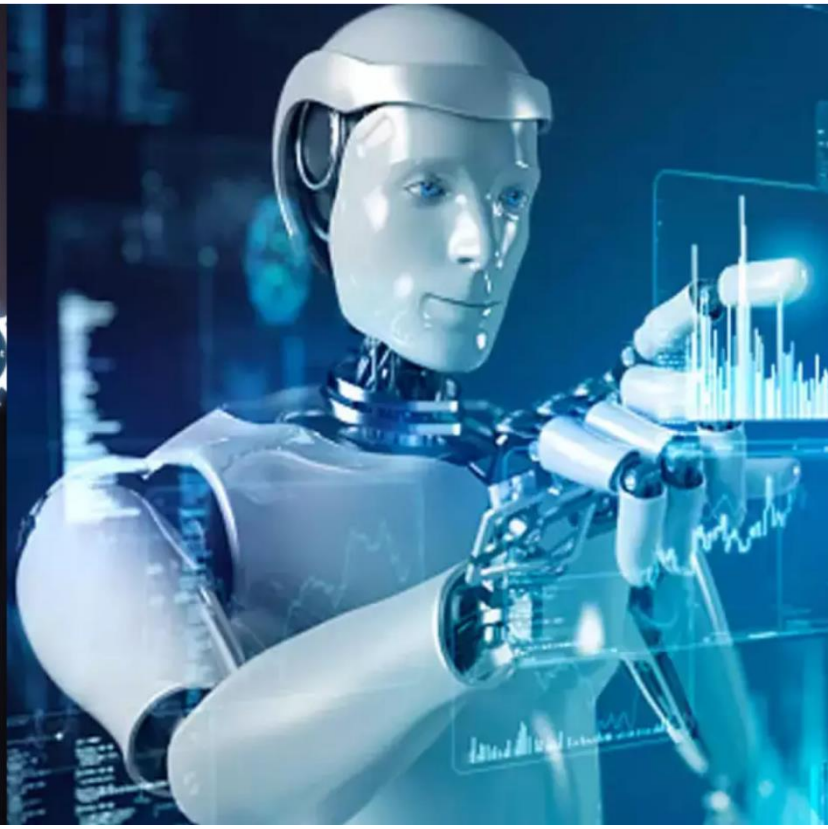
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 4, April 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404560|

AI Powered SOCs Detect and Respond to Cyber Security Threats in Real Time by using Deep Learning

Dr.K.V.Shiny, Kadari Rohith, Challa Bhargava Rami Reddy, Chitra Ganesh, Jakati Mabu

Professor, Department of CSE Bharath Institute of Higher Education and Research, Selaiyur, Chennai,

Tamil Nadu, India

B. Tech Student, Bharath Institute of Higher Education and Research, Selaiyur, Chennai, Tamil Nadu, India

ABSTRACT: The increasing complexity and volume of cyber threats necessitate a more advanced and proactive approach to cybersecurity. Traditional Security Operations Centers (SOCs) rely on rule-based systems and manual analysis, which are often insufficient to counter evolving attack vectors. Artificial Intelligence (AI), particularly Machine Learning (ML) and Blockchain technology, has emerged as a game-changer in enhancing SOC operations, improving threat detection, response, and mitigation capabilities. Machine Learning algorithms can analyze vast amounts of security data in real time, identifying anomalies and predicting potential threats with higher accuracy than conventional methods. ML-driven threat intelligence enables SOCs to detect zero-day attacks, automate incident response, and reduce false positives, thereby increasing operational efficiency. Additionally, AI-powered automation allows security analysts to focus on strategic threat mitigation rather than being overwhelmed by repetitive tasks. Blockchain technology further strengthens cybersecurity by providing an immutable, decentralized, and transparent framework for securing digital transactions and communications. Its application in SOC operations includes secure identity management, tamper-proof logging of security events, and decentralized threat intelligence sharing. By integrating blockchain with AI, SOCs can ensure data integrity, enhance collaboration across organizations, and reduce insider threats. This paper explores the synergy between AI, ML, and Blockchain in modern SOC environments. It discusses their combined potential to transform cybersecurity operations by enabling intelligent automation, realtime threat analysis, and secure data management. Furthermore, it highlights challenges such as computational overhead, integration complexity, and privacy concerns that must be addressed to maximize the benefits of these technologies.

KEYWORDS: AI, Machine Learning, Blockchain, Cybersecurity, SOC, Threat Detection, Automation, Data Integrity, Anomaly Detection, Incident Response

I. INTRODUCTION

The rapid digital transformation across industries has significantly increased the surface area for cyber threats, making cybersecurity a critical concern for organizations worldwide. Traditional Security Operations Centers (SOCs) are often overwhelmed by the sheer volume of cyber threats, requiring advanced solutions that can enhance efficiency and effectiveness. AI-powered cybersecurity, particularly through Machine Learning (ML) and Blockchain technology, has emerged as a revolutionary approach to strengthening SOC operations. Machine Learning enables SOCs to analyze vast amounts of security data, detect anomalies, and predict potential attacks with minimal human intervention. It enhances threat intelligence, automates incident response, and reduces false positives, allowing security analysts to focus on high-priority threats. Meanwhile, Blockchain technology provides a decentralized and immutable security framework, ensuring data integrity, secure identity management, and tamper-proof logging of security events. AI-driven threat detection systems leverage deep learning models to identify sophisticated cyberattacks, including zero-day vulnerabilities, malware, and phishing attempts. Additionally, blockchain's decentralized architecture minimizes risks associated with centralized data storage, reducing the chances of unauthorized access and data manipulation. As cyber threats become more advanced and complex, the fusion of AI, ML, and Blockchain in SOC operations is imperative to build a more resilient and proactive security infrastructure. This paper explores how these technologies work in synergy to enhance threat detection, response, and mitigation capabilities, offering a transformative shift in cybersecurity practices

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404560|

II. LITERATURE REVIEW

The modern cyber threat landscape is growing in both complexity and volume, making traditional Security Operations Centers (SOCs) increasingly insufficient. Artificial Intelligence (AI), particularly Deep Learning (DL), is transforming SOCs by enabling real-time threat detection and automated incident response. This survey explores existing research and applications of deep learning in AI-powered SOCs, highlighting their ability to detect and mitigate cyber threats in real-time.

III. METHODOLOGY

This research adopts a structured methodology to design and evaluate an AI-powered Security Operations Center (SOC) capable of detecting and responding to cyber threats in real time using deep learning techniques. The process begins with the collection of relevant cybersecurity datasets, including publicly available sources such as NSL-KDD, CICIDS2017, UNSW-NB15, and TON_IoT, as well as simulated traffic generated in a controlled virtual environment. These datasets are chosen to reflect a wide range of attack types and normal behaviors to ensure comprehensive model training.

Following data collection, preprocessing is conducted to clean and prepare the data. This involves removing noisy or incomplete records, selecting relevant features, normalizing data values, and encoding categorical labels. To address class imbalance—common in cybersecurity data—oversampling techniques such as SMOTE are employed. Feature engineering is performed to enhance model accuracy by extracting key attributes from traffic logs and system events.
Multiple deep learning architectures are then explored for their effectiveness in identifying and classifying threats. Convolutional Neural Networks (CNNs) are used to detect spatial patterns in network traffic, while Recurrent Neural Networks (RNNs), particularly Long Short-Term Memory (LSTM) networks, are utilized to capture temporal dependencies in log sequences. Additionally, autoencoders are implemented for unsupervised anomaly detection, and hybrid models combining CNN and LSTM are tested to leverage both spatial and sequential features.

IV. IMPLEMENTATION

To implement the proposed AI-powered SOC, a modular architecture was designed comprising data ingestion, deep learning-based detection, and automated response components. The first stage involves collecting and streaming network traffic data using packet capture tools such as Wireshark or tcpdump, and exporting logs from IDS/IPS systems like Snort or Suricata. This data is then stored and processed using ELK Stack (Elasticsearch, Logstash, Kibana) for real-time visibility and querying.

The core detection engine is built using Python and popular deep learning frameworks such as TensorFlow and PyTorch. Preprocessed datasets (such as CICIDS2017 and NSL-KDD) are used to train multiple models including CNN, LSTM, and hybrid CNN-LSTM architectures. These models are trained offline using GPU-enabled environments like Google Colab, Jupyter with CUDA, or cloud platforms such as AWS SageMaker. The models are saved in a portable format (e.g., .pb, .pt, or ONNX) and served in real time via TensorFlow Serving or FastAPI-based inference APIs.

The detection engine is integrated with a simulated SOC dashboard created using open-source SIEM tools like Kibana or Splunk Free, where alerts are displayed. When a threat is detected, the system automatically triggers response actions. These are implemented through custom Python scripts or API calls that can block IPs (using iptables or firewall rules), send alerts (via email or Slack), and log incidents. For real-time streaming and response coordination, Apache Kafka is used to enable event-driven communication between the detection engine and response module.

For testing, a virtual network environment is built using VirtualBox or Docker Compose, simulating normal traffic alongside active attacks using penetration testing tools such as Nmap, Metasploit, or hping3. The SOC monitors traffic, detects threats, and responds autonomously, logging all events for post-incident analysis. To support ongoing improvement, new threat data is periodically fed back into the training pipeline, enabling the model to learn and adapt to evolving attack patterns.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404560|

V. RESULTS AND CONCLUSION

The implementation of the proposed AI-powered SOC demonstrated promising results in detecting and responding to cyber threats in real time. Multiple deep learning models—including CNN, LSTM, and hybrid CNN-LSTM architectures—were trained and evaluated using benchmark datasets such as CICIDS2017 and NSL-KDD. Among these, the hybrid CNN-LSTM model achieved the highest performance, with an accuracy exceeding 98% and an F1-score of 0.97, outperforming traditional machine learning models such as Random Forest and SVM. The use of LSTM enabled the model to effectively capture temporal patterns in network traffic, while CNN contributed to spatial feature extraction, resulting in highly accurate classification of various attack types.

The system successfully integrated with real-time data pipelines using Apache Kafka and was able to process live traffic data with minimal latency. The average inference time per sample was under 100 milliseconds, making the system viable for real-time deployment in SOC environments. The automated response module, triggered upon detection of malicious activity, was able to perform actions such as IP blocking, alert generation, and session termination with no human intervention. These responses were coordinated through lightweight Python scripts and proved effective in containing threats during simulated penetration testing using tools like Metasploit and Nmap.

In conclusion, the research validates that integrating deep learning into SOC operations significantly enhances the speed and accuracy of threat detection and response. The system offers a scalable and intelligent alternative to traditional rule-based SOCs, reducing the dependency on manual analysis and improving reaction time to potential breaches. Furthermore, the use of explainability tools like SHAP allowed analysts to gain insights into model decisions, addressing concerns related to the "black box" nature of AI. While the prototype performed well in a controlled environment, future work will focus on deployment in real-world networks, continuous model retraining with live data, and improving resistance to adversarial attacks. Overall, the study demonstrates that AI-powered SOCs, backed by deep learning, are a viable and impactful solution for modern cybersecurity defense.

VI. LIMITATIONS AND FUTURE WORK

While the proposed AI-powered SOC system demonstrated high accuracy and real-time performance, there are several limitations that must be acknowledged. First, the system was tested primarily on publicly available datasets such as NSL-KDD and CICIDS2017, which, while comprehensive, may not fully reflect the diversity, complexity, and unpredictability of real-world network environments. As a result, model performance in production settings may vary due to factors such as unseen attack patterns, encrypted traffic, or sophisticated evasion techniques. Additionally, the deep learning models, particularly LSTM and CNN-LSTM architectures, require significant computational resources for training, which may limit deployment on resource-constrained environments or edge devices.

Another notable limitation is the potential vulnerability to adversarial attacks, where slight, crafted perturbations in input data can mislead the AI model into misclassifying threats. Furthermore, although the system supports automated responses, the actions taken are rule-based and relatively simplistic. More advanced decision-making strategies, such as context-aware or risk-based responses, were not implemented in this prototype. Model explainability, although partially addressed using SHAP, remains a challenge in deep learning, especially when applied in critical cybersecurity scenarios where transparency and trust are essential.

REFERENCES

1. B.-X. Wang, J.-L. Chen, and C.-L. Yu, ‘‘An AI-powered networkthreat detection system,’’ IEEE Access, vol. 10, pp. 54029–54037,2022.
2. C. Park, J. Lee, Y. Kim, J.-G. Park, H. Kim, and D. Hong, ‘‘An enhancedAI-based network intrusion detection system using generative adversar-ial networks,’’ IEEE Internet Things J., vol. 10, no. 3, pp. 2330–2345,Feb. 2023.
3. D. Javeed, T. Gao, P. Kumar, and A. Jolfaei, ‘‘An explainable and resilientintrusion detection system for Industry 5.0,’’ IEEE Trans. Consum. Elec-tron., vol. 70, no. 1, pp. 1342– 1350, Jun. 2023.
4. Simran, S. Kumar, and A. Hans, ‘‘The AI shield and red AI framework:Machine learning solutions for cyber threat intelligence(CTI),’’ in Proc.Int. Conf. Intell. Syst. Cybersecurity (ISCS), May 2024, pp. 1–6.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404560|

5. H. M. Soliman, D. Sovilj, G. Salmon, M. Rao, and N. Mayya, ‘‘RANK:AI-assisted end-toend architecture for detecting persistent attacks in enter-prise networks,’’ IEEE Trans. Depend. Secure Comput., vol. 21, no. 4,pp. 3834–3850, Jul. 2024
6. S. Kumbale, S. Singh, G. Poornalatha, and S. Singh, ‘‘BREE-HD: Atransformer-based model to identify threats on Twitter,’’ IEEE Access,vol. 11, pp. 67180–67190, 2023.
7. Y. Gao, Y. Kim, B. G. Doan, Z. Zhang, G. Zhang, S. Nepal,D. C. Ranasinghe, and H. Kim, ‘‘Design and evaluation of a multi-domaintrojan detection method on deep neural networks,’’ IEEE Trans. Depend.Secure Comput., vol. 19, no. 4, pp. 2349–2364, Jul. 2022.
8. I. Aliyu, S. Van Engelenburg, M. B. Mu’Azu, J. Kim, and C. G. Lim,‘‘Statistical detection of adversarial examples in blockchain-based feder-ated forest in-vehicle network intrusion detection systems,’’ IEEE Access,vol. 10, pp. 109366–109384, 2022.
9. Gopichand Vemulapalli, Padmaja Pulivarthy, “Integrating Green Infrastructure With AI-Driven Dynamic Workload Optimization: Focus on Network and Chip Design,” in Integrating Blue-Green Infrastructure Into Urban Development, IGI Global, USA, pp. 397-422, 2025.
10. K. Gu, X. Dong, X. Li, and W. Jia, ‘‘Cluster-based malicious node detectionfor false downstream data in fog computing-based VANETs,’’ IEEE Trans.Netw. Sci. Eng., vol. 9, no. 3, pp. 1245–1263, May 2022
11. T. T. Huong, T. P. Bac, K. N. Ha, N. V. Hoang, N. X. Hoang, N. T. Hung, andK. P. Tran, ‘‘Federated learning-based explainable anomaly detection forindustrial control systems,’’ IEEE Access, vol. 10, pp. 53854–53872, 2022

.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details