INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 10, October 2023, pp : 89-94

e-ISSN : 2583-1062

Impact Factor : 5.725

A DEEP LEARNING FRAMEWORK AND ALGORITHMS FOR AUTOMATIC CYBER ATTACKS DETECTION

Rathod Maheshwar[1], Dr. Mahesh Kandakatla[2]

[1]Research Scholar, Department Of CSE, Chaitanya Deemed to Be University, Hanamkonda, India.

[2]Assistant Professor, Department Of CSE, Chaitanya Deemed to Be University, Hanamkonda, India.

DOI: https://www.doi.org/10.58257/IJPREMS32114

ABSTRACT

Cybersecurity in the digital age faces increasing challenges posed by novel and adaptive cyber threats. Traditional Intrusion Detection Systems (IDS) struggle to keep pace with evolving attack vectors. To address this issue, our research presents a comprehensive framework that leverages deep learning and federated learning principles for cyber attack detection. Our primary objective is the development of an integrated model capable of efficiently detecting a wide range of cyber threats while preserving data privacy. We rigorously evaluate the framework's performance, emphasizing accuracy, scalability, and adaptability. Despite challenges such as data privacy constraints and computational demands, the potential applications of our research span across critical sectors, including IoT security, cloud platforms, financial institutions, government agencies, healthcare, e-commerce, and education. This research aims to significantly advance cyberattack detection capabilities in an ever-changing digital landscape.

Keywords: Cybersecurity. Deep Learning, Federated Learning

1. INTRODCUTION

The advent of the digital age has brought about unparalleled convenience and efficiency in numerous sectors, from business to communication. However, this increased connectivity and dependence on digital platforms also present a ripe opportunity for cyber threats. Cyberattacks have evolved in sophistication and frequency, causing immense financial, reputational, and operational repercussions [1].

Traditional Intrusion Detection Systems (IDS), which primarily rely on signature-based and heuristic-based methods, have shown limitations in detecting novel and adaptive attacks [2]. Their static nature makes it challenging to identify zero-day vulnerabilities and adaptive threats that can mutate or vary their patterns to evade detection [3].

In recent years, deep learning, a subset of machine learning, has garnered attention for its capacity to learn complex patterns and representations from vast amounts of data [4]. Its application in the realm of cyber security promises a more dynamic, adaptive, and effective detection mechanism. Preliminary studies have already demonstrated the efficacy of deep learning models, such as Convolution Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), in outperforming traditional IDS in certain scenarios [5].

This research seeks to explore and develop a comprehensive deep learning framework tailored for cyber attack detection, aiming to bridge the gap between advanced attack vectors and existing defense mechanisms.

2. RELATEDWORKS

Recent research has witnessed a growing interest in the fusion of deep learning and federated learning methodologies to bolster cyberattack detection systems. A pioneering work by McMahan et al. introduced the concept of communication-efficient learning from decentralized data, laying the foundation for federated learning [1]. Weiss et al. highlighted the transformative potential of deep learning in cybersecurity, illuminating the path towards combining it with federated learning for enhanced security measures [2]. The study by Ranshous et al. ventured into privacy-centric cybersecurity for IoT, addressing data privacy concerns in federated learning setups [3]. Moreover, Chen et al. explored secure and privacy-preserving federated learning, demonstrating its applicability to cybersecurity in diverse domains [4]. Additionally, investigations by He et al. and Liu et al. underscored the significance of federated learning in edge networks and mobile sensing, domains intrinsically linked to real-time cyberattack detection [5] [6]. These seminal works collectively underscore the promising convergence of deep learning and federated learning in fortifying the cybersecurity landscape.

3. MOTIVATION

We live in an interconnected digital era, where the boundaries of communication and commerce have expanded exponentially through the web. The wonders of this digital age, however, come with their own set of challenges. With an increasing amount of data being exchanged online every moment, the digital realm has become a prime target for malicious activities. Cyber attacks, which once were rare occurrences, have now become a frequent menace, threatening not only businesses but also individual users.

Traditional cybersecurity measures, predominantly the signature-based intrusion detection systems, operate on recognizing known threats. In essence, they are always a step behind, often ineffective against novel and uncharted cyber threats. The digital world's ever-evolving nature demands defenses that are not merely reactive but are also proactive, capable of anticipating and adapting to new kinds of threats.

Herein lies the motivation for this research. The dynamism and adaptability offered by deep learning present an opportunity to revamp our cybersecurity measures. Modeled after human brain workings, deep learning can sift through vast datasets, understand complex patterns, and crucially, evolve with new data. The potential to create a cybersecurity system that not only detects but also learns from these detections offers a promising avenue to safeguard our digital future.

4. STATEMENT OF THE PROBLEM

The rapid growth of the digital realm has brought about unparalleled advancements and opportunities in various sectors. However, it has concurrently given rise to an increasing number of cyber threats. These malicious threats not only have the potential to compromise sensitive information but can also disrupt the very infrastructure of digital ecosystems. Traditional cyber security mechanisms, especially signature-based intrusion detection systems, primarily identify known threats, leaving systems vulnerable to novel attack vectors.

The existing state of intrusion detection struggles to adapt to the dynamism of evolving cyber threats. While numerous measures can identify and counter known threats, the challenge lies in preemptively recognizing and mitigating novel cyber attacks that don't follow recognizable patterns. There's a dire need for a cyber security solution that not only reacts to threats but learns, adapts, and proactively defends against them.

The problem, therefore, is two-points:

1. The inadequacy of current intrusion detection systems in recognizing and defending against novel and evolving cyber threats.
2. The absence of a dynamic, learning-driven approach in cybersecurity that can anticipate and adapt to new attack vectors, ensuring robust protection in an ever-changing digital landscape.

5. RESEARCH GAPS

From the literature review significant research gaps were identified.

- As discussed in [1], [5], [6], [7], feature engineering plays crucial role in improving training for anomaly detection. There was need for proposing novel pre-processing and leveraging feature selection to improve anomaly detection performance towards cyber security.
- Literature insights, as discussed in [3], [8] and [10] also advocate the need for ensemble approach to improve attack detection performance. Ensemble of best performing models is a desired solution for leveraging intrusion detection performance.
- As discussed in [1], [3] and [5], with the emergence of advancements in neural networks and their capabilities, an important research gap is to explore deep learning techniques for improving anomaly detection research.

6. AIM AND OBJECTIVES

OBJECTIVES:

6.1. PRIMARY OBJECTIVE:

1. **Unified Development**: To develop a cohesive framework that seamlessly merges deep learning and federated learning principles, designed specifically for cyberattack detection.
2. **Performance Evaluation**: To rigorously assess the effectiveness of the combined deep learning and federated learning approach in detecting a wide range of cyber threats, using distributed data sources.
3. **Adaptive Optimization**: To iteratively refine the integrated deep and federated learning algorithms, focusing on enhancing real-time response, accuracy, and scalability in diverse environments.

6.2. SECONDARY OBJECTIVES:

1. **Decentralized Data Handling**: To establish efficient protocols for handling decentralized data across multiple nodes, optimizing for speed and reliability while preserving user privacy.
2. **Model Robustness**: To test the resilience and robustness of the model against adversarial attacks, ensuring its reliability in challenging scenarios.
3. **Resource Efficiency**: To optimize the computational and communication overheads associated with federated learning processes, ensuring that the system is both effective and efficient for practical deployment.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 10, October 2023, pp : 89-94

e-ISSN : 2583-1062

Impact Factor : 5.725

7. METHODOLOGY:

1. **Literature Review and Gap Identification**:
- Review existing research on deep learning and federated learning in the context of cybersecurity.
- Identify gaps and areas of improvement in current methodologies.
2. **Data Acquisition**:
- Collect datasets representative of various cyber threats. This can be from public repositories or simulated network environments.
- Pre-process the data, ensuring it's suitable for both deep learning and federated learning contexts.
3. **Model Design**:
- Design deep learning architectures suitable for cyberattack detection. Consider architectures like Convolutional Neural Networks (CNN) for pattern recognition or Recurrent Neural Networks (RNN) for sequential data.
- Incorporate federated learning principles, allowing the model to learn from decentralized data sources.
4. **Data Partitioning**:
- Emulate a federated environment by partitioning data across multiple simulated nodes. This is to mimic real-world scenarios where data might be scattered across different locations or devices.
5. **Training and Validation**:
- Implement federated training procedures, ensuring each node trains the model locally.
- Aggregate model updates from each node centrally and then distribute the updated model back to each node, iterating this process until convergence.
- Validate the performance of the model using a separate dataset, assessing its accuracy, recall, precision, and other relevant metrics.
6. **Optimization**:
- Fine-tune the model, addressing issues like overfitting or underfitting.
- Optimize communication and computational costs associated with federated learning processes.
7. **Robustness Testing**:
- Expose the model to adversarial attacks to test its resilience.
- Incorporate any necessary defenses or modifications to increase its robustness.
8. **Evaluation**:
- Benchmark the combined deep learning and federated learning model against traditional intrusion detection systems.
- Analyze the trade-offs in terms of accuracy, privacy preservation, computational costs, and communication overheads.

8. SCOPE AND LIMITATION

This research embarks on a comprehensive exploration of the integration of deep learning and federated learning techniques for enhancing the field of cyberattack detection. The scope encompasses the design and development of sophisticated deep learning models capable of detecting cyberattacks across diverse network environments. The study will seamlessly integrate federated learning principles, allowing decentralized learning from various data sources while safeguarding data privacy and security. Performance evaluation will be rigorous, considering accuracy, false positive rates, scalability, and adaptability to evolving threats. Attention will be given to the practical feasibility of deploying the framework in real-world cyber security scenarios. Nevertheless, limitations exist. Data availability, constrained by privacy regulations and access constraints, may impact model effectiveness. Computational demands and communication overheads could affect scalability and efficiency, particularly in low-bandwidth settings. Achieving full data privacy in federated learning remains a challenge, and complex model interpretability within the federated context may pose difficulties. Despite these limitations, this research aspires to advance cyberattack detection by leveraging the synergy of deep and federated learning while acknowledging and addressing associated challenges.'

9. APPLICATIONS OF RESEARCH

Given the integrated approach of research, combining feature selection, deep learning, and Explainable AI for intrusion detection, the potential applications are vast and pivotal in today's digitally connected world:

Cyber security Solutions:

research can provide the foundation for next-generation Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), which can be deployed in enterprise networks to safeguard against malicious activities.

IoT Security:

With the proliferation of Internet of Things (IoT) devices, there's an increased risk of cyber attacks. Model can be tailored to secure IoT networks, ensuring the safety of smart homes, wearable's, and other connected devices.

Cloud Security:

Cloud platforms, being a common target due to the vast amount of data they store, can benefit from research by implementing your model to detect and prevent intrusions.

Financial Institutions:

Banks and other financial entities can employ novel model to protect their digital infrastructure, ensuring the safety of financial transactions and sensitive customer data.

Government and Defense:

National cyber security agencies can use my research to safeguard critical infrastructure and state secrets, thereby bolstering national security.

Healthcare:

With the digitization of health records and telemedicine, the healthcare sector can integrate my system to protect patient data and ensure the confidentiality and integrity of medical records.

E-commerce Platforms:

Online shopping portals can deploy nvel model to ensure secure transactions and safeguard user data against potential breaches.

Educational Platforms:

Online learning platforms and universities can adopt novel intrusion detection system to protect academic data and intellectual property.

Development of Security Tools:

Cyber security firms can utilize your research findings to develop commercial security software and tools, catering to various sectors and needs.

10. CONCLUSTION

This research combines deep learning and federated learning to create a powerful cybersecurity system. This system can detect a wide range of cyber threats effectively. While there are some technical challenges to overcome, the potential applications in various sectors are significant, making our research valuable for improving cyber security in the digital age.

11. REFERENCES

[1] H. B. McMahan et al., "Communication-Efficient Learning of Deep Networks from Decentralized Data," in Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS), 2017.

[2] G. M. Weiss et al., "Deep Learning for Cybersecurity," in IEEE Access, vol. 7, pp. 3861-3879, 2018.

[3] S. Ranshous et al., "Differentially Private Federated Learning for Improved Cybersecurity in IoT," in 2020 IEEE International Conference on Edge Computing (EDGE), 2020.

[4] M. Chen et al., "Secure and Privacy-Preserving Federated Learning for IoT-Based Healthcare," in IEEE Internet of Things Journal, vol. 7, no. 8, pp. 6954-6967, 2020.

[5] D. He et al., "Federated Learning in Mobile Edge Networks: A Comprehensive Survey," in IEEE Communications Surveys & Tutorials, vol. 23, no. 3, pp. 2265-2311, 2021.

[6] J. Liu et al., "Federated Learning: A Privacy-Preserving Collaborative Learning Framework for Mobile Sensing," in IEEE Transactions on Big Data, vol. 6, no. 3, pp. 418-433, 2020.

[7] Vellela, S. S., Balamanigandan, R., & Praveen, S. P. (2022). Strategic Survey on Security and Privacy Methods of Cloud Computing Environment. Journal of Next Generation Technology, 2(1).

[8] Madhuri, A., Jyothi, V. E., Praveen, S. P., Sindhura, S., Srinivas, V. S., & Kumar, D. L. S. (2022). A New Multi-Level Semi-Supervised Learning Approach for Network Intrusion Detection System Based on the 'GOA'. Journal of Interconnection Networks, 2143047.

[9] Vellela, S. S., Reddy, B. V., Chaitanya, K. K., &Rao, M. V. (2023, January). An Integrated Approach to Improve E-Healthcare System using Dynamic Cloud Computing Platform. In 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 776-782). IEEE.

[10] S Phani Praveen, Rajeswari Nakka, Anuradha Chokka, Venkata Nagaraju Thatha, Sai Srinivas Vellela and Uddagiri Sirisha, "A Novel Classification Approach for Grape Leaf Disease Detection Based on Different Attention Deep Learning Techniques" International Journal of Advanced Computer Science and Applications (IJACSA), 14(6), 2023. http://dx.doi.org/10.14569/IJACSA.2023.01406128

[11] Praveen, S. P., Sarala, P., Kumar, T. K. M., Manuri, S. G., Srinivas, V. S., &Swapna, D. (2022, November). An Adaptive Load Balancing Technique for Multi SDN Controllers. In 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) (pp. 1403-1409). IEEE.

[12] Vellela, S. S., BashaSk, K., &Yakubreddy, K. (2023). Cloud-hosted concept-hierarchy flex-based infringement checking system. International Advanced Research Journal in Science, Engineering and Technology, 10(3).

[13] Sk, K. B., Roja, D., Priya, S. S., Dalavi, L., Vellela, S. S., & Reddy, V. (2023, March). Coronary Heart Disease Prediction and Classification using Hybrid Machine Learning Algorithms. In 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA) (pp. 1-7). IEEE.

[14] Venkateswara Rao, M., Vellela, S., Reddy, V., Vullam, N., Sk, K. B., &Roja, D. (2023, March). Credit Investigation and Comprehensive Risk Management System based Big Data Analytics in Commercial Banking. In 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS) (Vol. 1, pp. 2387-2391). IEEE.

[15] Vellela, S.S., Balamanigandan, R. Optimized clustering routing framework to maintain the optimal energy status in the wsn mobile cloud environment. Multimed Tools Appl (2023). https://doi.org/10.1007/s11042-023- 15926-5

[16] Vullam, N., Vellela, S. S., Reddy, V., Rao, M. V., SK, K. B., &Roja, D. (2023, May). Multi-Agent Personalized Recommendation System in E-Commerce based on User. In 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC) (pp. 1194-1199). IEEE.

[17] Rao, K. N., Gandhi, B. R., Rao, M. V., Javvadi, S., Vellela, S. S., & Basha, S. K. (2023, June). Prediction and Classification of Alzheimer's Disease using Machine Learning Techniques in 3D MR Images. In 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS) (pp. 85-90). IEEE.

[18] Rao, D. M. V., Vellela, S. S., Sk, K. B., & Dalavai, L. (2023). Stematic Review on Software Application Under-distributed Denial of Service Attacks for Group Website. Dogo Rangsang Research Journal, UGC Care Group I Journal, 13.

[19] Venkateswara Reddy, B., &Khader BashaSk, R. D. Qos-Aware Video Streaming Based Admission Control And Scheduling For Video Transcoding In Cloud Computing. In International Conference on Automation, Computing and Renewable Systems (ICACRS 2022).

[20] Madhuri, A., Praveen, S. P., Kumar, D. L. S., Sindhura, S., &Vellela, S. S. (2021). Challenges and issues of data analytics in emerging scenarios for big data, cloud and image mining. Annals of the Romanian Society for Cell Biology, 412-423.

[21] Vellela, S. S., Balamanigandan, R., & Praveen, S. P. (2022). Strategic Survey on Security and Privacy Methods of Cloud Computing Environment. Journal of Next Generation Technology (ISSN: 2583- 021X), 2(1).

[22] Venkateswara Reddy, B., Vellela, S. S., Sk, K. B., Roja, D., Yakubreddy, K., & Rao, M. V. Conceptual Hierarchies for Efficient Query Results Navigation. International Journal of All Research Education and Scientific Methods (IJARESM), ISSN, 2455-6211.

[23] Sk, K. B., Vellela, S. S., Yakubreddy, K., & Rao, M. V. (2023). Novel and Secure Protocol for Trusted Wireless Ad-hoc Network Creation. Khader Basha Sk, Venkateswara Reddy B, Sai Srinivas Vellela, Kancharakunt Yakub Reddy, M Venkateswara Rao, Novel and Secure Protocol for Trusted Wireless Ad-hoc Network Creation, 10(3).

[24] Sk, K. B., & Vellela, S. S. (2019). Diamond Search by Using Block Matching Algorithm. DIAMOND SEARCH BY USING BLOCK MATCHING ALGORITHM", International Journal of Emerging Technologies and Innovative Research (www. jetir. org), ISSN, 2349-5162.

[25] S. S. Priya, S. Srinivas Vellela, V. R. B, S. Javvadi, K. B. Sk and R. D, "Design And Implementation of An Integrated IOT Blockchain Framework for Drone Communication," 2023 3rd International Conference on Intelligent Technologies (CONIT), Hubli, India, 2023, pp. 1-5, doi: 10.1109/CONIT59222.2023.10205659.

[26] N. Vullam, K. Yakubreddy, S. S. Vellela, K. Basha Sk, V. R. B and S. Santhi Priya, "Prediction And Analysis Using A Hybrid Model For Stock Market," 2023 3rd International Conference on Intelligent Technologies (CONIT), Hubli, India, 2023, pp. 1-5, doi: 10.1109/CONIT59222.2023.10205638.

[27] Vellela, S. S., & Krishna, A. M. (2020). On Board Artificial Intelligence With Service Aggregation for Edge Computing in Industrial Applications. Journal of Critical Reviews, 7(07).

[28] Babu, G. B., Gopal, M. V., Srinivas, V. S., & Krishna, V. Efficient Key Generation for Multicast Groups Based on Secret Sharing.

[29] Yakubreddy, K., Vellela, S. S., Sk, K. B., Reddy, V., & Roja, D. (2023). Grape CS-ML Database-Informed Methods for Contemporary Vineyard Management. International Research Journal of Modernization in Engineering Technology and Science, 5(03).

[30] Vellela, Sai Srinivas and Chaganti, Aswini and Gadde, Srimadhuri and Bachina, Padmapriya and Karre, Rohiwalter, A Novel Approach for Detecting Automated Spammers in Twitter (June 7, 2022). Mukt Shabd Journal Volume XI, Issue VI, JUNE/2022 ISSN NO : 2347-3150, pp. 49-53 , Available at SSRN: https://ssrn.com/abstract=4490635

[31] Vellela, S. S., Roja, D., Reddy, V., Sk, K. B., & Rao, M. V. (2023). A New Computer-Based Brain Fingerprinting Technology. Vellela, S. S., Sk, K. B., & Reddy, V. (2023). Cryonics on the Way to Raising the Dead Using Nanotechnology.

[32] Vellela, Sai Srinivas and Basha Sk, Khader and B, Venkateswara Reddy and D, Roja and Javvadi, Sravanthi, MOBILE RFID APPLICATIONS IN LOCATION BASED SERVICES ZONE (June 14, 2023). International Journal of Emerging Technologies and Innovative Research, Vol.10, Issue 6, page no. ppd851-d859, June-2023, http://www.jetir.org/papers/JETIR2306410.pdf, Available at SSRN: https://ssrn.com/abstract=4478104

[33] Dalavai, L., Javvadi, S., Sk, K. B., Vellela, S. S., & Vullam, N. (2023). Computerised Image Processing and Pattern Recognition by Using Machine Algorithms.

[34] Vellela, Sai Srinivas and Pushpalatha, D and Sarathkumar, G and Kavitha, C.H. and Harshithkumar, D, Advanced Intelligence Health Insurance Cost Prediction Using Random Forest (March 1, 2023). ZKG International, Volume VIII Issue I MARCH 2023, Available at SSRN: https://ssrn.com/abstract=4473700

[35] Vellela, Sai Srinivas and Narapasetty, Suma and Somepalli, Mahendra and Merikapudi, Venkateswarlu and Pathuri, Sandeep, Fake News Articles Classifying Using Natural Language Processing to Identify in-article Attribution as a Supervised Learning Estimator (June 10, 2022). Mukt Shabd Journal, Volume XI, Issue VI, JUNE/2022, Available at SSRN: https://ssrn.com/abstract=4473702

[36] Vellela, Sai Srinivas and B, Venkateswara Reddy and Sk, Khader Basha, Detection Of Spammers And Fake User Identification In Social Networks (2016). IJCRT | Volume 4, Issue 4 November 2016, Available at SSRN: https://ssrn.com/abstract=4531199

[37] Sai Srinivas Vellela,Khader Basha Sk,Venkateswara Reddy B, "Skin Diseases Detection and Classification using Deep Learning Algorithm Convolutional Neural Network", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.5, Issue 3, pp.177-181, September 2017, Available at :http://www.ijcrt.org/papers/IJCRT1135177.pdf

[38] "A Blood Cell Classification Using a Deep Learning Algorithm CNN", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.5, Issue 2, page no.258-263, February-2018, Available :http://www.jetir.org/papers/JETIR1802339.pdf

[39] Reddy, N.V.R.S., Chitteti, C., Yesupadam, S., Desanamukula, V.S., Vellela, S.S., Bommagani, N.J. (2023). Enhanced speckle noise reduction in breast cancer ultrasound imagery using a hybrid deep learning model. Ingénierie des Systèmes d'Information, Vol. 28, No. 4, pp. 1063-1071. https://doi.org/10.18280/isi.280426

[40] Vellela, S.S., Balamanigandan, R. An intelligent sleep-awake energy management system for wireless sensor network. Peer-to-Peer Netw. Appl. (2023). https://doi.org/10.1007/s12083-023-01558-x