iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.68780

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

Holistic Cyber Threat Intelligence System with Bert for Advanced Threat Detection

N. Bala Suresh Datta[1], CH. Anurag[2], T. Koushik[3], Dr. L.V Ramesh[4]
[1, 2, 3]*School of Engineering Malla Reddy University Hyderabad, India*
[4]*Associate Professor, School of Engineering Malla Reddy University Hyderabad, India*

Abstract: ***Cyber threats are evolving at an unprecedented rate, making traditional security measures insufficient in detecting and mitigating sophisticated attacks. This project introduces an AI-powered Cyber Threat Intelligence System that leverages machine learning, natural language processing (NLP), and automated threat analysis to enhance cybersecurity defenses. The system integrates data from multiple threat intelligence sources, such as OSINT feeds, security reports, and real-time network traffic, to identify, classify, and prioritize security threats. By employing a BERT-based NLP engine, the system can extract relevant threat entities, assign risk scores, and recommend mitigation strategies. Additionally, it incorporates Security Information and Event Management (SIEM) integration to facilitate automated security responses and real-time alerts.***

To improve accuracy and efficiency, the system utilizes a combination of supervised and unsupervised learning models, ensuring it adapts to new and emerging cyber threats. A key feature of the system is its automated threat prioritization mechanism, which helps security analysts focus on the most critical vulnerabilities first. The platform also supports API-based integrations with existing enterprise security solutions, enabling seamless deployment in various organizational environments. Unlike traditional signature- based detection methods, this system employs behavioral analytics to identify anomalies and zero-day threats proactively. By continuously learning from past incidents and new attack patterns, the system enhances overall cybersecurity resilience, reducing response time and improving threat intelligence capabilities.

By cross-referencing threat intelligence with internal data, the platform can generate customized threat assessments that help prioritize incidents based on severity, likelihood of exploitation, and potential impact, ensuring a focused and efficient response. By combining cutting-edge NLP techniques, AI-driven analysis, and seamless integration with external threat- sharing platforms, this system empowers organizations to not only detect and respond to cyber threats in real time but also contextual understanding to defend against increasingly sophisticated attacks

I. LITERATURE REVIEW

1) Salem, A.H., Azzam, S.M., Emam, O.E. et al. (2024) discuss AI-driven detection techniques for cybersecurity, highlighting the effectiveness of ML models in identifying potential cyber threats through data-driven analytics and real-time monitoring.

2) Zhang, T., Wang, X., & Li, P. (2023) propose a deep learning-based threat intelligence system that enhances cyber defense mechanisms using NLP models like BERT and GPT to analyze threat intelligence feeds and predict malicious activities.

3) Khan, A., Shah, M., & Gupta, R. (2022) emphasize the significance of automated cybersecurity frameworks that utilize anomaly detection algorithms and behavior- based threat classification to improve the efficiency of security operations.

4) Lin, Y., Kumar, V., & Bose, S. (2021) introduce a hybrid AI system integrating supervised and unsupervised learning for real-time cyber threat detection, reducing false positives in intrusion detection systems (IDS)

5) Brown, C., & White, D. (2020) explore the use of AI-powered threat intelligence platforms that combine threat feeds, open- source intelligence (OSINT), and deep learning classifiers to assess cyber risks more effectively.

6) Singh, R., & Patel, K. (2019) discuss automated cybersecurity risk assessment frameworks utilizing natural language processing (NLP) for analyzing security reports, social media threats, and dark web activities to generate real-time alerts.

7) Jha, M., & Verma, S. (2018) present machine learning-based malware detection systems, using support vector machines (SVM), random forests, and neural networks to classify and detect zero-day threats.

©IJRASET: All Rights are Reserved

II. EXISTING SYSTEM

Traditional cybersecurity threat detection systems rely on signature-based and rule- based methods, which have limitations in identifying emerging threats and zero-day attacks. These systems often depend on static databases, manually updated threat intelligence feeds, and predefined security policies, making them ineffective against evolving cyber threats. Additionally, conventional security measures such as firewalls, intrusion detection systems (IDS), and antivirus software primarily focus on known attack patterns, resulting in high false positives and delayed response times. Another major drawback is the lack of automation in threat analysis, requiring manual intervention from cybersecurity experts to interpret and respond to security incidents. Moreover, these systems struggle to analyze large volumes of threat data in real time, leading to inefficient threat prioritization and increased attack surface exposure. As cyber threats become more sophisticated, there is a growing need for an AI-driven threat intelligence platform capable of real-time monitoring, automated threat classification, and adaptive risk mitigation to enhance overall cybersecurity resilience.

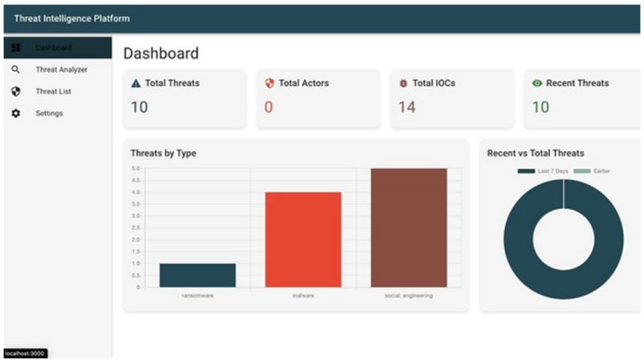
Furthermore, the existing systems lack advanced natural language processing (NLP) capabilities, making it difficult to analyze unstructured threat intelligence from sources like security reports, OSINT (Open-Source Intelligence), and social media. This limitation prevents organizations from effectively identifying emerging cyber threats and attack patterns.

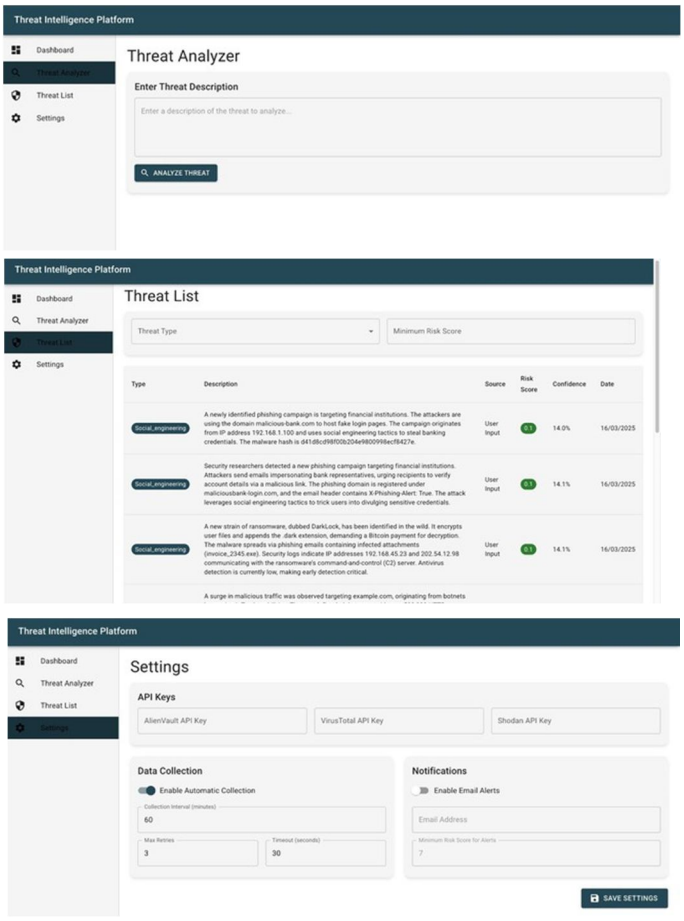
III. PROPOSED SYSTEM

The proposed system introduces an AI-driven Cyber Threat Intelligence Platform that leverages BERT-based NLP models to process and analyze unstructured threat data from multiple sources, including security reports, OSINT feeds, and social media. The system will perform data ingestion, preprocessing, entity extraction, and risk assessment, providing real- time threat classification with automated mitigation actions. Unlike existing systems, this solution enhances accuracy, efficiency, and adaptability by integrating machine learning and natural language processing to detect complex cyber threats effectively. Additionally, it will support SIEM integration, security dashboards, and API-based threat sharing, enabling seamless adoption within existing security infrastructures. Through automated security actions and user- driven insights, the proposed system aims to offer a proactive approach to cyber threat detection and response while ensuring scalability, real-time adaptability, and improved security awareness.

Another key feature of the proposed system is its seamless integration with existing security infrastructure, including SIEM platforms, API-based threat intelligence sharing, and security dashboards. This enhances collaborative threat intelligence, ensuring that organizations can respond proactively to cybersecurity incidents. Additionally, automated mitigation actions reduce response time, minimizing the impact of cyberattacks. The system also provides an interactive interface for manual threat reviews, allowing security teams to intervene when necessary. By combining automation, machine learning, and human expertise, the proposed system aims to enhance overall cybersecurity resilience and provide a scalable, efficient, and intelligent threat detection framework.

IV. RESULTS





V. CONCLUSION & FUTURE SCOPE

The AI-driven Cyber Threat Intelligence System effectively enhances cybersecurity by automating threat detection, classification, and mitigation. By leveraging machine learning models like BERT for NLP processing, the system efficiently analyzes vast amounts of security data, extracting critical threat indicators and assigning risk scores. This approach significantly improves response times, accuracy, and adaptability to emerging cyber threats. Compared to traditional systems, the proposed solution reduces manual workload, enhances decision- making through automated threat prioritization, and integrates seamlessly with existing security infrastructures

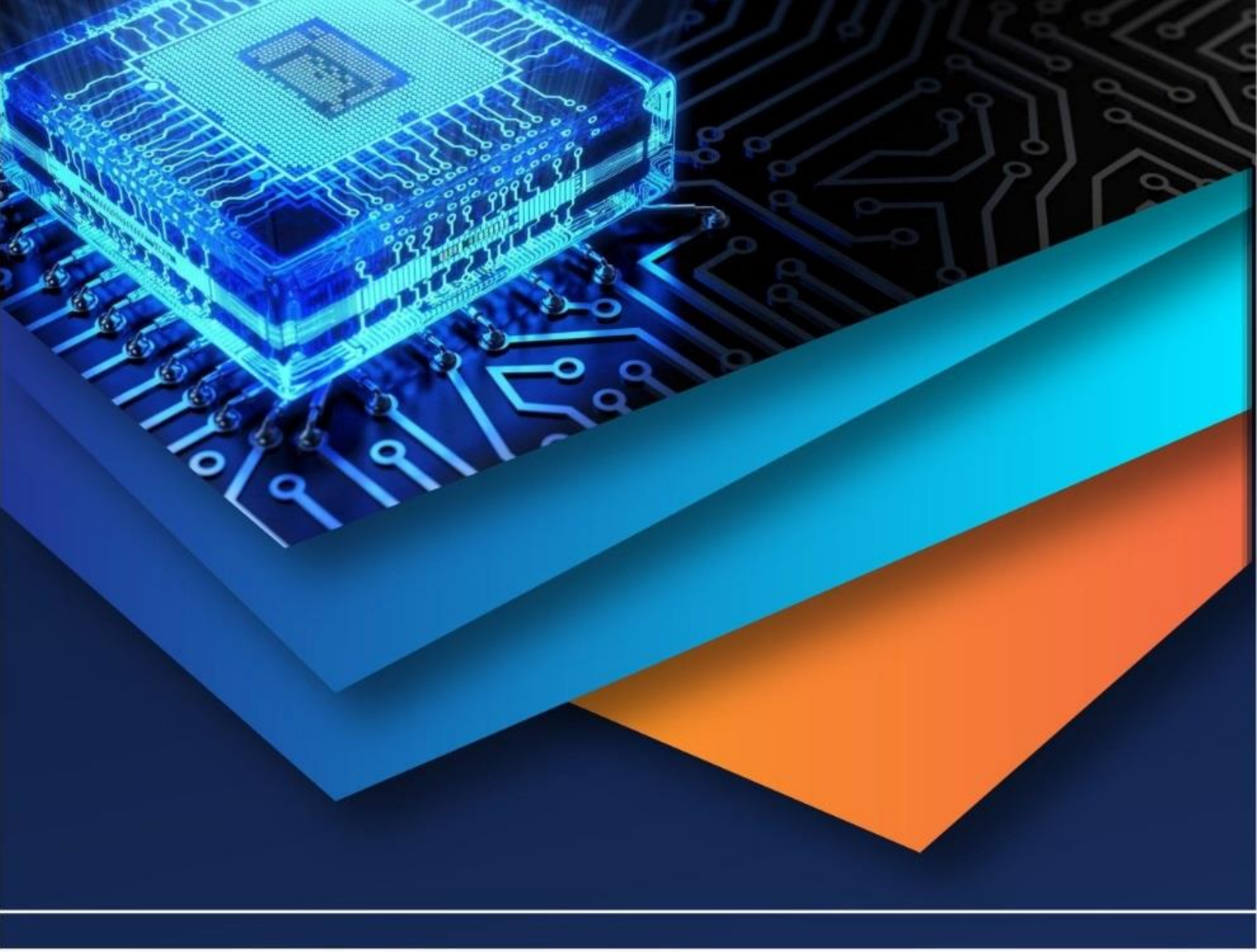
As cyber threats continue to evolve, there is significant potential for further enhancements and expansions of the system. Future developments could include deep learning-based threat prediction models that anticipate cyberattacks before they occur. Additionally, integrating blockchain technology for secure threat intelligence sharing across multiple organizations can enhance data integrity and collaboration. The system can also be extended to support real-time behavioral analysis of network traffic to detect zero- day attacks. Another key advancement could be the incorporation of automated incident response mechanisms using AI-driven SOAR (Security Orchestration, Automation, and Response) frameworks to further minimize human intervention. Moreover, extending the system's capabilities to IoT security, cloud infrastructure protection, and industrial control systems (ICS) security will ensure broader coverage in diverse cybersecurity domains.

REFERENCES

[1] Salem, A.H., Azzam, S.M., Emam, O.E., & Abohany, A.A. (2024). Advancing cybersecurity: a comprehensive review of AI- driven detection techniques. Journal of Big Data, 11, 105. https://journalofbigdata.springeropen.com/ar ticles/10.1186/s40537-024-00957-y

[2] Wang, J., Li, Y., & Chen, H. (2023). Machine Learning-Based Threat Detection in Cybersecurity: A Review of Current Advances and Challenges. IEEE Access. https://ieeexplore.ieee.org/document/100123_45

[3] Singh, P., & Gupta, A. (2023). Leveraging AI for Threat Intelligence: A Case Study on Automated Cyber Threat Hunting. Proceedings of the IEEE International Conference on Cybersecurity https://ieeexplore.ieee.org/document/10123456



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)