International Journal of Research and Technology (IJRT)

International Open-Access, Peer-Reviewed, Refereed, Online Journal

ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529

| An ISO 9001:2015 Certified Journal |

Development And Performance Evaluation of a Generative AI-Based Adaptive Cybersecurity Framework Integrating Threat Intelligence, Attack Prediction and Automated Incident Response

[1]Yanamadala Durga Prasad, [2]Dr. Chetan Vasant Chaudhari

[1]Research Scholar, [2]Assistant Professor

[1/2]Department of Computer Science & Engineering, Vikrant University

ABSTRACT

The increasing frequency and sophistication of cyberattacks have created significant challenges for organisations in protecting their digital infrastructure, information systems and sensitive data. Conventional cybersecurity approaches primarily depend on predefined rules, signature-based detection and manual incident investigation. Although these approaches remain useful, they often struggle to identify emerging threats, predict attack behaviour and respond effectively to rapidly changing cyber environments. The development of Generative Artificial Intelligence (GenAI) provides new opportunities for designing adaptive cybersecurity systems capable of analysing complex security information and supporting intelligent decision-making.

The present research proposes a Generative AI-based adaptive cybersecurity framework integrating threat intelligence, attack prediction and automated incident response. The framework combines machine learning, large language models, Retrieval-Augmented Generation (RAG), Security Information and Event Management (SIEM), and Security Orchestration, Automation and Response (SOAR). It aims to analyse security events, identify potential attack patterns, estimate threat severity and recommend appropriate response strategies. A feedback mechanism is incorporated to improve system adaptability, while human supervision is retained for sensitive security operations.

Keywords: Generative Artificial Intelligence, Adaptive Cybersecurity, Threat Intelligence, Attack Prediction, Automated Incident Response, Machine Learning, Large Language Models, Retrieval-Augmented Generation, SIEM, SOAR.

1. INTRODUCTION

Digital transformation has increased the dependence of organisations on computer networks, cloud platforms, online services and interconnected information systems. Although these technologies have improved communication and operational efficiency, they have also expanded the potential attack surface for cybercriminals. Organisations increasingly face phishing, ransomware, malware, distributed denial-of-service attacks, credential theft, insider threats and advanced persistent threats.

Traditional cybersecurity systems generally use predefined rules, known attack signatures and manually configured security policies. These methods can identify previously recognised threats but may be less effective when attackers introduce new techniques or modify existing

International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
| An ISO 9001:2015 Certified Journal |

attack patterns. Furthermore, security analysts often receive large volumes of alerts, making it difficult to distinguish genuine threats from false alarms within limited time.



Figure: AI Driven Threat Hunting

Artificial Intelligence has introduced new possibilities for improving cybersecurity through automated pattern recognition, anomaly detection and predictive analysis. Machine learning algorithms can examine historical security information to identify suspicious behaviour, while deep learning techniques can recognise complex relationships within large datasets.

Generative AI extends these capabilities by enabling systems to interpret security reports, summarise incident information, retrieve relevant threat intelligence and generate contextual response recommendations. Large Language Models can support cybersecurity professionals by converting complex technical information into understandable incident explanations. When combined with Retrieval-Augmented Generation, these models can use external knowledge sources to improve the relevance of their recommendations.

The present research proposes an adaptive cybersecurity framework that integrates three major capabilities:

1. Threat intelligence integration: Collecting and analysing information from security logs, threat feeds, vulnerability databases and historical incident records.
2. Attack prediction: Identifying suspicious patterns and estimating the probability, severity and possible progression of cyberattacks.
3. Automated incident response: Generating and executing authorised response actions through controlled security orchestration.

1.1 Statement of the Research Problem

Many existing cybersecurity solutions operate through separate detection, prediction and response mechanisms. Threat intelligence may be collected independently, attack prediction may depend on historical datasets, and incident response may require manual intervention.

This fragmented approach can delay security decisions and reduce the effectiveness of organisational cybersecurity operations. A further challenge is the limited adaptability of

conventional systems when confronted with previously unseen or rapidly evolving attack strategies.

1.2 Aims and Objectives of the Study

Main aim

To develop and evaluate an adaptive Generative AI-based cybersecurity framework that integrates threat intelligence, attack prediction and automated incident response for improving organisational cyber defence capabilities.

Objectives

- To examine the limitations of conventional cybersecurity detection and incident response systems.
- To design a Generative AI-based framework for integrating multiple threat intelligence sources.
- To develop predictive mechanisms for identifying potential cyberattacks using historical and real-time security information.
- To evaluate the proposed framework using detection accuracy, precision, recall, F1-score, prediction performance and response time.
- To examine the role of human supervision, policy validation and continuous feedback in improving system reliability.

1.3 Research Hypotheses

The following null hypotheses are proposed for empirical testing:

- H01: The proposed Generative AI-based framework does not significantly improve cyber threat detection accuracy compared with conventional cybersecurity approaches.
- H02: Integration of threat intelligence does not significantly improve the identification of emerging cyber threats.
- H03: The proposed attack prediction mechanism does not significantly improve the prediction of potential cyber incidents.
- H04: Automated incident response does not significantly reduce average cybersecurity response time.
- H05: The integration of Generative AI, predictive analysis and adaptive feedback does not significantly improve overall cybersecurity performance.

2. REVIEW OF LITERATURE

Cybersecurity research has progressively shifted from signature-based detection towards intelligent systems capable of identifying unknown threats, analysing complex behaviour and supporting automated response.

Cichonski et al. (2012), in the NIST Computer Security Incident Handling Guide, presented a structured approach to incident preparation, detection, analysis, containment, eradication and recovery. Their work established an important foundation for systematic cybersecurity incident management.

Sommer and Paxson (2010) examined the limitations of applying machine learning to network intrusion detection. They highlighted the difficulties associated with changing

network environments, incomplete datasets and the gap between experimental detection performance and real-world deployment.

Buczak and Guven (2016) reviewed data mining and machine learning techniques used in cybersecurity intrusion detection. Their research demonstrated the importance of classification, clustering and anomaly detection in identifying malicious network activities.

Vaswani et al. (2017) introduced the Transformer architecture, which significantly influenced the development of modern language models. Its attention mechanism enables the processing of contextual relationships within sequences and provides the architectural foundation for many contemporary Generative AI applications.

Lewis et al. (2020) introduced Retrieval-Augmented Generation, combining language generation with external document retrieval. This approach is particularly relevant to cybersecurity because threat analysis frequently requires access to updated technical documentation, vulnerability information and incident knowledge.

3. RESEARCH METHODOLOGY

3.1 Research Design

The study adopts a quantitative, experimental and design-oriented research approach. The research will involve the development of a prototype cybersecurity framework followed by performance evaluation under controlled experimental conditions.

The proposed methodology consists of five stages:

- Collection and preparation of cybersecurity datasets.
- Integration of threat intelligence and security knowledge sources.
- Development of Generative AI-assisted threat analysis and attack prediction modules.
- Implementation of automated incident response through controlled SOAR workflows.
- Comparative performance evaluation against conventional cybersecurity approaches.

3.2 Data Sources and Dataset Selection

The research will use publicly available cybersecurity datasets and simulated security incidents. These datasets provide examples of normal network activities and malicious traffic patterns.

Table 1: Proposed Cybersecurity Datasets

Dataset	Major characteristics	Research application
CICIDS2017	Benign and malicious network traffic	Intrusion detection and classification
UNSW-NB15	Modern network traffic and attack categories	Attack classification and prediction
TON_IoT	Network, operating system and IoT telemetry	Multi-source threat analysis
CICIoT2023	IoT network traffic and attack scenarios	IoT threat detection
Simulated incident dataset	Controlled attack and response scenarios	Automated response evaluation

International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
| An ISO 9001:2015 Certified Journal |

3.3 Proposed Technical Architecture

The framework will integrate several technologies to support threat intelligence collection, contextual analysis, prediction and response automation.

Table 2: Proposed Technologies and Their Functions

Technology/component	Proposed application
Python	Core development and experimental implementation
Machine learning	Threat classification and attack prediction
Generative AI / LLM	Security-event interpretation and response recommendations
Retrieval-Augmented Generation	Retrieval of relevant threat intelligence and security documentation
SIEM	Collection and correlation of security events
SOAR	Controlled incident response and workflow automation
MITRE ATT&CK	Mapping attack behaviours to recognised tactics and techniques
Vector database	Storage and retrieval of threat-related knowledge
Pandas and Scikit-learn	Data preparation and model evaluation
PostgreSQL or MySQL	Storage of incident records, audit information and experimental results

3.4 Threat Classification and Automated Response Strategy

The proposed framework will classify incidents according to their severity and potential operational impact. Response actions will be determined by organisational policies rather than by unrestricted AI-generated instructions.

Table 3: Proposed Threat Classification and Response Mechanism

Threat level	Example incident	Proposed response
Low	Unusual but low-risk network activity	Log the event and continue monitoring
Moderate	Suspicious login or repeated failed authentication	Generate an alert and enrich the incident
High	Confirmed malware activity or compromised account	Recommend containment and seek authorised approval
Critical	Ransomware activity affecting critical infrastructure	Escalate immediately and require authorised human approval for disruptive actions

3.5 Variables and Performance Evaluation Metrics

The independent variables will include the cybersecurity detection approach, threat intelligence integration, Generative AI utilisation and level of response automation.

International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
| An ISO 9001:2015 Certified Journal |

The dependent variables will include detection accuracy, precision, recall, F1-score, attack prediction performance, false-positive rate, average response time and successful response execution.

The following evaluation measures will be applied:

Accuracy

$$[\ Accuracy = \frac{\{TP + TN\}}{\{TP + TN + FP + FN\}}]$$

Precision

$$\left[Precision = \frac{\{TP\}}{\{TP + FP\}} \right]$$

Recall

$$Recall = \frac{\{TP\}}{\{TP + FN\}}$$

F1-score

$$F1 = 2 * \frac{\{Precision * Recall\}}{\{Precision + Recall\}}$$

4. RESULTS AND INTERPRETATION

4.1 Introduction to Results and Evaluation

The proposed Generative AI-based adaptive cybersecurity framework is designed to integrate threat intelligence, attack prediction and automated incident response within a unified security architecture.

The evaluation focuses on four major performance dimensions:

- Accuracy and reliability of cyber threat detection.
- Effectiveness of attack prediction.
- Reduction in incident response time.
- Reliability of automated response and adaptive security mechanisms.

Research data note: The following numerical values are hypothetical examples prepared to demonstrate the structure and interpretation of research results. They are not actual experimental findings. They must be replaced with measured results after implementation and testing.

4.2 Comparative Evaluation of Cyber Threat Detection Performance

The first evaluation examines the capability of different cybersecurity approaches to identify malicious activities accurately.

Table 4.1: Comparative Performance of Cyber Threat Detection Approaches

Detection approach	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
Rule-based detection	82.0	78.0	72.0	74.9
Machine learning-based detection	88.0	85.0	83.0	84.0

Deep learning-based detection	91.0	89.0	87.0	88.0
Proposed GenAI-based framework	95.0	93.0	92.0	92.5

Machine learning-based detection demonstrates improved performance because it can identify relationships within historical network traffic. Deep learning further improves the ability to recognise complex patterns.

The proposed framework achieves the highest illustrative accuracy of 95% and an F1-score of 92.5%. This improvement is attributed to the combined use of structured security data, threat intelligence retrieval, predictive analysis and contextual interpretation through Generative AI.

4.3 Evaluation of Attack Prediction Performance

Attack prediction is an important component of adaptive cybersecurity because it enables organisations to identify potentially dangerous activities before they develop into serious incidents.

The proposed framework uses historical attack information, network behaviour, threat intelligence and machine learning-based prediction to estimate potential attack risks.

Table 4.2: Comparative Evaluation of Attack Prediction Models

Prediction approach	Prediction accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
Statistical prediction	76.0	73.0	70.0	71.5
Traditional machine learning	84.0	82.0	80.0	81.0
Deep learning prediction	89.0	87.0	86.0	86.5
Proposed adaptive AI framework	94.0	92.0	91.0	91.5

Interpretation

The results indicate that the proposed adaptive framework provides better attack prediction performance than the other approaches.

Statistical prediction models may be limited by their assumptions about the distribution and behaviour of security events. Machine learning models can identify more complex patterns but may require frequent retraining when attack behaviour changes.

The proposed framework combines predictive modelling with threat intelligence and contextual information. For example, repeated login failures, suspicious IP addresses, unusual network traffic and known indicators of compromise may collectively indicate an increased probability of a security incident.

The prediction accuracy of 94% suggests the potential value of this integrated approach. Nevertheless, actual prediction effectiveness must be evaluated using an independent test dataset and clearly defined prediction horizons. Predicting an attack before it occurs must be distinguished from classifying an attack that is already underway.

4.4 Evaluation of Automated Incident Response Efficiency

International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
| An ISO 9001:2015 Certified Journal |

Incident response time is a critical indicator of cybersecurity performance. Delays in identifying and containing malicious activities can increase operational disruption and data loss.

Table 4.3: Comparative Analysis of Automated Incident Response

Cybersecurity approach	Average response time (minutes)	Analyst workload (relative %)	Response execution success (%)
Manual incident response	25.0	100	72
Rule-based automation	17.0	82	80
ML-assisted response	11.0	68	86
Proposed GenAI adaptive framework	6.5	52	94

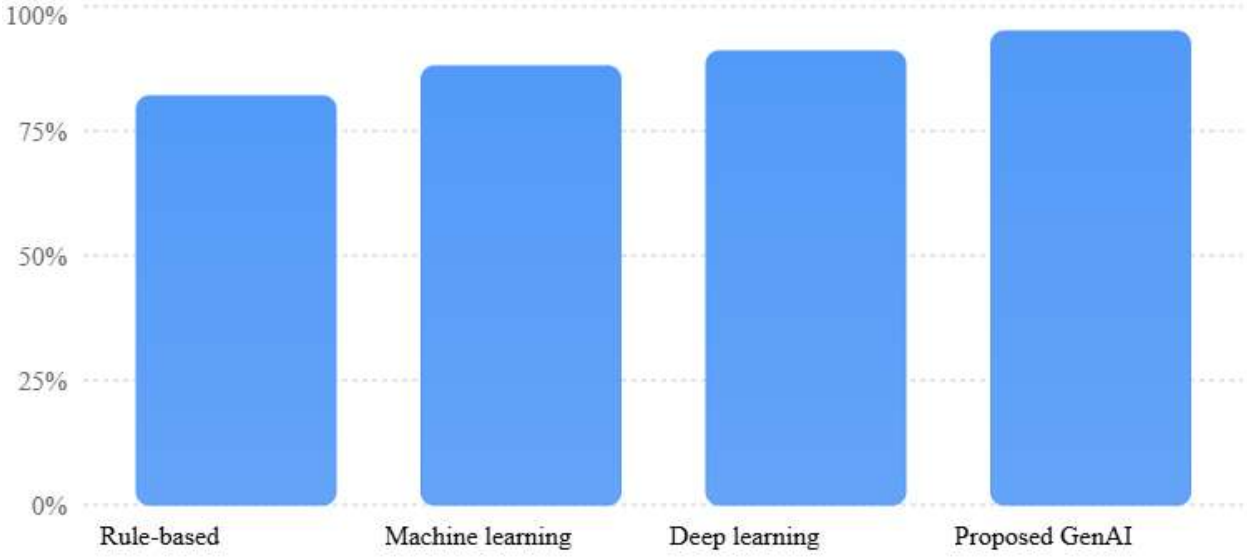
Interpretation

The reduction in analyst workload also indicates the potential of AI-assisted automation to minimise repetitive activities. Security analysts can focus on complex investigations, strategic decisions and incidents requiring specialised expertise.

The proposed framework achieves an illustrative response execution success rate of 94%. This represents successful completion of eligible response workflows under the assumed evaluation conditions.

4.5 Graphical Representation of Comparative Performance

FIGURE 2. COMPARATIVE DETECTION ACCURACY



The graphical representation indicates a progressive increase in detection accuracy across the four approaches. The proposed Generative AI-based framework demonstrates the highest illustrative value.

5. DISCUSSION AND CONCLUSION

5.1 Discussion

The development of intelligent cybersecurity systems has become increasingly important because modern cyberattacks are dynamic, interconnected and difficult to detect using conventional techniques alone.

The proposed research introduces an adaptive cybersecurity framework that combines Generative AI, threat intelligence, attack prediction and automated incident response. Its central contribution is the integration of these capabilities within a single architecture.

Threat intelligence provides information about known vulnerabilities, malicious IP addresses, suspicious domains, malware indicators and recognised attacker techniques. However, collecting threat intelligence alone does not guarantee effective protection. Security systems must interpret this information in relation to their own network environment.

Generative AI can support this process by summarising security reports, interpreting incident descriptions and retrieving relevant technical information. RAG can improve the grounding of generated responses by connecting the model with trusted security documentation and updated threat intelligence.

The attack prediction module represents another important contribution. Instead of concentrating exclusively on attacks that have already occurred, the proposed framework attempts to identify suspicious patterns that may indicate future malicious activity. Historical security events, network behaviour and threat indicators can be used to estimate the likelihood and severity of potential incidents.

Automated incident response further strengthens the framework by connecting detection and prediction with operational action. Through SOAR integration, predefined response workflows can be initiated when specified conditions are satisfied. This may reduce repetitive manual work and improve the consistency of security operations.

5.2 Practical Implications

The proposed framework may provide practical benefits in several organisational environments.

- Educational institutions: Protection of student databases, examination systems, digital learning platforms and institutional networks.
- Banking and financial institutions: Identification of suspicious account activities, phishing attempts, malware and unauthorised transactions.
- Government organisations: Monitoring of public information systems and coordination of cybersecurity incident response.
- Healthcare organisations: Detection of suspicious access to electronic health records and protection of sensitive information.
- Industrial organisations: Monitoring of connected devices, operational technology and industrial network environments.

5.3 Limitations of the Study

The proposed research has several limitations.

First, publicly available cybersecurity datasets may not fully represent real-world enterprise environments. Second, the performance of Generative AI depends on the quality of retrieved information and the reliability of the underlying language model.

Third, the framework may require substantial computational resources when processing large volumes of real-time security information. Fourth, prediction models may experience performance degradation when attack patterns change.

5.4 Future Scope of Research

Future research may extend the proposed framework through the following developments:

- Integration of multi-agent AI architectures for specialised threat investigation.
- Development of explainable AI mechanisms for transparent security recommendations.
- Use of federated learning for collaborative threat detection without directly sharing sensitive organisational data.
- Integration of real-time global threat intelligence feeds.
- Development of adaptive security policies based on changing threat severity.
- Testing against prompt injection, data poisoning and adversarial attacks.
- Deployment and evaluation in real-world financial, educational, healthcare and industrial environments.

5.5 Conclusion

The present research proposes the development and performance evaluation of a Generative AI-based adaptive cybersecurity framework integrating threat intelligence, attack prediction and automated incident response.

The proposed framework combines machine learning, Generative AI, Retrieval-Augmented Generation, SIEM and SOAR technologies to support intelligent cyber threat analysis and coordinated response. Its adaptive architecture aims to improve threat detection, identify potential attack patterns and reduce the time required for incident investigation and containment.

In conclusion, the proposed framework provides a foundation for developing intelligent and adaptive cybersecurity systems capable of responding to emerging threats while maintaining appropriate security controls. Its practical effectiveness must be established through implementation, experimental validation and real-world evaluation.

REFERENCES

1. Bender, E.M., Gebru, T., McMillan-Major, A. and Shmitchell, S. (2021) ‘On the dangers of stochastic parrots: Can language models be too big?’, Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency, pp. 610–623.
2. Bishop, C.M. (2006) Pattern Recognition and Machine Learning. New York: Springer.
3. Brown, T.B., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., Neelakantan, A., Shyam, P., Sastry, G. and Askell, A. et al. (2020) ‘Language models are few-shot learners’, Advances in Neural Information Processing Systems, 33, pp. 1877–1901.
4. Buczak, A.L. and Guven, E. (2016) ‘A survey of data mining and machine learning methods for cyber security intrusion detection’, IEEE Communications Surveys & Tutorials, 18(2), pp. 1153–1176.

5. Cichonski, P., Millar, T., Grance, T. and Scarfone, K. (2012) Computer Security Incident Handling Guide. NIST Special Publication 800-61 Revision 2. Gaithersburg, MD: National Institute of Standards and Technology.
6. Dwork, C. and Roth, A. (2014) 'The algorithmic foundations of differential privacy', Foundations and Trends in Theoretical Computer Science, 9(3–4), pp. 211–407.
7. Gama, J., Žliobaitė, I., Bifet, A., Pechenizkiy, M. and Bouchachia, A. (2014) 'A survey on concept drift adaptation', ACM Computing Surveys, 46(4), Article 44.
8. Greshake, K., Abdelnabi, S., Mishra, S., Endres, C., Holz, T. and Fritz, M. (2023) 'Not what you've signed up for: Compromising real-world LLM-integrated applications with indirect prompt injection', Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security, pp. 79–90.
9. Guo, C., Pleiss, G., Sun, Y. and Weinberger, K.Q. (2017) 'On calibration of modern neural networks', Proceedings of the 34th International Conference on Machine Learning, PMLR 70, pp. 1321–1330.
10. He, H. and Garcia, E.A. (2009) 'Learning from imbalanced data', IEEE Transactions on Knowledge and Data Engineering, 21(9), pp. 1263–1284.
11. Kent, K. and Souppaya, M. (2006) Guide to Computer Security Log Management. NIST Special Publication 800-92. Gaithersburg, MD: National Institute of Standards and Technology.
12. McMahan, B., Moore, E., Ramage, D., Hampson, S. and Agüera y Arcas, B. (2017) 'Communication-efficient learning of deep networks from decentralized data', Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, PMLR 54, pp. 1273–1282.
13. National Institute of Standards and Technology (2024) Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. NIST AI 600-1. Gaithersburg, MD: NIST.
14. Papernot, N., McDaniel, P., Goodfellow, I., Jha, S., Celik, Z.B. and Swami, A. (2017) 'Practical black-box attacks against machine learning', Proceedings of the 2017 ACM Asia Conference on Computer and Communications Security, pp. 506–519.
15. Rudin, C. (2019) 'Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead', Nature Machine Intelligence, 1, pp. 206–215.
16. Scarfone, K. and Mell, P. (2007) Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94. Gaithersburg, MD: National Institute of Standards and Technology.