ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

AI-Enhanced Threat Detection and Response in Cloud Infrastructure Using Deep Learning Techniques

Anila Gogineni

Independent Researcher, USA

ABSTRACT

Cybersecurity must be proactive and flexible to keep up with the ever-changing cyber threat scenario. As cloud infrastructure becomes a primary target for cyber-attacks, there is a growing need for advanced threat detection systems to protect critical data and services. This document adopts deep learning methods to establish an AI-based threat detection structure for protecting cloud security. The framework applies the Edge-IIoTset dataset to detect numerous attack scenarios that occur in IoT and IIoT environments, particularly DoS/DDoS attacks. The framework uses Edge-IIoTset dataset which goes through strict data preprocessing steps and normalization and feature selection to enhance model optimization. The obtained experimental findings establish BERT as the top model because it delivers a detection accuracy of 98.2% and precision/recall/F1-score readings of 98%, which validate its superior ability to detect complex threat patterns. The BERT model achieves high classification accuracy across attack types based on its performance analyses through confusion matrix and ROC curve. The study demonstrates how BERT contributes to enhancing cloud infrastructure cybersecurity frameworks by delivering dependable and scalable solutions for protecting Industrial Internet of Things networks from threats.

***Corresponding author**

Anila Gogineni, Independent Researcher, USA.

Received: February 08, 2024; **Accepted:** February 12, 2024; **Published:** February 19, 2024

Keywords: Cloud Security, Cyber Threats, Threat Detection, Deep Learning, Cloud Infrastructure, Edge-IIoTset Dataset

Introduction

The rapid spread of cloud computing technology enables customers along with businesses to access flexible and cost-effective solutions for their data storage needs and processing requirements as well as application deployment services. Cloud technology enhances industrial operations and innovation because it provides shared infrastructure alongside demand-based services [1]. Cloud adoption speeds up while making the related cybersecurity threats intensify simultaneously [2]. Cloud environments present increased attack opportunities to cyber attackers because of their linked operation models [3]. The security measures for protecting sensitive data, along with system integrity and service availability, depend entirely on cloud infrastructure security protocols. Modern cloud system attacks have evolved into more advanced threats like APTs and insider threats and also include Do attacks and data breaches and their sophisticated variants [4]. Financial losses, together with reputational damage and legal penalties, constitute potential results when these assaults occur. Security threats in cloud ecosystems remain insufficient due to their distributed structure and constantly evolving environment thus making signature- based detection along with perimeter defenses ineffective. The market needs adaptive real-time threat identification systems since cyber threats continue to advance in complexity.

Effective cloud security deployment requires violent threat detection alongside countermeasures to protect against threats. Threat detection depends on discovering irregular activities, unexpected situations, and unauthorized entry efforts in cloud infrastructure. The goal of mitigation strategies is to control recognized threats while stopping any possible damage from occurring. Modern cloud infrastructure complexity exceeds the capacity of conventional security solutions to track down emerging security challenges [5]. AI, together with DL, has established itself as a groundbreaking technological approach to cybersecurity [6].

The use of automated threat detection and response systems based on DL has greatly improved cybersecurity operations [7]. DL models serve as a prevention method for cloud security through their efficient security data processing capabilities and their ability to detect complex patterns and identify irregularities [8]. These models can identify zero- day attacks, detect insider threats, and enhance incident response capabilities, making them an invaluable asset for securing cloud infrastructures.

Significance and Contribution

The threat detection framework stands vital since it employs deep learning techniques to enhance Industrial IoT cybersecurity systems. The Edge-IIoTset dataset receives preprocessing alongside normalization and feature selection methods through which the framework delivers optimal model performance through high-quality data input. The analysis benefits from strengthened robustness when BERT operates for cloud-based threat detection alongside comparison with Decision Tree and CNN systems. Evaluation indicators like as recall, accuracy, precision, F1-score, and ROC curve provide for a comprehensive assessment of the model's effectiveness, which in turn enables improved and preemptive threat mitigation strategies. The main contributions are shown below:

- The team must develop AI models for cloud threat detection using Edge-IIoT set dataset information.
- Advances data preprocessing methods like encoding and normalization and feature importance implementation are used to boost the detection precision of the system.
- Proposes using BERT for cloud-based threat detection, enhancing the ability to detect sophisticated cyber threats.
- Compare BERT's performance against CNN and Decision Tree models to ascertain which threat detection strategy works best.
- An exhaustive examination of the model's efficacy in cloud security via the use of many evaluation measures, including ROC-AUC, confusion matrices, and F1-score.

Justification and Novelty

The increasing complexity and frequency of cyber- attacks on cloud infrastructures necessitate advanced threat detection systems capable of identifying and mitigating sophisticated threats. This paper introduces a novel AI- enhanced framework for cloud security using deep learning techniques, specifically focusing on the BERT model. Unlike traditional methods, which may struggle to capture complex attack patterns, BERT leverages its advanced contextual understanding to achieve superior performance in detecting a wide range of IoT and IIoT-related attacks, including DoS/DDoS, MITM, Injection, and Information Gathering. The novelty of this work lies in its application of BERT for cloud-based threat detection, a relatively underexplored approach, and its comparative evaluation against other well- established models like CNN and Decision Tree.

Structure of the Paper

The study is structured as follows: Section II reviews prior research on threat detection in cloud environments. Section III details the dataset, preprocessing, and methodology. Section IV presents experimental results, comparing model performance. Section V wraps up with important results, highlighting how deep learning approaches improve cloud security and mitigate threats.

Literature Review

This section examines various review articles on threat detection in cloud infrastructure. The effective identification and mitigation of cyber risks is emphasized by the employment of ML and DL algorithms. Some of review papers are as:

Asaduzzaman and Rahman the training data was supplemented with additional attack data using the top 12 characteristics of a timeseries Generative Adversarial Network (TGAN). The results showed that the combined dataset performed better with 93.53% accuracy, compared to 84.29% accuracy with the AWID dataset alone [9].

Tiwari and Jain provide a fresh take on firewalls by securing cloud computing environments using ML and DL. The results are derived using UNSW-NB-15, a dataset that is available to the public. It improves anomaly detection by 97.68 percent, according to the statistics [10].

Bin Sarhan and Altwaijry recent advances in modern ML techniques, such as ensemble models and DL, make it simpler to address a number of challenging problems by modelling data and uncovering hidden patterns. Based on past data, researchers extracted behavioral traits using the Deep Feature Synthesis technique. Using PCA to reduce the number of dimensions, they developed 69,738 user attributes and used advanced ML techniques, including classification and anomaly identification models, to find insider threats. A 91% accuracy rate was attained using the anomaly detection model [11].

Tekin and Yilmaz shows the collected Twitter security data underwent deep learning algorithm processing. Recursive neural networks perform categorization of cyber threat intelligence that includes DDoS and malware as well as ransomware and other threats. The researchers achieved success in identifying cyber threat information relevance in 88.64% of cases and correctly determined threat intelligence types in 89.49% of analyzed data [12].

Yan and Xiong propose Web-APT-Detect (WAD), an unsupervised approach based on anomaly detection, in which there is an attention mechanism employed to design an encoder-decoder as a self-translation model. The approach achieves an F1-Score of 0.9844 in trials on the CSIC 2010 dataset, matching the level of the advanced supervised algorithm and surpassing the known unsupervised algorithm [13].

Table 1 provides a comparative analysis of previous studies on AI-driven threat detection in cloud infrastructure, outlining the datasets used, key findings, limitations, and future research directions to enhance security and detection capabilities.

Table 1: Summary of background study on cloud-based threat Detection using Deep Learning Algorithm

Authors	Methods	Dataset	Key Findings	Limitations & Future Scope
Asaduzzaman and Rahman	Time-series GAN for data augmentation, Hybrid LSTM- CNN model	AWID dataset	Concatenated dataset (original + GAN-generated) improved accuracy to 93.53% vs. 84.29% with the original dataset.	Further exploration of GAN-based data augmentation for other cyber threat datasets
Tiwari and Jain	Machine learning & DL system, "Most Frequent Decision" methodology	U N S W - N B - 15 dataset	Improved anomaly detection to 97.68% accuracy	Testing on real-world cloud traffic and refining decision logic for adversarial robustness
(Bin Sarhan and Altwaijry	Deep Feature Synthesis, PCA, Machine Learning (Anomaly Detection and classification Models)	Insider Threat Dataset	Anomaly detection model achieved 91% accuracy in identifying insider threats.	Potential improvement in feature selection and scalability for larger datasets. Further validation on diverse datasets required.

Tekin and Yilmaz	Recursive Neural Networks (RNN) for cyber threat intelligence classification	Twitter data (cybersecurity threats)	88.64% accuracy in detecting relevant intelligence, 89.49% in classifying threat types	Expansion to multilingual tweets and real-time threat intelligence applications
Yan and Xiong	Unsupervised anomaly detection (Web-APT-Detect), Encoder- Decoder with Attention Mechanism	CSIC 2010 dataset	Achieved F1-score of 0.9844, surpassing existing unsupervised algorithms	Adapting the model for real-time HTTP request monitoring and broader datasets

Methodology

The methodology of the AI-enhanced threat detection framework utilizes deep learning techniques, as illustrated in Figure 1 flowchart. The research begins with the Edge-IIoTset dataset, which undergoes data preprocessing, including handling missing values and applying label encoding for labeling. Following preprocessing, data normalization is performed using a min-max scaler to standardize feature values, ensuring optimal model performance. Then, the most important traits are kept by using feature selection. The dataset is subsequently split into training (80%) and testing (20%) subsets to evaluate model effectiveness. The BERT model is proposed for cloud-based threat detection, while CNN and Decision Tree (DT) are used for comparison. The effectiveness of the model is evaluated by performance assessment utilizing the following metrics: accuracy, precision, recall, F1-score, and ROC curve.

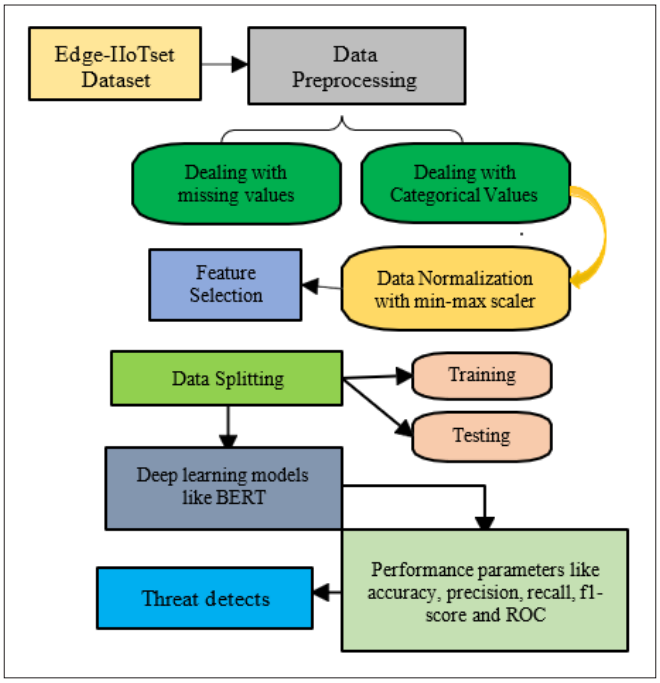

Figure 1: Flowchart for Cloud-Based Threat Detection

This section provides a concise explanation of the flowchart's subsequent steps:

Data Collection

The Edge-IIoT set dataset is perfect for their research since it accurately portrays real-world scenarios with its diverse range of devices, sensors, protocols, and cloud/edge configurations. The following five types of attacks are included in this dataset, all of which pertain to protocols used for connection in the IoT and IIoT: DDoS, Information Gathering, man-in-the-middle (MITM), and injection assaults are all potential threats. Figure 2 illustrates the prevalence of various cyber threat categories.

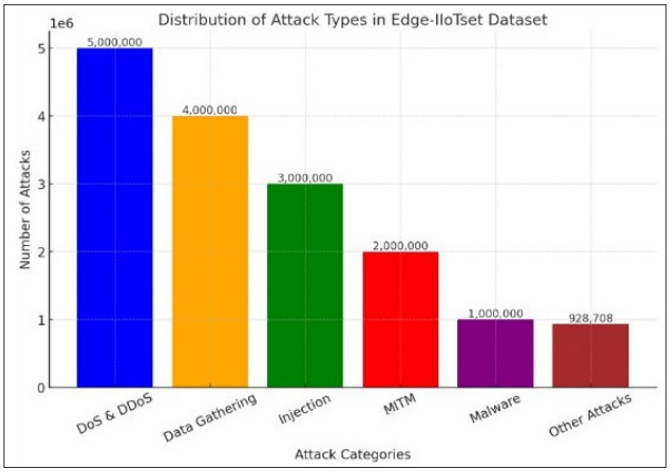

Figure 2: Distribution of Attack Type

Figure 2's bar chart shows how the Edge-IIoTset dataset's attack types are distributed. DoS and DDoS attacks dominate with 5 million instances, followed by Data Gathering (4M), Injection (3M), and MITM (2M). Malware (1M) and Other Attacks (0.93M) highlight diverse threats, aiding cloud-based threat detection strategies.

Data Preprocessing

Data preparation entails cleaning and converting raw data into an acceptable format in order to make it ready for analysis [14]. The first step in data processing is cleaning the dataset of any extraneous information. Eliminating information linked to unsuccessful breaches is the first stage of this procedure. In order to reduce space and improve processing performance, empty fields are removed. After data cleansing, labels are applied [15]. Further pre-processing is given below:

- **Dealing with Missing values:** Methods for preserving the integrity of the dataset include filling in missing values using the median, mode, or mean and deleting rows that contain null values.
- **Dealing with Categorical Values:** The categorical data types are transformed into numerical data types using label encoding techniques. Label encoding is a method that uses numerical labels to transform categorical input into numerical data.

Data Normalization

For data normalization, min-max normalization was used to increase the efficiency of the aforementioned methods by setting all features to a value between 0 and 1 [16,17]. Maximum-minimum scales examine each characteristic independently in light of the subsequent Equation (1).

$$x' = \frac{(x - x_{min})}{(x_{max} - x_{min})} \quad (1)$$

where x′ denotes the scaled value of x.

Feature Importance

Feature importance refers to a technique used to assign a relative importance to each feature (or variable) in a dataset, indicating how significantly each contributes to the prediction of the target variable in a machine learning model. It helps identify the most influential features, enabling better model interpretability, feature selection, and improved performance by focusing on relevant variables. Feature importance scores are displayed in Figure 3.

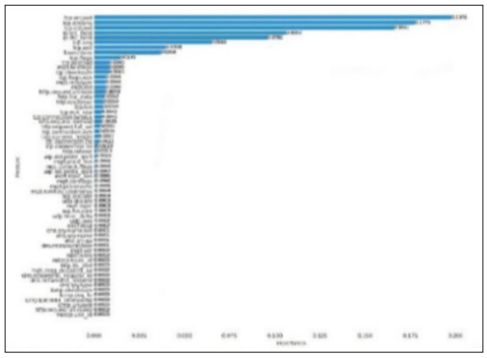

Figure 3: Features Importance of Data

The feature importance analysis in Figure 3 ranks attributes based on their impact on threat detection in the Edge-IIoT set dataset. The x-axis represents importance, while the y-axis lists features. Higher-ranked features on the left significantly enhance detection accuracy, while lower- ranked ones contribute minimally. The dataset, comprising network traffic and system logs, optimizes predictive capabilities, strengthening cloud security.

Data Splitting

The training and testing datasets were kept separate. The models were trained using the training set, and their performance was evaluated using the test set. The training set included 80% of the data used for DL threat identification, whereas the testing set contained 20%.

Proposed BERT Model

BERT is a pre-trained transformer-based deep learning model designed for cybersecurity applications, such as threat detection, intrusion detection, and malware classification [18]. It builds upon the BERT architecture and is fine-tuned on cybersecurity-related textual data, including network logs, security alerts, and threat intelligence reports. BERT leverages self-attention mechanisms to extract meaningful contextual representations, improving threat detection accuracy and enhancing cybersecurity defenses [19]. BERT's core mechanism relies on multi-head self-attention, which captures relationships between words in a sequence Equation (2):

$$Attention\,(Q,K,V) = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V \qquad (2)$$

Where Q is the Query Matrix, K is the Key Matrix, V is the Value Matrix, and d sub k is the Scaling factor (dimension of key vectors).

Performance Measures

The performance of the ML may be measured by training a prediction model on a specified quantity of data. This ML classifier needs to have its features set fed with class label outcomes during training [20].

- True Positive (TP) occurs when the model's prediction of the positive class is accurate.
- FP stands for "False Positive," which is the result when the model gets a positive class prediction wrong. Also known as a type-1 error.
- False Negative, or FN, is a result that occurs when the model gets the negative class wrong. Type-2 error is another term for it.
- True Negative, or TN, is a result that occurs when the model accurately predicts the negative category.

Accuracy: Equation (3) provides the accuracy-based proportion of correct classifications relative to all inputs.

$$Accuracy = \frac{TPFN}{TP+FP+TN+FN} \qquad (3)$$

Precision: Precision is defined as the ratio of the number of attack outcomes that were properly predicted to the total number of attack classes, as indicated in Equation (4):

$$Precision = \frac{TP}{TP+FP} \qquad (4)$$

Recall: The "recall" metric measures how many assaults were accurately identified relative to the total number of samples that were supposed to be assaulted; it is calculated using Equation (5):

$$Recall = \frac{TP}{TP+FN} \qquad (5)$$

F1-score: An accurate statistical function for measuring a system's accuracy is the F-measure, which is the harmonic mean of recall and precision. It is given by Equation (6)

$$F1-Score = \frac{2(Precision*Recall)}{Precision+Recall} \qquad (6)$$

Loss: In classification problems, the cross-entropy loss quantifies the discrepancy between the actual and anticipated probability distributions. It is shown in Equation (7)

$$L = -\sum_i \widehat{y_i} \quad \log\left(\widehat{y_i}\right) \qquad (7)$$

Here, $_i$ is the ground truth value (1 if the class is correct, otherwise 0) and yi The model's predicted probability for class $_i$.

ROC-AUC: The ROC curve provides a visual representation of the prediction model's accuracy. The AUC is used to calculate the area under the ROC curve.

Result Analysis and Discussion

The experiment was evaluated in an experimental setting using a computer with Python 3.11 and Jupyter Notebook to implement the experiment to deal with the Edge-IIoTset dataset. The Intel(R) Core (TM) i5-1135G7 @ 2.40GHz and 16 GB RAM are used in Threat detection in cloud infrastructure. Table 2 summarizes the outcomes of the BERT model's assessment on an Edge-IIotset dataset and shows that it performs well with balanced evaluation criteria including as precision, accuracy, recall, f1-score, and ROC, further proving its usefulness.

Table 2: BERT Model Performance for the Cloud-Based Threat Detection on Edge-IIotset Dataset

Performance Measures	BERT (Bidirectional Encoder Representations from Transformers)
Accuracy	98.2
Precision	98
Recall	98
F1-score	98

The BERT model performs its analysis of cloud-based threat detection which is detailed in Table II. The detected cyber threats reached 98.2% accuracy demonstrating how the model shows reliable distinctions between safe and dangerous actions according to research findings. The model demonstrates effective threat detection ability due to its precision of 98% alongside a re-call value of 98% and an F1- score measurement of 98%. BERT uses its deep contextual learning capability to boost cloud environment cybersecurity by effectively analyzing difficult threats and developing immediate threats mitigation approaches.

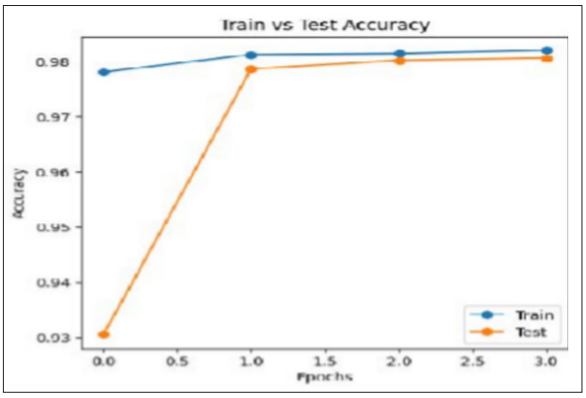

Figure 4: Train and Test Accuracy of BERT

Figure 4 demonstrates how BERT achieves its training and testing accuracy for detecting cloud threats. A single epoch leads to test accuracy reaching 93% before it converges with the training accuracy to reach 98%. Strong generalization occurs while maintaining minimal underfitting based on these results. The modest difference between training and test accuracy metrics maintains minimal chances of overfitting the model with their data. The obtained results demonstrate that BERT successfully learns security patterns in the Edge-IIoTset dataset to achieve optimal cloud security detection accuracy.

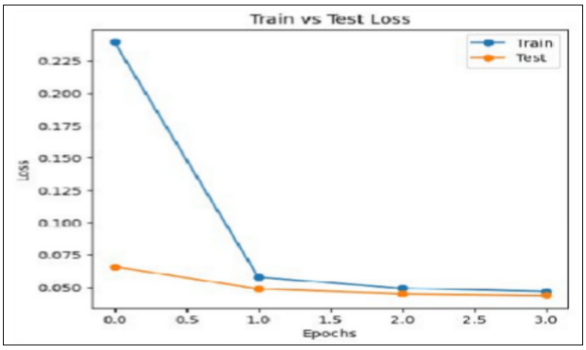

Figure 5: Train and Test Loss of BERT model

Figure 5 displayed a training and test loss graph, illustrating the convergence of the BERT model for cloud threat detection. The training loss, denoted by a blue line, starts at a high value but decreases sharply within the first epoch, aligning closely with the test loss. Both losses stabilize around 0.05, indicating minimal overfitting. The small gap among the training and test loss curves confirms strong generalization and model robustness.

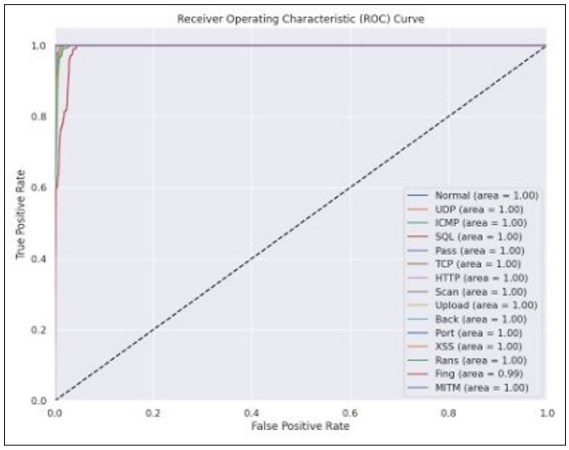

Figure 6: ROC Graph of BERT Model

The ROC curve for the BERT model, which uses an Edge-IIoTset dataset for cloud-based threat identification, is shown in Figure 6. To evaluate the model's efficacy, one may look at the ROC curve, which shows the compromise among the TPR (sensitivity) and FPR at various classification levels. The AUC values for most threat categories, including Normal, UDP, ICMP, SQL, TCP, HTTP, and various attack types, are close to 1.00, indicating near-perfect classification capability. The BERT model demonstrates exceptional threat detection accuracy, with minimal variation (e.g., Rans AUC = 0.99), confirming its reliability in distinguishing normal and malicious activities for cloud security.

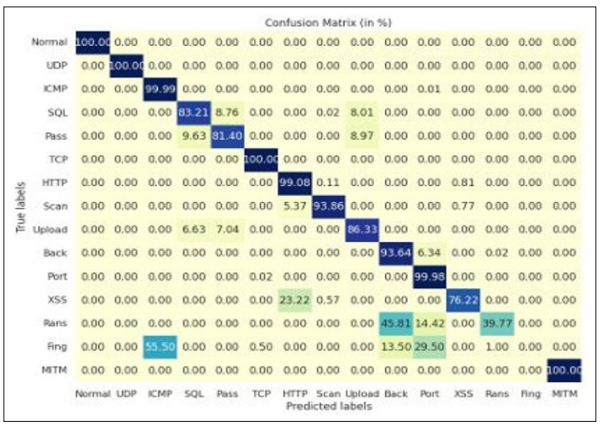

Figure 7: Confusion Matrix of BERT Model

Figure 7 displays the BERT model's confusion matrix, which emphasizes the classification accuracy for different sorts of threats. Most categories, including Normal, UDP, ICMP, TCP, and MITM, achieve 100% accuracy, while some misclassifications occur in SQL, Pass, XSS, and Ransomware (Rans). Despite minor errors, the model demonstrates strong overall performance, effectively identifying cloud security threats with high precision.

Comparative Analysis

The comparative analysis evaluates DL models like CNN and Decision Tree (DT) against BERT, the highest- performing model [21,22]. Metrics like accuracy, precision, recall, and F1-score highlight BERT's superior performance, ensuring robust cloud-based threat detection shown in Table 3.

Table 3: Deep Learning Models Comparison on the Edge-IIoTset Dataset for Cloud-Based Threat Detection

Models	Accuracy	Precision	Recall	F1-score
BERT	98.2	98	98	98
CNN [21]	95	96	95	95
DT [22]	73	70	72	69

Table 3 compares the performance of BERT, CNN, and DT models for cloud-based threat detection on the Edge- IIoTset dataset. BERT surpasses other models in performance due to its complex context processing which yields 98.2% accuracy measurement along with 98% precision, recall and F1-score values. The CNN model demonstrates strong performance against the other models with an accuracy of 95% while showing precision, re-call, and F1-score values of 96%, 95%, and 95% respectively. This indicates slightly lower accuracy compared to BERT. The DT model exhibits reduced success rates because of its performance metrics reaching 73% accuracy and 70% precision and 72% recall and 69% F1-score indicating its limitations in addressing sophisticated security challenges. BERT stands out as the best model when applied to this task with CNN being the next most effective while DT exhibits limited suitability.

The implementation of BERT in an AI threat detection framework provides 98.2% accurate results which produces balanced precision, recall and F1-score metrics for reliable threat identification. The model BERT achieves better ability to handle complicated contextual details than CNN (95%) and DT (73%) which leads to less false positive outcomes. BERT demonstrates robust capabilities for real-time cloud security thanks to its validated generalization power which converges loss data and produces high ROC values to deliver advanced protection against changing cyber threats.

Conclusion and Future Work

The essential role of cloud computing in contemporary IT infrastructure demands top priority for safeguarding cloud- based systems. Cyber-attacks particularly DoS, DDoS, Injection and Information Gathering have elevated cloud platforms to become priority targets for cybercriminals. Traditional threat detection methods often struggle to identify these sophisticated threats due to their reliance on rule-based systems or limited processing power for complex datasets. BERT serves as a deep learning model that analyzes security threats from the Edge-IIoTset dataset to provide classifications. Research findings validate the superiority of BERT over CNN and DT models since it reaches 98.2% accuracy with performance metrics of 98% precision, recall, and F1-score. The BERT model with its transformer architecture proves efficient in capturing context patterns through pre-training to detect various cybersecurity attacks DoS/DDoS, MITM, Injection, and Information Gathering. Researchers should apply transfer learning with hyperparameter optimization strategies to BERT to achieve improved efficiency along with enhanced performance. Future research is also possible for expanding the dataset to include more types of attacks, as well as adaptive mechanisms for evolving threats.

References

1. Murri S (2022) Data Security Challenges and Solutions in Big Data Cloud Environments. Int J Curr Eng Technol 12.
2. Kolluri V (2015) An Extensive Investigation into Guardians of The Digital Realm: Ai-Driven Antivirus and Cyber Threat Intelligence. TIJER 2.
3. Steingartner W, Galinec D, Kozina A (2021) Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model. Symmetry (Basel) 13.
4. Neeli SSS (2023) Critical Cybersecurity Strategies for Database Protection against Cyber Attacks. JArtif. Intell Mach Learn Data Sci 1: 5.
5. Ferrag MA, Friha O, Hamouda D, Maglaras L, Janicke H (2022) Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. IEEE Access 10: 40281-40306.
6. Neeli SSS (2022) Gen Database Administration: Integrating AI and Technology Advancements. Int J Lead Res Publ 3: 10.
7. Rajendran S, Valarmathi A, Kumar MS (2022) Threat Detection and Incident Response in Cloud Security. Priv Secur Challenges Cloud Comput 207-227.
8. Gudimetla SR, Kotha NR (2018) Ai-Powered Threat Detection in Cloud Environments. Turkish J Comput Math Educ 9: 638-642.
9. Asaduzzaman M, Rahman MM (2022) An Adversarial Approach for Intrusion Detection Using Hybrid Deep Learning Model. International Conference on Information Technology Research and Innovation, ICITRI https://ieeexplore.ieee.org/document/9970221/.
10. Tiwari G, Jain R (2022) Detecting and Classifying Incoming Traffic in a Secure Cloud Computing Environment Using Machine Learning and Deep Learning System. Proceedings - 2022 IEEE 7th International Conference on Smart Cloud, SmartCloud https://ieeexplore.ieee.org/document/9944834.
11. Bin Sarhan B, Altwaijr N (2022) Insider Threat Detection Using Machine Learning Approach. Appl Sci 13: 259.
12. Tekin U, Yilmaz EN (2021) Obtaining Cyber Threat Intelligence Data from Twitter with Deep Learning Methods. 5th International Symposium on Multidisciplinary Studies and Innovative Technologies, Proceedings https://ieeexplore.ieee.org/document/9604715.
13. Yan L, Xiong J (2020) Web-APT-Detect: A Framework For Web- Based Advanced Persistent Threat Detection Using Self-Translation Machine With Attention. IEEE Lett. Comput. Soc 3: 66-69.
14. Neeli SSS (2021) Ensuring Data Quality: A Critical Aspect of Business Intelligence Success. Int J Lead Res Publ 2: 7.
15. Wang BX, Chen JL, Yu CL (2022) An AI-Powered Network Threat Detection System. IEEE Access https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9775989.
16. Oliveira N, Praça I, Maia E, Sousa O (2021) Intelligent cyber attack detection and classification for network-based intrusion detection systems. Appl Sci https://www.mdpi.com/2076-3417/11/4/1674.
17. Boddu B (2023) Scaling Data Processing with Amazon Redshift Dba Best Practices for Heavy Loads. International Journal of Core Engineering & Management 7: 5.
18. Rajarshi Tarafdar YH (2018) Finding majority for integer elements. J Comput Sci Coll 33: 187-191.
19. Pahune S, Chandrasekharan M (2023) Several Categories of Large Language Models (LLMs): A Short Survey. Int J Res Appl Sci Eng Technol 11: 615-633.
20. Nkongolo M, van Deventer JP, Kasongo SM, Zahra SR, Kipongo J (2022) A Cloud Based Optimization Method for Zero- Day Threats Detection Using Genetic Algorithm and Ensemble Learning. Electron 11: 1-26.
21. Ferrag MA, Hamouda D, Debbah M, Maglaras L, Lakas A (2023) Generative Adversarial Networks-Driven Cyber Threat Intelligence Detection Framework for Securing Internet of Things. Proc - 19th Int Conf Distrib Comput Smart Syst

Internet Things, DCOSS-IoT 196-200.

22. Bin Samin O, Algeelani NAA, Bathich A, Adil GM, Qadus A, et al. (2023) Malicious Agricultural IoT Traffic Detection and Classification: A Comparative Study of ML Classifiers. J Adv Inf Technol 14: 811-820.