WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

AutoSecAI: Autonomous Cyber Threat Intelligence and Self-Healing Cloud Security System Using Generative AI

Kushal Kumar G D[1], Aditya R H[2], Arsal S K[3], Akash B S[4] , Guides : Shalini M R[5] , Chethan Chandra S Basavaraddi[6]

[1-4]Department of Computer Science and Engineering, G M Institute of Technology Davanagere
[5]Assistant Professor, Department of Computer Science and Engineering, GM University Davanagere
[6]Associate Professor, Department of Computer Science and Engineering, GM University Davanagere
Email : kushalkumargd@gmail.com, adityarh2020@gmail.com, arsalshujakhazi@gmail.com,akashhhbs24@gmail.com, shalinimr@gmit.ac.in,chetanchandrasb@gmu.ac.in

DOI : https://doi.org/10.55248/gengpi.07.1026.34076

A B S T R A C T :

AutoSecAI is a cyber threat detection and self-healing system that combines machine learning and generative artificial intelligence to identify suspicious activities. It collects system, application, and AWS security logs, preprocesses the data, and detects threats using machine learning techniques such as Isolation Forest and Random Forest.

The system analyzes detected threats, assigns risk levels, and uses Ollama to explain threats and recommend security actions. A validation-based self-healing engine executes approved responses, while a database stores event details and a React dashboard displays alerts and monitoring information. The application is developed and tested locally before deployment on AWS for live security monitoring.

Keywords: Cybersecurity, Machine Learning, Generative AI, Threat Detection, Self-Healing Security.

Introduction

Cyber threats such as failed login attempts, unauthorized access, privilege escalation, and suspicious API activity can compromise application security.

Traditional monitoring methods may require manual investigation and predefined rules. AutoSecAI combines machine learning, generative AI, and automated response mechanisms to detect suspicious events, explain potential threats, and support faster security responses.

The application is developed locally and deployed on AWS to monitor real security logs. AWS is used for deployment and operational monitoring, not as the primary subject of the project.

Related Work

Research in cybersecurity has explored intrusion detection, machine learning, anomaly detection, security log analysis, generative AI, and automated incident response. These areas provide the foundation for AutoSecAI, which integrates threat detection, AI-assisted analysis, risk assessment, and controlled automated remediation.

1.1. Intrusion Detection in Cloud Environments

Intrusion detection systems monitor system activities and security events to identify unauthorized access and suspicious behaviour. Log monitoring and event analysis help detect potential security incidents. AutoSecAI uses AWS CloudTrail and CloudWatch logs to monitor security events and identify suspicious activities.

1.2. Machine Learning-Based Threat Detection

Machine learning techniques can identify abnormal patterns and classify security events using relevant features extracted from datasets. Their effectiveness depends on data quality, preprocessing, and model evaluation. AutoSecAI incorporates data preprocessing and machine learning techniques, including Isolation Forest and Random Forest, to support threat detection and classification.

1.3. Security Log Monitoring and Threat Classification

Security monitoring approaches analyze system and application logs to identify suspicious events, classify threats, and assess their severity. Different detection methods can identify predefined attack patterns or unusual activities. AutoSecAI analyzes security logs to identify threats such as failed console logins, unauthorized access, privilege escalation, and unusual API activity.

1.4. Generative AI for Cybersecurity Analysis

Generative AI can assist security systems by explaining detected threats, identifying possible causes, and recommending appropriate security actions. However, generated recommendations require verification to avoid incorrect responses. AutoSecAI uses Ollama to provide threat explanations and suggested actions, while a separate validation mechanism controls response execution.

1.5. Automated Incident Response and Self-Healing Security

Automated incident response helps reduce manual intervention by executing appropriate actions when security threats are detected. Self-healing mechanisms can support responses such as blocking suspicious IP addresses, disabling compromised accounts, or isolating affected services. AutoSecAI incorporates a validation-based self-healing engine that checks proposed actions before execution and records response details in the database for auditing and monitoring.

Literature Survey

Recent research shows increasing use of artificial intelligence and machine learning for detecting and responding to cybersecurity threats. Studies focus on improving intrusion detection accuracy, analyzing large volumes of security events, reducing manual investigation, and automating incident response. These developments provide the research foundation for AutoSecAI, which combines threat detection, AI-assisted analysis, and validated self-healing responses.

1.6. AI-Powered Cyber Incident Detection and Response

Farzaan *et al.* proposed an AI-powered system for detecting and responding to cyber incidents in cloud environments. The system integrates network traffic classification, web intrusion detection, and malware analysis using machine learning and deep learning techniques. Their experiments included Random Forest and datasets such as NSL-KDD, UNSW-NB15, and CIC-IDS-2017. Hertfordshire Research Archive AutoSecAI similarly uses AI/ML for threat detection but additionally incorporates generative-AI explanations and validated self-healing actions.

1.7. AI and Machine Learning in Security Operations

Recent IEEE research on AI-enabled Security Operations Centers highlights the use of machine learning, behavioural analytics, deep learning, and automated incident response to improve threat identification and security operations. It also identifies AI/ML integration as an important direction for reducing operational challenges in security monitoring. IEEE Xplore AutoSecAI follows a similar direction by integrating detection, analysis, monitoring, and response within a single system.

1.8. Deep Learning-Based Intrusion Detection

A recent IEEE Access survey reviewed deep-learning-based network intrusion detection approaches, including generative models, transformers, convolutional networks, and hybrid techniques. The study identifies data quality, scalability, adversarial robustness, privacy, and interpretability as continuing challenges for practical intrusion detection systems. IEEE Xplore AutoSecAI addresses part of this problem by combining machine-learning detection with interpretable threat information and dashboard-based monitoring.

1.9. AI-Based Intrusion Detection Models

Recent IEEE research has examined machine learning and deep learning techniques such as Random Forest, Support Vector Machines, CNNs, and generative models for intrusion detection. These techniques offer different trade-offs in detection accuracy, computational requirements, scalability, and false-positive rates. IEEE Xplore AutoSecAI incorporates machine-learning-based detection together with rule-based analysis to identify suspicious security activities.

Research Methodology

- **Data Collection:** Collect security logs, datasets, and AWS CloudTrail/CloudWatch events.
- **Data Preprocessing:** Remove duplicates, handle missing values, and extract relevant features.
- **Threat Detection:** Identify suspicious activities using machine learning and predefined rules.
- **AI-Based Analysis:** Use Ollama to explain detected threats and recommend actions.
- **Validation and Self-Healing:** Validate and execute approved security responses.
- **Deployment and Evaluation:** Deploy on AWS and evaluate detection, database storage, dashboard updates, and response execution.

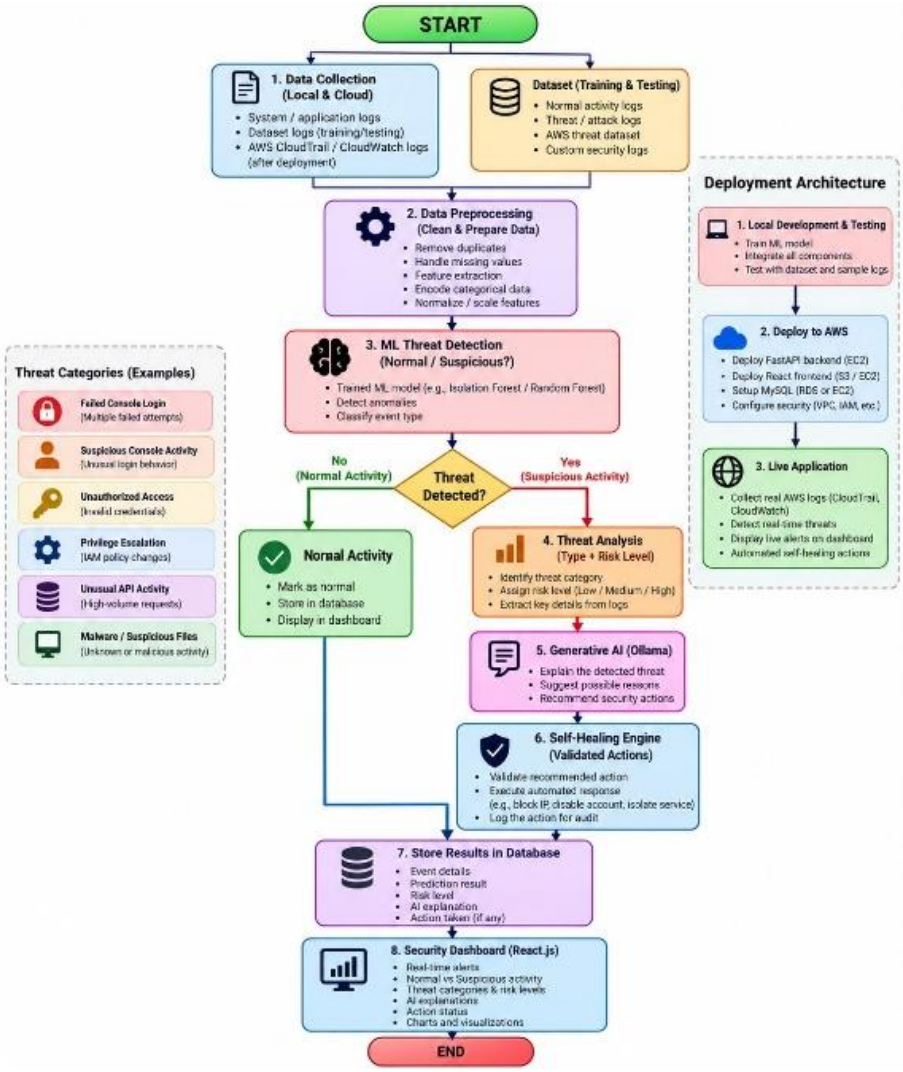


Fig. 1 – Flowchart

Implementation

- **Data Collection:** Integrate system logs, datasets, AWS CloudTrail, and CloudWatch.
- **Preprocessing:** Clean and prepare security data for analysis.
- **Threat Detection:** Implement machine learning models and rule-based detection.
- **AI Integration:** Use Ollama to explain threats and recommend security actions.
- **Self-Healing:** Validate and execute approved threat-response actions.
- **Deployment and Dashboard:** Deploy the application on AWS and display alerts, risk levels, and response status through a React dashboard.

Results

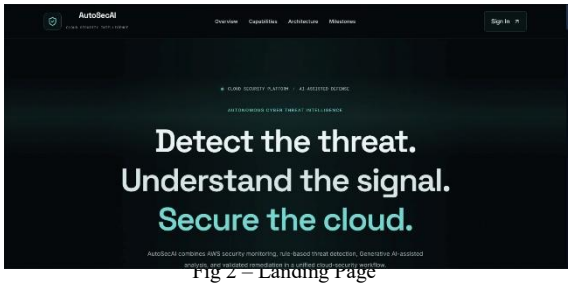


Fig 2 – Landing Page

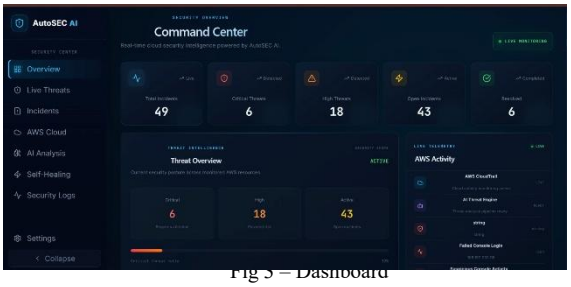


Fig 3 – Dashboard

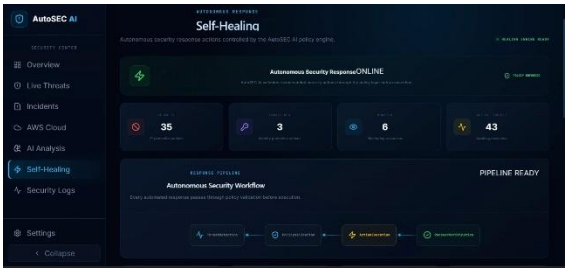


Fig 4 – Self Healing Dashboard

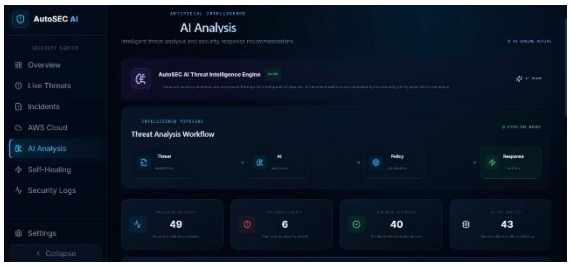


Fig 5 – Generative AI Analysis Dashboard

The AutoSecAI project is implemented with a web-based interface that provides an overview of security events, live threat monitoring, AWS activity tracking, AI-based threat analysis, and self-healing operations. The dashboard displays security statistics, detected incidents, risk levels, and response status.

The AI Analysis module presents threat analysis workflows and AI-generated recommendations, while the Self-Healing module shows automated response workflows and action status. The AWS Cloud module supports security event monitoring, and the security logs and database maintain records for investigation and auditing.

The project demonstrates the integration of threat detection, AI-assisted analysis, and validated response mechanisms in a single application deployed on AWS. Actual detection accuracy and response performance must be established through testing.

5. Conclusion

AutoSecAI integrates machine learning, generative AI, and automated security responses to detect and analyze suspicious activities. The system uses AWS CloudTrail and CloudWatch for security log monitoring, Ollama for threat explanations, and a validation-based self-healing engine for controlled responses. The React dashboard provides real-time security insights, while the database maintains event and response records. Deployment on AWS enables operational monitoring and supports future improvements in threat detection accuracy, response efficiency, and overall system performance.

References

1. M. A. M. Farzaan, M. Chahine Ghanem, A. El-Hajjar, and D. N. Ratnayake, “AI-Powered System for an Efficient and Effective Cyber Incidents Detection and Response in Cloud Environments,” IEEE Transactions on Machine Learning in Communications and Networking, vol. 3, pp. 623–643, 2025. DOI: 10.1109/TMLCN.2025.3564912.

2. “Design and Computational Modeling of an AI-Based Automated Cybersecurity Incident Response System,” IEEE Access, vol. 13, pp. 154383–154394, 2025. DOI: 10.1109/ACCESS.2025.3603975.

3. “Machine Learning-Based Network Intrusion Detection Optimization for Cloud Computing Environments,” IEEE Transactions on Consumer Electronics, vol. 70, no. 4, 2024. DOI: 10.1109/TCE.2024.3458810.

4. “AI-Based Methods to Detect and Counter Cyber Threats in Cloud Environments to Strengthen Cloud Security,” in 2024 International Conference on Electrical Electronics and Computing Technologies (ICEECT), 2024. DOI: 10.1109/ICEECT61758.2024.10739173.

5. “Enhancing Cloud Security: A Novel Intrusion Detection System Using Deep Learning Algorithms,” in 2024 7th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), 2024. DOI: 10.1109/ISRITI64779.2024.10963477.

6. “Design and Implementation of a Multi-Agent Threat Intelligence Assistant Based on Generative AI,” in 2025 IEEE International Conference on Big Data (BigData), 2025. DOI: 10.1109/BigData66926.2025.11400902.

7. "A Hybrid GNN-LLM Framework for Correlating Cybersecurity Incidents," in 2025 Fourth International Conference on Theoretical and Applicative Aspects of Computer Science (ICTAACS), 2025. DOI: 10.1109/ICTAACS69003.2025.11399321.

8. "Intrusion Detection in Cloud Systems Using a Deep Attention Pyramid Network," in 2025 10th International Conference on Research in Intelligent Computing in Engineering (RICE), 2025. DOI: 10.1109/RICE67503.2025.11439927