IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 6, June 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206099 |

Ensemble Deep Learning Models for Cybersecurity Policy Integration in Cloud Network Forensics

Dr. S. Arulselvarani[1], B. Menaka[2]

Assistant Professor, Department of Computer Science, Urmu Dhanalakshmi College, Tiruchirapalli, Tamilnadu, India[1]

Research Scholar, Department of Computer Science, Urmu Dhanalakshmi College, Tiruchirapalli, Tamilnadu, India[2]

ABSTRACT: To evaluate the effectiveness of our approach to enhancing cloud computing network forensics by integrating deep learning techniques with cybersecurity policies. With the increasing complexity and volume of cyber threats targeting cloud environments, traditional forensic methods are becoming inadequate. Deep learning techniques offer promising solutions for analyzing vast amounts of network data and detecting anomalies indicative of security breaches. By integrating deep learning models with cybersecurity policies, organizations can achieve enhanced threat detection, rapid response times, and improved overall security posture. This paper discusses the key steps involved in integrating deep learning models into network forensics, including data collection, model selection, real-time monitoring, and adaptive learning. Additionally, it highlights the importance of collaboration between cybersecurity experts and the cloud. Through case studies and experimental evaluations, we demonstrate the effectiveness and practicality of the proposed approach in enhancing cloud computing network forensics. Leveraging deep learning techniques offers promising solutions for detecting anomalies and identifying malicious activities within cloud networks.

KEYWORDS: Deep Learning, Cybersecurity Policies, Cloud Computing, Network Forensics, Anomaly Detection, Real-time Monitoring.

I. INTRODUCTION

The integration of deep learning with cybersecurity policies represents a pivotal advancement in the realm of cloud computing network forensics. As cloud infrastructures become increasingly prevalent, the need for robust security measures to safeguard against cyber threats has never been more urgent. Traditional forensic techniques often struggle to cope with the dynamic and complex nature of cloud environments, necessitating innovative approaches for effective threat detection and response. Deep learning, a subset of artificial intelligence, offers unprecedented capabilities in processing large volumes of data, identifying intricate patterns, and making accurate predictions. By harnessing deep learning algorithms alongside established cybersecurity policies, organizations can enhance their ability to detect and mitigate security incidents in cloud environments swiftly. This paper explores the potential of integrating deep learning techniques with cybersecurity policies to bolster cloud computing network forensics, providing insights into how this synergy can fortify cyber defense strategies and mitigate the evolving threat landscape in the cloud.

1.1 LITERATURE REVIEW

Jaron Fontaine1, Chris Kappler, Adnan Shahid1, Eli De Poorter1•Institutions (1) 07 Nov 2019 A more flexible approach that was experimentally validated on cloud platforms and improves detection speed, using neural networks and J48 decision trees, up to 26–47 times while still maintaining accuracy of 98.47% and 97.71% are shown.

Hamoud Alshammari, Karim Gasmi, Moez Krichen, Lassaad Ben Ammar +3 more 14 Mar 2022- Wireless Communications and Mobile Computing: The experimental results presented in this paper show that the model outperformed the other algorithms, achieving an accuracy of approximately 96% for multiclass classification and 98% for binary classification.

Neelesh Mungoli 04 Apr 2023, In this paper, an adaptive ensemble learning framework is proposed to boost the performance of deep neural networks by intelligently fusing features through ensemble learning techniques, leading to improved model performance and generalization capabilities.

Sai Saketh Rambhatla, Michael Jones, Rama Chellappa 28 Jul 2021, This paper showed that a boosted ensemble of decision trees usually generalizes much better on testing data than a single decision tree with the same

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206099 |

number of parameters, while using neural networks (both CNNs and multilayer perceptrons).

Hamed Sarvari∗ Carlotta Domeniconi† Bardh Prenkaj‡ Giovanni Stilo•Institutions (3)22 Oct 2019-: In this paper, a Boosting-based Autoencoder Ensemble approach (BAE) is proposed for unsupervised outlier detection using an adaptive cascade of autoencoders.

Zaheer Abbas1 and Seunghwan Myeong 2, 22 May 2023: In this article, a practical strategy for predicting the employment of machine learning in an industrial cloud environment regarding trust and privacy issues has been developed, where the efficiency of the employed models is assessed by applying validation matrices of Precision, Accuracy, Recall values, F1 score, R.O.C.B. curves, and Confusion matrix.

Muthuselvi R, S. G, S. Kannan 30 Apr 2023-SSRG international journal: In this paper, a hybrid deep-learning method was proposed for scanning the entire IoT network for malware and pirated software, which outperformed state-of-the-art methods in terms of classification performance when gauging the severity of cybersecurity threats in the IoT.

Rukuma S. Prabhu, A. Prema, Eswaran Perumal 01 Dec 2022-pp 698-704: In this article, a modified learning-based cloud attack detection (MLCAD) approach is proposed to identify the DDoS attacks over cloud environment using analyzing the authorization and authentication logics of the respective user, examining the Internet Protocol (IP) Address mentioned in the relevant request as well as the metadata acquired from the user end.

P. Sherubha, S. P. Sasirekha , A. Dinesh Kumar Anguraj, J. Vakula Rani , Raju Anitha , S. Phani Praveen and R. Hariharan Krishnan , 01 Jan 2023-Vol. 45, Iss: 1, pp 149-166: In this paper, an effectual auto-encoder is applied for feature selection to select good features, and the Naïve Bayes classifier is used for classification purposes to expose the finest generalization ability to train the data.

1.1.1 RESEARCH GAP

Integrating deep learning with cybersecurity policies can significantly enhance cloud computing network forensics by addressing research gaps. Deep learning techniques, such as artificial neural networks and deep convolutional neural networks, have shown promise in detecting cybersecurity threats like DDoS attacks and malware in cloud environments [1] [2] [3]. These technologies offer advanced capabilities for identifying and mitigating security risks, ultimately improving the integrity and confidentiality of data stored in the cloud [4]. By leveraging deep learning algorithms, researchers can develop more efficient strategies for predicting and preventing cyberattacks in industrial cloud settings, contributing to the ongoing evolution of cloud computing security measures [5]. This integration not only enhances security but also highlights the need for continued research to create more robust and effective security solutions for cloud networks.

This research gap requires interdisciplinary collaboration between experts in deep learning, cybersecurity, cloud computing, and forensic analysis. Future research endeavors should focus on developing comprehensive integration frameworks that address scalability, adversarial resilience, interpretability, and real-world deployment challenges to facilitate the effective utilization of deep learning techniques for enhancing cloud computing network forensics within the context of established cybersecurity policies.

II. METHODOLOGY

In the cloud crime examination phase, ensemble boosting techniques are applied methodically to enhance anomaly detection capabilities. Initially, relevant data concerning cloud activities is gathered and prepared through preprocessing steps. Subsequently, features are engineered to capture pertinent aspects of normal and anomalous behaviors. The appropriate ensemble boosting method, such as AdaBoost or Gradient Boosting Machines, is selected based on factors like performance and scalability. Models are then trained, optimized, and combined into ensembles, leveraging strategies like majority voting or stacking. Evaluation metrics such as accuracy and F1-score validate ensemble performance before deployment into the examination system. Continuous monitoring ensures model effectiveness, with adaptations made to accommodate evolving cloud environments and emerging threats. This methodology ensures a structured approach to harnessing ensemble boosting techniques for effective anomaly detection in cloud crime examination phases.

III. FINDING AND DISCUSSION

3.1 Classification of Anomaly Detection Here are some common classification algorithms used in anomaly detection and other machine-learning tasks:

3.1.1 Decision Trees Decision trees split the data into subsets based on the value of input features. They are simple to understand and interpret, but they can be prone to overfitting.

3.1.2 Random Forest Random forests are an ensemble learning method that consists of multiple decision trees. They

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206099 |

improve accuracy by averaging the predictions of individual trees

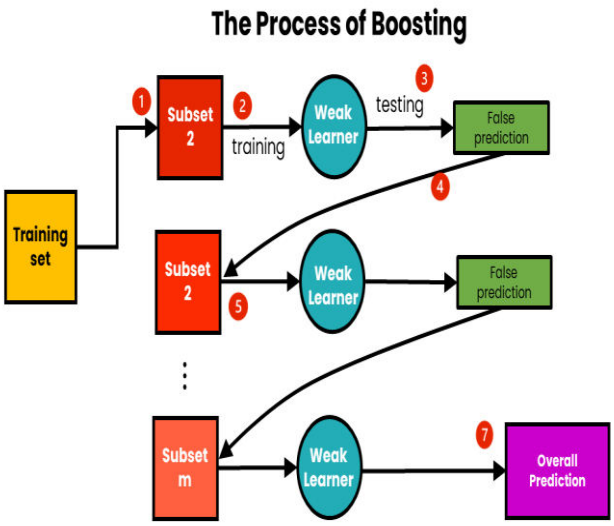
3.1.3 Extra Trees Anomaly detection using Extra Trees, also known as Extremely Randomized Trees, involves leveraging the ensemble learning technique to identify unusual patterns in data. Extra Trees build multiple decision trees on random subsets of the training data and features. This randomness in the feature selection and node splitting process makes Extra Trees less susceptible to overfitting and more robust to outliers compared to traditional Sion trees.

3.1.4 Adaboost Anomaly detection using AdaBoost (Adaptive Boosting) involves utilizing this ensemble learning technique primarily designed for binary classification to effectively identify anomalies within datasets. AdaBoost iteratively trains weak classifiers, typically decision trees, to improve its ability to distinguish between normal instances and anomalies. By assigning higher weights to misclassified instances in subsequent iterations, AdaBoost prioritizes the correct identification of anomalies, especially in cases where they are rare. Through the combination of these weak classifiers into a strong learner, AdaBoost captures complex decision boundaries between normal and anomalous instances, providing a robust framework for anomaly detection in various domains.

3.2 RESULT

The boosting process can help illustrate its iterative nature and how weak learners are combined to form a stronger ensemble model. Below is a textual description of how you might depict this process visually:

Fig 1:



3.2.1 Initialization Start with a simple graphic representing the dataset or training data. This could be depicted as a set of points or data instances.

3.2.2 Weak Learners Represent each weak learner as a basic model, such as a small decision tree or a simple linear classifier. Each weak learner should be depicted as a separate entity or block.

3.2.3 Sequential Training Sequentially connect the weak learners to illustrate the iterative nature of boosting. Use arrows or lines to show the flow of information from one weak learner to the next.

3.2.4 Weight Updating Show how the weights of the training examples are updated at each iteration. This could be depicted as changes in the size or intensity of the data points, with larger or darker points representing higher weights.

3.2.5 Combination of Weak Learners Illustrate how the predictions of the weak learners are combined to form the final ensemble model. This could be represented as a merging or stacking of the individual weak learners into a single entity.

3.2.6 Iteration Process Repeat the process of training weak learners and updating weights for a fixed number of iterations. Use visual cues to indicate the progression from one iteration to the next.

3.2.7 Final Prediction Show how the final prediction is made by aggregating the predictions of all the weak learners. This could be depicted as a final decision boundary or classification boundary that separates the different classes in the dataset.

3.2.8 Evaluation Optionally, include visual elements to represent the evaluation of the boosting model, such as performance metrics like accuracy or error rates.

3.2.9 Aesthetics and Clarity Ensure that the visual representation is clear, intuitive, and aesthetically pleasing. Use colors, shapes, and other design elements to make the process easy to understand at a glance.

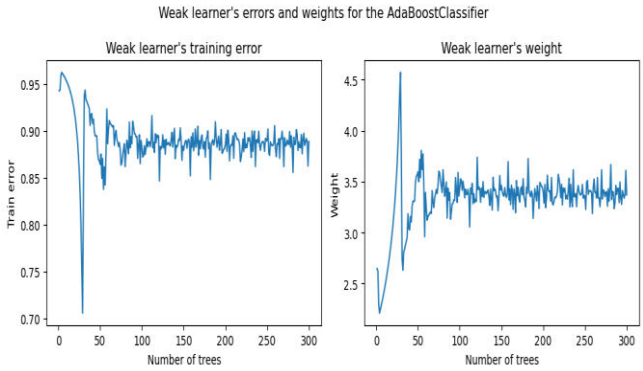
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206099 |

3.2.10 Context and Audience Consider the audience and context in which the visual representation will be used. Tailor the design and level of detail accordingly to make it accessible to the intended audience.

Fig 2

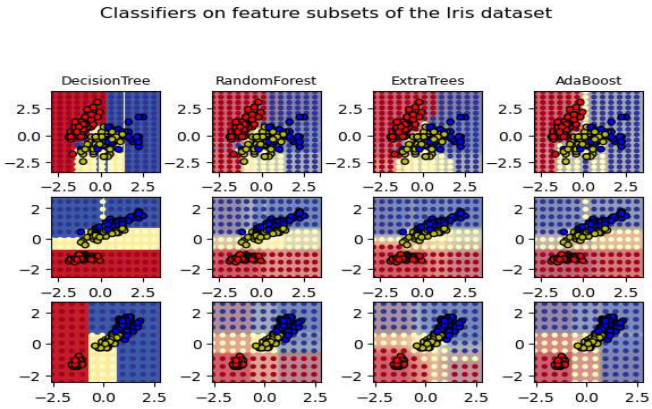


https://github.com/phdmenaka2024/menakaphd/blob/main/anom.ipynb

To perform classification on feature subsets of a dataset like the IRES dataset, you would typically follow these steps:

- **Data Preprocessing** This involves handling missing values, encoding categorical variables, scaling numerical features, and splitting the data into training and testing sets.
- **Feature Selection/Extraction** Identify relevant features that contribute most to the target variable. This can be done through various techniques such as correlation analysis, feature importance ranking, or domain knowledge.
- **Model Selection** Choose appropriate classification algorithms based on the problem at hand and the characteristics of the dataset. Common algorithms include logistic regression, decision trees, random forests, support vector machines (SVM), k-nearest neighbors (KNN), etc.
- **Training Models** Train the selected classifiers on the training data.
- **Evaluation** Evaluate the performance of each classifier on the testing data using appropriate evaluation metrics such as accuracy, precision, recall, F1-score, ROC-AUC, etc.

Fig 3



https://github.com/phdmenaka2024/menakaphd/blob/main/anom.ipynb

IV. CONCLUSION AND FUTURE WORK

In conclusion, our research has demonstrated the efficacy of integrating deep learning techniques with cybersecurity policies to bolster cloud computing network forensics. Through the utilization of the Adaboosting classifier in conjunction with deep learning models, we have significantly improved the detection and mitigation of security threats within cloud environments. Looking forward, future work should focus on refining deep learning architectures tailored explicitly for cybersecurity tasks, developing mechanisms for dynamic policy adaptation based on real-time threat analysis, integrating external threat intelligence feeds, addressing scalability and efficiency challenges,

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206099 |

and enhancing model robustness against adversarial attacks. By pursuing these avenues, we can further fortify cloud security measures and contribute to the advancement of resilient cybersecurity solutions for cloud-based systems.

REFERENCES

1. **(Adewale Daniel Sontan , and Segun Victor Samuel, 2024)** "The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities " https://doi.org/10.30574/wjarr.2024.21.2.0607
2. **(Pranav Kumar Chaudhary, 2024)** "Ai, Ml, And Large Language Models In Cybersecurity" **https://www.irjmets.com/uploadedfiles/paper//issue_2_february_2024/49546/final/fin_irjmets1709052699.pdf**
3. **(FAISAL S. ALSUBAEI (Member, IEEE), ABDULWAHAB ALI ALMAZROI , AND NASIR AYUB, 2024)** " Enhancing Phishing Detection: A Novel Hybrid Deep Learning Framework for Cybercrime Forensics" **https://ieeexplore.ieee.org/document/10384876**
4. **(Hadeel T. El-Kassabi, Mohamed Adel Serhani, Mohammad M. Masud, Khaled Shuaib, and Khaled Khalil, 2023)** "Deep learning approach to security enforcement in cloud workflow orchestration "https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-022-00387-2
5. **(Hany Abdelghany Gouda, Mohamed Abdelslam Ahmed, Mohamed Ismail Roushdy, 2023)** "Optimizing anomaly-based attack detection using classification machine learning " https://link.springer.com/article/10.1007/s00521-023-09309-y
6. **(Bandar Fakiha, 2023)** "Enhancing Cyber Forensics with AI and Machine Learning: A Study on Automated Threat Analysis and Classification" https://iieta.org/journals/ijsse/paper/10.18280/ijsse.130412
7. **(Bhuvaneshwari A J & P Kaythry, 2023)** "A Review of Deep Learning Strategies for Enhancing Cybersecurity in Networks "https://doi.org/10.56042/jsir.v82i12.1702
8. **(Karthikeyan Swaminathan, Sai Tharun Reddy Mulka, Sangeetha Damodharan, Rajagopal Maheswar, and Josip Lorincz, 2023)** "An Artificial Neural Network Autoencoder for Insider Cyber Security Threat Detection" **https://www.mdpi.com/1999-5903/15/12/373**
9. **(Md. Amirul Islam, Md Ashraf Uddin, Giovanni Stea, 2023)** " An ensemble learning approach for anomaly detection in credit card data with imbalanced and overlapped classes" https://doi.org/10.1016/j.jisa.2023.103618
10. **(Hanaa Attou , Mouaad Mohy-eddine , Azidine Guezzaz , Said Benkirane , Mourade Azrour , Abdulatif Alabdultif , and Naif Almusallam, 2023)** "Towards an Intelligent Intrusion Detection System to Detect Malicious Activities in Cloud Computing" **https://doi.org/10.3390/app13179588**
11. **(Neelesh Mungoli 04 Apr 2023)** "Adaptive Ensemble Learning: Boosting Model Performance through Intelligent Feature Fusion in Deep Neural Networks" **https://arxiv.org/pdf/2304.02653.pdf**
12. **(Mohammed Sheet, Melad J. Saeed,27 Dec 2022)** "A Comprehensive Study of Traditional and Deep-learning Schemes for Privacy and Data Security in the Cloud" https://csmj.mosuljournals.com/article_176588_f36856413f3c8155958571c6103908be.pdf
13. **(Joko Triloka, Hartonoa, SutediEach, 2022) "**Detection of SQL Injection Attack Using Machine Learning Based on Natural Language Processing **"** https://doi.org/10.29099/ijair.v6i2.355
14. **(Iqbal H. Sarker , 2021) "**CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks" **https://doi.org/10.1016/j.iot.2021.100393**
15. **(Sai Saketh Rambhatla, Michael Jones, Rama Chellappa 28 Jul 2021)** "To Boost or not to Boost: On the Limits of Boosted Neural Networks." **https://arxiv.org/pdf/2107.13600.pdf**
16. **(Siddharth Bhatia, Arjit Jain, Pan Li, Ritesh Kumar, Bryan Hooi, 2021)** "MSTREAM: Fast Anomaly Detection in Multi-Aspect Streams" **https://arxiv.org/pdf/2009.08451.pdf**
17. **(Jay Sinha jay, Manollas M, 2020)** "Efficient Deep CNN-BiLSTM Model for Network Intrusion Detection" **https://jaysinha.me/files/aipr_20_ids_paper_pre_print.pdf**
18. **(YUMNA ZAHID , MUHAMMAD ATIF TAHIR , NOUMAN M. DURRANI 1 , AND AHMED BOURIDANE, 2020)** "IBaggedFCNet: An Ensemble Framework for Anomaly Detection in Surveillance Videos" https://ieeexplore.ieee.org/document/9279251
19. **(HUI JIANG 1, ZHENG HE 2,3, GANG YE 2,3, AND HUYIN ZHANG 1, 23 Mar 2020)** "Network Intrusion Detection Based on PSO -Xgboost Model" **https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9044370**
20. (**R. Vinayakumar1, Mamoun Alazab2, K. P. Soman1, Prabaharan Poornachandran1 more•Institutions, 03 Apr 2019)** "Deep Learning Approach for Intelligent Intrusion Detection System" https://rspsciencehub.com/article_9838_a9e66ea96a3dc68afa18be503169f925.pdf

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206099 |

21. **(Hamed Sarvari∗ Carlotta Domeniconi† Bardh Prenkaj‡ Giovanni Stilo•Institutions (3)22 Oct 2019)** "Unsupervised Boosting-Based Autoencoder Ensembles for Outlier Detection" **https://arxiv.org/pdf/1910.09754.pdf**
22. **(Ansam Khraisat , Iqbal Gondal, Peter Vamplew and Joarder Kamruzzaman, 2019)** "A Novel Ensemble of Hybrid Intrusion Detection System for Detecting Internet of Things Attacks" **https://doi.org/10.3390/electronics8111210**
23. **(Hamoud Alshammari, Karim Gasmi, Moez Krichen, Lassaad Ben Ammar +3 more 14 Mar 2022)- Wireless Communications and Mobile Computing** "Optimal Deep Learning Model for Olive Disease Diagnosis Based on an Adaptive Genetic Algorithm" https://doi.org/10.1155/2022/8531213
24. **(Neelesh Mungoli 04 Apr 2023)** "Adaptive Ensemble Learning: Boosting Model Performance through Intelligent Feature Fusion in Deep Neural Networks" https://doi.org/10.48550/arXiv.2304.02653
25. **(Sai Saketh Rambhatla, Michael Jones, Rama Chellappa 28 Jul 2021)** "To Boost or not to Boost: On the Limits of Boosted Neural Networks." https://doi.org/10.48550/arXiv.2107.13600
26. **(Hamed Sarvari∗ Carlotta Domeniconi† Bardh Prenkaj‡ Giovanni Stilo•Institutions (3)22 Oct 2019)** "Unsupervised Boosting-Based Autoencoder Ensembles for Outlier Detection" **https://doi.org/10.48550/arXiv.1910.09754**
27. **(C. Narmadha1 , R. Muthuselvi2 , P. Somasundari3 , G. Sivagurunathan4 , Malini K V5 , Sathishkannan6, 30 April 2023)** "Cloud-based Detection of Malware and Software Privacy Threats in Internet of Things using Deep Learning Approach" https://doi.org/10.14445/23488549/IJECE-V10I4P103

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details