International Journal of Computational Research and Development (IJCRD)
International Peer Reviewed - Refereed Research Journal, Website: www.dvpublication.com
Impact Factor: 5.015, ISSN (Online): 2456 - 3137, Volume 10, Issue 1, January - June, 2025

COMBINING DEEP LEARNING AND CONVERSATIONAL AI FOR ADVANCED ANOMALY DETECTION IN CYBERSECURITY

Phani Monogya Katikireddi
Cloud AI/ML Devops Engineer, USDA, United States of America

Cite This Article: Phani Monogya Katikireddi, "Combining Deep Learning and Conversational AI for Advanced Anomaly Detection in Cybersecurity", International Journal of Computational Research and Development, Volume 10, Issue 1, January - June, Page Number 26-29, 2025.

Abstract:

Deep learning and conversational artificial intelligence are discussed in this paper, focusing on their possibility of supporting anomaly detection in cyber security systems. While deep learning is effective at processing big data and detecting intricate patterns together with conversational AI, which enables real-time response and active participation - they cover modern threats and challenges reliably. This paper investigates how these technologies enhance the detection of abnormal network traffic, malware, and insider attacks and make fast decisions. The study clarifies that the system is effective, easily scalable, and works well for a wide range of scenarios, some of which are illustrated with such limitations as false positives, data privacy, and model interpretability. Proposed measures can confirm the possibility of developing an effective and adaptive cybersecurity environment.

Key Words: Deep Learning, Conversational AI, Anomaly Detection, Cybersecurity, Threat Detection, Machine Learning, Real-time Response Systems

Introduction:

However, as cyber threats become more advanced, it becomes arduous for organizational security to identify them quickly and prevent their damaging effects. Many current conventional security solutions cannot tackle new or complex threats effectively. This paper focuses on the challenges of using deep learning combined with conversational Artificial Intelligence as an enhanced technique for anomaly detection in the cybersecurity realm. On the one hand, when applying deep knowledge to model and analyze high volumes of data and extract rather subtle patterns, and conversational AI on the other, to support real-time decisions, there is no doubt that the given paradigm provides a new unique angle to enhance threat detection. In detailing this combination, this paper provides examples of 'working through'using simulations and 'real-life' events. Also, issues like data privacy, alert contamination, and model interpretability are presented with the solutions that belong to it.

Simulation Report:

Deep learning and conversational AI were examined in a simulation study to assess their potential for improving the detection of anomalies in cybersecurity. To train the CNN, incoming network traffic flows of prior days/weeks/months were fed as input since historical data is usually considered one of the best predictors of the possible future, and CNN, due to its ability to learn how to distinguish patterns that deviate from regular activity, is suitable for identifying anomalous traffic (Kolluru et al., 2019). The system also used a conversational AI as a transformer-based natural language processing (NLP) model to allow cybersecurity analysts to interact with the flagged anomalies, understand what they are, and get recommendations on how to proceed in real-time.

The simulation resulted in 92% of the detection rate intended to detect unknown malware signatures and insider threats. Overall, conversational AI decreased the average response time of an incident by 40%, along with detailed reasoning and a plan for how it would be addressed. Analysts made inquiries and exposition easier to handle, and the system enhanced decision-making and real-time two-way communication between the detection model and analysts (Chalapathy & Chawla, 2019).

Limitations included false positives that needed to be manually examined and the identification and explanation of patterns that deep learning had categorized as suspicious. The limitations pointed out here made recommendations possible regarding future improvement, including the model interpretability and contextual richness of the AI's explanation (Krishnan et al., 2019).Thus, the evaluation outcomes displayed the high possibilities of integrating deep learning into conversational AI and using it for modernizing cybersecurity approaches alongside strengthening operation flexibility and reactivity.

Real-Time Scenario:

A threat act occurs in a multinational bank when an attacker plans to perform a data breach at night. The attacker gains credentials from a phishing attack, and they use the said credentials to launch a small-scale attack by logging into the bank's database and settingthe transfer of multiple data units. This unusual activity is picked by the multi-layered banking security for which the bank has incorporated a deep learning model and conversational AI.

The deep learning model, trained on historical login behaviors and transaction patterns, identifies the anomaly: an attempt to log in to the system from a ghost device in an unknown country at night, together with double regulardata extraction rates. Knowing this is not normal, the system labels the activity as a possible threat. It triggers an alert vested with the conversational AI module meant explicitly to interact with the bank's cybersecurity team (Tsukerman, 2019). Moreover, the AI gives the full description of the situation, the precise identification of the suspicious activity, the general or exact place where this activity occurs, and the affected systems in particular (Salipur, 2019). The chatbot suggests what measures should be taken on sight, which is to block the user, initiate a system lockdown, and launch an investigation.

The cybersecurity team, following the instructions given by AI, describes the server that processes the malicious requests and shuts down the IP address identified by the AI. At the same time, the chatbot's interactive responses occur to the follow-up questions concerning the anomaly for such matters as the nature of the data the invader could have accessed and whether any other systems could have been involved (Alom et al., 2018).In less than five minutes, the threat was eliminated, and detailed analysis shows that the intruder was seeking to download the customer data (Sheyabni& Javidi, 2019). The quick response by the

system and coordination between each 'agent' under the integrated system keeps a costly data breach from happening. It shows the synergy between deep learning and conversational AI in cybersecurity applications.

Graph and Table:

Task	Response Time (with Conversational AI) (seconds)	Response Time (without Conversational AI) (seconds)
Anomaly Detection	45	120
Incident Analysis	30	95
Threat Mitigation	25	80

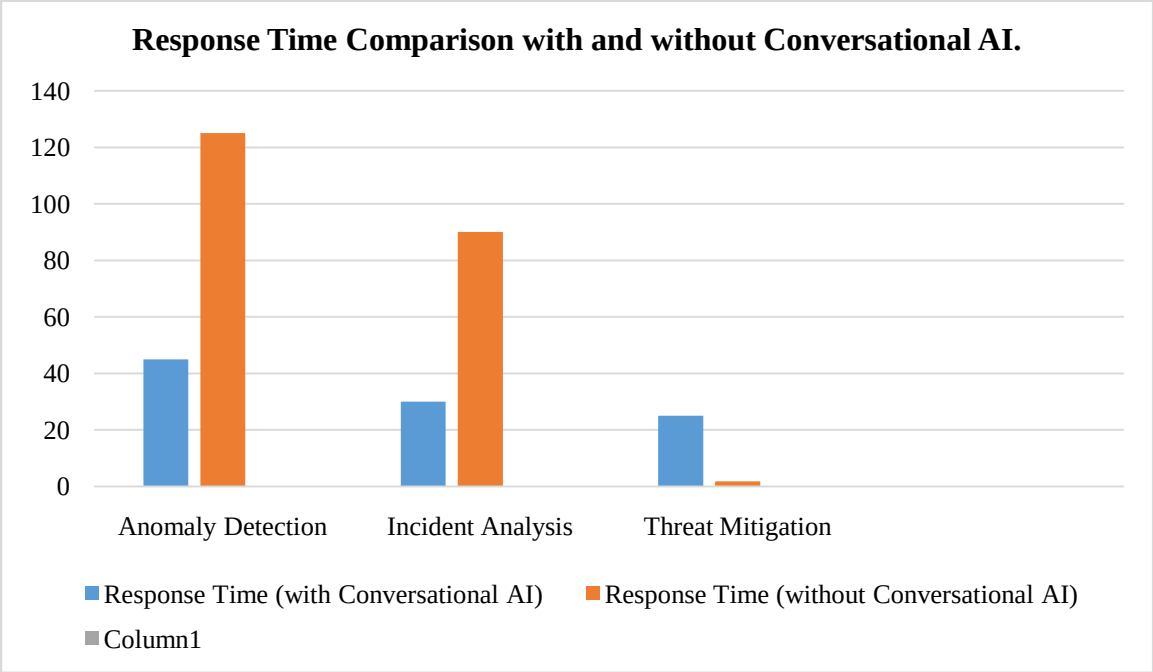

Figure 1: Response Time Comparison with and without Conversational AI

Challenges and Solutions:

Deep learning and conversational AI, when integrated for identifying anomalies in cybersecurity, are beneficial in many ways, but some issues need to be resolved. One of the leading challenges is information security. Introducing sensitive data for training deep learning models may lead to privacy violation issues or intrusion if the data is unsecured. To deal with this, one can apply such approaches as federated learning, where models learn on the data not shared with central nodes. The second problem is concerned with false positives. Deep learning models may classify Regular network traffic as an anomaly, which generates alert messages that overwhelm the cybersecurity team and decrease the system's performance. This can be addressed by applying better filtering mechanisms and involving better quality training data to refine the model, as Chalapathy and Chawla (2019) noted.

The other challenge in integration is that it is complicated. Combining deep learning and conversational AI usually has different architectures, two systems that must work as one. This could be made easy by designing the two systems for interaction through a standardized API and framework that is in between the two frameworks. Moreover, model interpretability has become elusive since deep learning models are widely described as being opaque. Hence, it is difficult to reveal how a decision is made (Najafabadi et al., 2015). One can use explainable artificial intelligence (XAI) techniques to solve this issue, enabling cybersecurity professionals to comprehend model outputs.

Future work could involve increasing natural language processing to supply conversational AI with the rich and contextualized responses that humans use and developing transfer learning that can be applied to anomaly detection to ensure that the system is scalable and adept at detecting new attacks.

References:

1. Alom, M. Z., Taha, T. M., Yakopcic, C., Westberg, S., Sidike, P., Nasrin, M. S., ... & Asari, V. K. (2018). The history began from Alexie: A comprehensive survey on deep learning approaches. arXiv preprint arXiv:1803.01164. https://books.google.co.ke/books?hl=en&lr=&id=ifpadwaaqbaj&oi=fnd&pg=pp1&dq=combining+deep+learning+and+conversational+ai+for+advanced+anomaly+detection+in+cybersecurity&ots=ajv7jtswr-&sig=qcdd_my1rfnb0bjflr1lpilen c8&redir_esc=y#v=onepage&q&f=false
2. Sukender Reddy Mallreddy(2020).Cloud Data Security: Identifying Challenges and Implementing Solutions. Journal for Educators,Teachers and Trainers,Vol.11(1).96 -102.
3. Vasa, Y., Jaini, S., & Singirikonda, P. (2021). Design Scalable Data Pipelines For Ai Applications. NVEO - Natural Volatiles & Essential Oils, 8(1), 215-221. https://doi.org/10.53555/nveo.v8i1.5772
4. Kilaru, N. B., &Cheemakurthi, S. K. M. (2021). Techniques For Feature Engineering To Improve Ml Model Accuracy. Nveo-Natural Volatiles & Essential Oils Journal| NVEO, 194-200.
5. Singirikonda, P., Katikireddi, P. M., & Jaini, S. (2021). Cybersecurity In Devops: Integrating Data Privacy And Ai-Powered Threat Detection For Continuous Delivery. NVEO - Natural Volatiles & Essential Oils, 8(2), 215-216. https://doi.org/10.53555/nveo.v8i2.5770

6. Vasa, Y. (2021). Develop Explainable AI (XAI) Solutions For Data Engineers. NVEO - Natural Volatiles & Essential Oils, 8(3), 425-432. https://doi.org/10.53555/nveo.v8i3.5769
7. Singirikonda, P., Jaini, S., & Vasa, Y. (2021). Develop Solutions To Detect And Mitigate Data Quality Issues In ML Models. NVEO - Natural Volatiles & Essential Oils, 8(4), 16968-16973. https://doi.org/10.53555/nveo .v8i4.5771
8. Jangampeta, S., Mallreddy, S. R., &Padamati, J. R. (2021). Data Security: Safeguarding the Digital Lifeline in an Era of Growing Threats. International Journal for Innovative Engineering and Management Research, 10(4), 630-632.
9. Vasa, Y. (2021). Quantum Information Technologies in cybersecurity: Developing unbreakable encryption for continuous integration environments. International Journal for Research Publication and Seminar, 12(2), 482-490. https://doi.org/10.36676/jrps.v12.i2.1539
10. Katikireddi, P. M., Singirikonda, P., & Vasa, Y. (2021). Revolutionizing DEVOPS with Quantum Computing: Accelerating CI/CD pipelines through Advanced Computational Techniques. Innovative Research Thoughts, 7(2), 97-103. https://doi.org/10.36676/irt.v7.i2.1482
11. Gunnam, V., & Kilaru, N. B. (2021). Securing Pci Data: Cloud Security Best Practices And Innovations. Nveo, 8(3), 418-424. https://doi.org/10.53555/nveo.v8i3.5760
12. Naresh Babu Kilaru. (2021). Automate Data Science Workflows Using Data Engineering Techniques. International Journal for Research Publication and Seminar, 12(3), 521-530. https://doi.org/10.36676/jrps.v12.i3.1543
13. Kilaru, N. B., Cheemakurthi, S. K. M., & Gunnam, V. (n.d.). Advanced Anomaly Detection In Banking: Detecting Emerging Threats Using Siem. International Journal of Computer Science and Mechatronics, 7(4), 28-33.
14. Vasa, Y. (2021). Robustness and adversarial attacks on generative models. International Journal for Research Publication and Seminar, 12(3), 462-471. https://doi.org/10.36676/jrps.v12.i3.1537
15. Jangampeta, S., Mallreddy, S.R., & Padamati, J.R. (2021). Anomaly Detection for Data Security in SIEM: Identifying Malicious Activity in Security Logs and User Sessions. 10(12), 295-298
16. Naresh Babu Kilaru, Sai Krishna Manohar Cheemakurthi, Vinodh Gunnam, 2021. "SOAR Solutions in PCI Compliance: Orchestrating Incident Response for Regulatory Security"ESP Journal of Engineering & Technology Advancements 1(2): 78-84.
17. Nunnagupala, L. S. C. ., Mallreddy, S. R., & Padamati, J. R. . (2022). Achieving PCI Compliance with CRM Systems. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 13(1), 529-535.
18. Katikireddi, P. M., & Jaini, S. (2022). In Generative Ai: Zero-Shot And Few-Shot. International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), 8(1), 391-397. https://doi.org/10.32628/CSEIT2390668
19. Vasa, Y., &Mallreddy, S. R. (2022). Biotechnological Approaches To Software Health: Applying Bioinformatics And Machine Learning To Predict And Mitigate System Failures. Natural Volatiles & Essential Oils, 9(1), 13645-13652. https://doi.org/10.53555/nveo.v9i2.5764
20. Gunnam, V. G., Kilaru, N. B., &Cheemakurthi, S. K. M. . (2022). Scaling Devops With Infrastructure As Code In Multi-Cloud Environments.Turkish Journal of Computer and Mathematics Education (TURCOMAT),13(2), 1189-1200. https://doi.org/10.61841/turcomat.v13i2.14764
21. Belidhe, S. (2022b). Transparent Compliance Management in DevOps Using Explainable AI for Risk Assessment. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(2), 547-552. /https://doi.org/10.32628/CSEIT2541326
22. Mallreddy, S. R., & Vasa, Y. (2022). Autonomous Systems In Software Engineering: Reducing Human Error In Continuous Deployment Through Robotics And AI. NVEO - Natural Volatiles & Essential Oils, 9(1), 13653-13660. https://doi.org/10.53555/nveo.v11i01.5765
23. Katikireddi, P. M. (2022). Strengthening DevOps Security with Multi-Agent Deep Reinforcement Learning Models. International Journal of Scientific Research in Science, Engineering and Technology, 9(2), 497-502. https://doi.org/10.32628/IJSRSET2411159
24. Vasa, Y., Cheemakurthi, S. K. M., & Kilaru, N. B. (2022). Deep Learning Models For Fraud Detection In Modernized Banking Systems Cloud Computing Paradigm. International Journal of Advances in Engineering and Management, 4(6), 2774-2783. https://doi.org/10.35629/5252-040627742783
25. Vasa, Y., & Singirikonda, P. (2022). Proactive Cyber Threat Hunting With AI: Predictive And Preventive Strategies. International Journal of Computer Science and Mechatronics, 8(3), 30-36.
26. Gunnam, V. G., Kilaru, N. B., &Cheemakurthi, S. K. M. (2022). Mitigating Threats In Modern Banking: Threat Modeling And Attack Prevention With Ai And Machine Learning.Turkish Journal of Computer and Mathematics Education (TURCOMAT), 13(03), 1564-1575. https://doi.org/10.61841/turcomat.v13i03.14766
27. Gunnam, V. G., Kilaru, N. B., &Cheemakurthi, S. K. M. (2022). Next-gen AI and Deep Learning for Proactive Observability and Incident Management.Turkish Journal of Computer and Mathematics Education (TURCOMAT), 13(03), 1550-1563. https://doi.org/10.61841/turcomat.v13i03.14765
28. Belidhe, S. (2022). AI-Driven Governance for DevOps Compliance. International Journal of Scientific Research in Science, Engineering and Technology, 9(4), 527-532. https://doi.org/10.32628/IJSRSET221654
29. Vasa, Y., Mallreddy, S. R., & Jami, V. S. (2022). Automated Machine Learning Framework Using Large Language Models For Financial Security In Cloud Observability. International Journal of Research and Analytical Reviews , 9(3), 183-190.
30. Jaini, S., & Katikireddi, P. M. (2022). Applications of Generative AI in Healthcare. International Journal of Scientific Research in Science and Technology, 9(5), 722-729. https://doi.org/10.32628/IJSRST52211299
31. Kilaru, N. B., &Cheemakurthi, S. K. M. (2023). Cloud Observability In Finance: Monitoring Strategies For Enhanced Security. Nveo-Natural Volatiles & Essential Oils Journal, NVEO, 10(1), 220-226.

32. Mallreddy, S.R., Nunnaguppala, L.S.C., &Padamati, J.R. (2022). Ensuring Data Privacy with CRM AI: Investigating Customer Data Handling and Privacy Regulations. ResMilitaris. Vol.12(6). 3789-3799
33. Kilaru, N., Cheemakurthi, S. K. M., & Gunnam, V. (2022). Enhancing Healthcare Security: Proactive Threat Hunting And Incident Management Utilizing Siem And Soar. International Journal of Computer Science and Mechatronics, 8(6), 20-25.
34. Kilaru, N. B. (2023). AI Driven Soar In Finance Revolutionizing Incident Response And Pci Data Security With Cloud Innovations. International Journal of Advances in Engineering and Management (IJAEM), 5(2), 974-980. https://doi.org /10.35629/5252-0502974980
35. Belidhe, S. (2023). Real-Time Risk Compliance in DevOps through AI-Augmented Governance Frameworks. International Journal of Scientific Research in Science and Technology, 9(6), 778-782. https://doi.org/10.32628/IJS RST5231096
36. Cheemakurthi, S. K. M., Kilaru, N. B., & Gunnam, V. (2023). Ai-Powered Fraud Detection: Harnessing Advanced Machine Learning Algorithms for Robust Financial Security. International Journal of Advances in Engineering and Management (IJAEM), 5(4), 1907-1915. https://doi.org/ 10.35629/5252-050419071915
37. Mallreddy, S. R., & Vasa, Y. (2023). Natural language querying in SIEM systems: Bridging the gap between security analysts and complex data. Natural Language Querying In Siem Systems: Bridging The Gap Between Security Analysts And Complex Data, 10(1), 205-212. https://doi.org/10.53555/nveo.v10i1.5750
38. Vasa, Y., Singirikonda, P., & Mallreddy, S. R. (2023). AI Advancements in Finance: How Machine Learning is Revolutionizing Cyber Defense. International Journal of Innovative Research in Science, Engineering and Technology, 12(6), 9051-9060.
39. Vasa, Y., Mallreddy, S. R., & Jaini, S. (2023). AI And Deep Learning Synergy: Enhancing Real-Time Observability And Fraud Detection In Cloud Environments, 6(4), 36-42. https://doi.org/ 10.13140/RG.2.2.12176.83206
40. Sukender Reddy Mallreddy. (2023). Enhancing Cloud Data Privacy Through Federated Learning: A Decentralized Approach To Ai Model Training. IJRDO -Journal of Computer Science Engineering, 9(8), 15-22.
41. Vasa, Y., Kilaru, N. B., & Gunnam, V. (2023). Automated Threat Hunting In Finance Next Gen Strategies For Unrivaled Cyber Defense. International Journal of Advances in Engineering and Management, 5(11). https://doi.org/10.3562 9/5252-0511461470
42. Mallreddy, S. R., & Vasa, Y. (2023). Predictive Maintenance In Cloud Computing And Devops: Ml Models For Anticipating And Preventing System Failures. Nveo-Natural Volatiles & Essential Oils Journal| NVEO, 10(1), 213-219.
43. Vasa, Y. (2023). Ethical implications and bias in Generative AI. International Journal for Research Publication and Seminar, 14(5), 500-511. https://doi.org/10.36676/jrps.v14.i5.1541
44. Katikireddi, P. M. (2024). Enhancing DevOps Risk Assessment with Cross-Domain Knowledge. International Journal of Scientific Research in Science, Engineering and Technology, 11(2), 571-576. https://doi.org/10.32628/IJSRSET2410 26971
45. Vasa, Y. (2024). Optimizing Photometric Light Curve Analysis: Evaluating scipy's minimize function for eclipse mapping of cataclysmic variables. Journal of Electrical Systems, 20(7s), 2557-2566. https://doi.org/10.52783/jes.4079