioni, L. Rundo, M. Codari, G. Di Leo, C. Salvatore, M. Interlenghi, F. Gallivanone, A. Cozzi, N.C. D'Amico, and F. Sardanelli, "AI applications to medical images: From machine learning to deep learning," Physica Medica, vol. 83, pp. 9-24, 2021. doi: 10.1016/j.ejmp.2021.08.004

[3] A.P. Cheema, B. Khokher, N. Jha, and N. Verma, "Animal Detection for Farmlands using Image Processing and IoT," in 2023 International Conference on Computer Communication and Informatics (ICCCI), pp. 1-6, IEEE, January 2023. doi: 10.1109/ICCCI53676.2023.9618913

[4] S. Chauhan et al., "SEX DISPARITY IN TRANSPLANTATION INDIA: THE PROBLEM STATEMENT!," Transplantation, vol. 104, no. S3, p. S469, 2020. doi: 10.1097/01.tp.0000697634.73232.32

[5] S. Chauhan, V. Kute, H. Patel, D. Engineer, P. Shah, S. Banerjee, P. Modi, H. Shankar, S. Desai, R. Chauhan, and S. Chauhan, "SEX DISPARITY IN TRANSPLANTATION IN INDIA: THE PROBLEM STATEMENT!," Transplantation, vol. 104, no. S3, p. S469, 2020. doi: 10.1097/01.tp.0000697634.73232.32

[6] D.S. Civitarese, J. Schmude, J. Jakubik, A. Jones, N. Nguyen, C. Phillips, S. Roy, S. Singh, C. Watson, and R. Ganti, "AI foundation models for weather and climate: Applications, design, and implementation," arXiv preprint arXiv:2309.10808, 2023. doi: 10.1109/IC3I53511.2022.9684963

[7] J.P. Cohen, P. Morrison, L. Dao, K. Roth, T.Q. Duong, and M. Ghassemi, "Covid-19 image data collection: Prospective predictions are the future," arXiv preprint arXiv:2006.11988, 2020. doi: 10.1101/2020.06.10.20127876

[8] M.B. Coomans, M.C. Peeters, J.A. Koekkoek, J.W. Schoones, J. Reijneveld, M.J. Taphoorn, and L. Dirven, "Research objectives, statistical analyses and interpretation of health-related quality of life data in glioma research: a systematic review," Cancers, vol. 12, no. 12, p. 3502, 2020. doi: 10.3390/cancers12123502

[9] L.M. D'Arrietta, V.N. Vangaveti, M.J. Crowe, and B.S. Malau-Aduli, "Rethinking health professionals' motivation to do research: a systematic review," Journal of Multidisciplinary Healthcare, pp. 185- 216, 2022. doi: 10.2147/JMDH.S343542

[10] L. Dewangan and AR Vaishnava, "Energy-efficient smart wearable IoT device for the application of collapse motion detection and alert," IETE Journal of Research, vol. 69, no. 2, pp. 1133-1139, 2023. doi: 10.1080/03772063.2021.1896571

[11] SK Dhir and P. Gupta, "Formulation of the research question and composing study outcomes and objectives," Indian Pediatrics, vol. 58, pp. 584-588, 2021. doi: 10.1007/s13312-021-2284-6

[12] MK DiBenedetto, "Motivation and social cognitive theory," Contemporary educational psychology, vol. 60, p. 101832, 2020. doi: 10.1016/j.cedpsych.2020.101832

[13] Z. Dörnyei and E. Ushioda, "Teaching and researching motivation,"Routledge, 2021. doi: 10.4324/9781315763296

[14] M. Douiba, S. Benkirane, A. Guezzaz, and M. Azrour, "An improved anomaly detection model for IoT security using decision tree and gradient,"

[15] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM computing surveys (CSUR), vol. 41, no. 3, pp. 1-58, 2009. doi: 10.1145/1541880.1541882.

[16] R. Chalapathy and S. Chawla, "Deep learning for anomaly detection: A survey," arXiv preprint arXiv:1901.03407, 2019. doi: 10.1145/3282309.3282312.
[17] Y. Otoum, D. Liu, and A. Nayak, "DL-IDS: a deep learning–based intrusion detection framework for securing IoT," Transactions on Emerging Telecommunications Technologies, Nov. 2019, doi.org/10.1002/ett.3803.
[18] M. Alsoufi, S. Razak, M. Siraj, I. Nafea, F. Ghaleb, F. Saeedet al., "Anomaly-based intrusion detection systems in IoT using deep learning.
[19] Z. Ahmad, A. Shahid Khan, K. Nisar, I. Haider, R. Hassan, M.R. Haque, S. Tarmizi, and J.J. Rodrigues, "Anomaly-based intrusion detection systems in IoT using deep learning: A systematic literature review," Applied Sciences, vol. 11, no. 18, p. 8383, 2021. doi: 10.3390/app11188383.
[20] M.K. Alam, "A systematic qualitative case study: questions, data collection, NVivo analysis and saturation," Qualitative Research in Organizations and Management: An International Journal, vol. 16, no. 1, pp. 1-31, 2021. doi: 10.1108/QROM-09-2020-1964.
[21] B.R. Albuquerque, S.A. Heleno, M.B.P. Oliveira, L. Barros, and I.C. Ferreira, "Phenolic compounds: Current industrial applications, limitations and future challenges," Food & Function, vol. 12, no. 1, pp. 14-29, 2021. doi: 10.1039/D0FO01947G.
[22] M.A. Alsoufi, S. Razak, M.M. Siraj, I. Nafea, F.A. Ghaleb, F. Saeed, and M. Nasser, "Anomaly-based intrusion detection systems in IoT using deep learning: A systematic literature review," Applied Sciences, vol. 11, no. 18, p. 8383, 2021. doi: 10.3390/app11188383
[23] L. Aversano, M.L. Bernardi, M. Cimitile, R. Pecori, and L. Veltri, "Effective anomaly detection using deep learning in IoT systems," Wireless Communications and Mobile Computing, vol. 2021, pp. 1-14, 2021. doi: 10.1155/2021/8895392.
[24] V. Bansal, S. Pandey, S.K. Shukla, D. Singh, S.A. Rathod, and J.L.A. Gonzáles, "A framework of security attacks, issues classifications and configuration strategy for IoT networks for the successful implementation," in 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), pp. 1336-1339,
[25] E. Bazgir, E. Haque, N.B. Sharif, and M.F. Ahmed, "Security aspects in IoT based cloud computing," World Journal of Advanced Research" IEEE, December 2022. doi: 10.1109/IC3I53511.2022.9684963.
[26] S. ALAmri, F. ALAbri, and T. Sharma, "Artificial Intelligence Deployment to Secure IoT in Industrial Environment," Quality Control- An Anthology of Cases, Jan. 2023, doi:10.5772/intechopen.104469.
[27] Iman Sharafaldin, Arash Habibi Lashkari, and Ali A. Ghorbani,"Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization", 4th International Conference on Information Systems Security and Privacy (ICISSP), Portugal, January 2018.
[28] Singh, S., & Kumar, D. (2024, June 1). Data Fortress: Innovations in Big Data Analytics for Proactive Cybersecurity Defense and Asset Protection. International Journal of Research Publication and Reviews.
[29] Muneer, A., Taib, S. M., Fati, S. M., Balogun, A. O., & Aziz, I. A. (2022). A Hybrid Deep Learning-Based Unsupervised Anomaly Detection in High Dimensional Data. Computers, Materials & Continua, 70(3).
[30] M. Ling, W. Qi, D. Chang, X. Zhang, and C. Zhang, "Machine learning-based network sparsification modeling for IoTs security analysis," Aug. 2023, doi: .doi.org/10.1117/12.2690061.
[31] Hwang et al. "IoT Service Slicing and Task Offloading for Edge Computing" Ieee internet of things journal (2021) doi:10.1109/jiot.2021.3052498.
[32] Meduri, K., Satish, S., Gonaygunta, H., Nadella, G. S., Maturi, M. H., Meduri, S. S., & Podicheti, S. (2024). Understanding The Role Of Explainable AI And Deep Learning In Threat Analysis, 4(5).