THREATSENTINELGPT: REAL-TIME AI FRAMEWORK FOR DETECTING SECURITY THREATS AND GENERATING AUTOMATED ALERTS IN CYBERSECURITY AND PHYSICAL SURVEILLANCE SYSTEMS

[,1] Mr. N. Lakshmi Narayan,[2]Pittu Bindu Siva Madhavi, [3]Pallam Yestheru Rani, [4]Pallapu Prasanth

[1]Assistant Professor, COMPUTER SCIENCE AND ENGINEERING, St. Ann's College of Engineering and Technology, Chirala-523187, India.

[2,3,4]B. Tech Student, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

ABSTRACT

ThreatSentinelGPT is an intelligent real-time AI-based security framework designed to detect, analyze, and respond to security threats in both cybersecurity and physical surveillance environments. The system integrates machine learning, deep learning, and Generative Pre-trained Transformer (GPT) models to monitor network traffic, system logs, CCTV video streams, and IoT sensor data. By combining anomaly detection, computer vision, and natural language processing, the framework identifies suspicious activities and generates automated alerts with contextual explanations. The system ensures scalability, low latency, and reliability through real-time processing and role-based access control. ThreatSentinelGPT enhances situational awareness, minimizes false positives, and reduces response time, making it suitable for smart cities, enterprises, and critical infrastructure protection.

KEYWORDS

ThreatSentinelGPT, Cybersecurity, Physical Surveillance, Real-Time Threat Detection, Artificial Intelligence, Automated Alerts

INTRODUCTION

The rapid advancement of digital technologies has significantly increased security risks across cyber and physical

domains. Cyber threats such as malware, phishing, ransomware, and unauthorized access continue to evolve, while physical threats like intrusion, suspicious behaviour, and surveillance breaches pose serious safety concerns. Traditional security systems operate independently and rely heavily on rule-based detection and manual monitoring, which limits their ability to respond to modern, complex threats. ThreatSentinelGPT introduces a unified AI-driven framework that integrates cybersecurity monitoring with physical surveillance. The system employs machine learning models to detect anomalies in network traffic and system logs, deep learning techniques for analyzing real-time video feeds, and GPT-based natural language processing for intelligent threat interpretation. This integrated approach enables faster detection, automated alert generation, and improved decision-making, ensuring a proactive and adaptive security solution.

LITERATURE REVIEW

Several studies have explored AI-based intrusion detection systems using machine learning and deep learning techniques. Signature-based and anomaly-based IDS solutions have been widely adopted; however, they often fail to detect zero-day attacks. Research in physical surveillance has focused on object detection, facial recognition, and activity recognition using convolutional neural networks. Recent advancements in NLP and transformer-based models have shown potential in analyzing security logs and generating human-readable threat reports. However, most existing solutions address cybersecurity and physical surveillance separately. There is limited research on unified frameworks that combine AI-driven cyber threat detection with intelligent physical surveillance and automated alerting mechanisms.

RELATED WORK

Earlier security systems relied on centralized monitoring tools such as firewalls, IDS, and SIEM platforms for cybersecurity, while physical security depended on CCTV-based monitoring with human supervision. Some studies proposed blockchain-based security logging and hybrid cyber-physical security models, but these approaches suffer from high complexity, scalability issues, and delayed response times. Recent works have introduced AI-based automation in security monitoring, yet they lack contextual understanding and real-time correlation between cyber and physical threats. ThreatSentinelGPT overcomes these limitations by integrating GPT-based

intelligence to correlate events, generate meaningful alerts, and provide real-time threat explanations.

EXISTING METHOD

Existing security solutions primarily use rule-based detection techniques and isolated monitoring systems. Cybersecurity tools depend on predefined signatures and fixed thresholds, which are ineffective against sophisticated and zero-day attacks. Physical surveillance systems require continuous human monitoring, making them prone to errors, fatigue, and inefficiency. These systems lack real-time integration between cyber and physical data, automated alert generation, and intelligent threat correlation. As a result, they produce high false-positive rates, delayed incident responses, and limited situational awareness.

PROPOSED METHOD

The proposed ThreatSentinelGPT framework integrates AI-driven threat detection across cyber and physical environments. The system collects real-time data from network logs, servers, endpoints, CCTV cameras, and IoT sensors. Machine learning models detect anomalies in cyber data, while deep learning-based computer vision models analyze video feeds for suspicious physical activities. A GPT-based intelligence module processes detected events, correlates multi-source data, and generates contextual threat descriptions. Automated alerts are sent to security personnel through dashboards, email notifications, and mobile alerts. Role-based access control and encrypted communication ensure system security and data integrity.

ARCHITECTURE

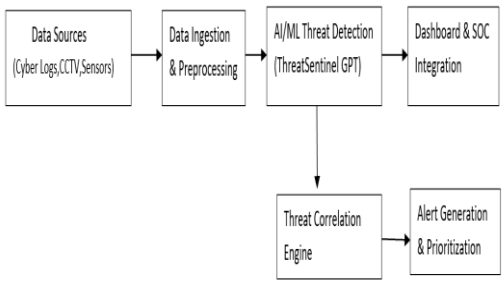


Fig1: System Architecture

The system architecture of ThreatSentinelGPT, showing the flow of data from cyber logs and CCTV sensors through data ingestion and preprocessing to AI/ML-based threat detection.

METHODOLOGY DESCRIPTION

The methodology begins with real-time data collection from cybersecurity and physical surveillance sources. Data preprocessing removes noise and normalizes inputs. Machine learning models identify cyber anomalies, while

deep learning models detect suspicious activities in video streams. The GPT module analyzes detected events, generates human-readable threat summaries, and assigns severity levels. Automated alerts are triggered based on threat priority, and all incidents are logged for auditing and future analysis. The server-based architecture ensures scalability and low-latency performance.

RESULTS AND DISCUSSION



Fig2: Home Page

The home page of ThreatSentinelGPT introduces the real-time AI-based security framework for detecting cyber and physical threats. It provides a simple interface with options to view system details, sign in for authorized access, and sign up for new users. The page ensures secure and user-friendly entry into the system.

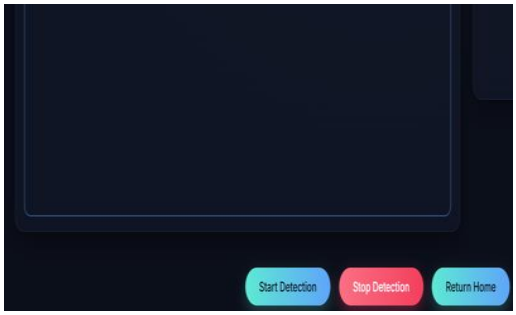


Fig3: Surveillance Display Area

Surveillance Display Area displays the live CCTV feed used for real-time detection of suspicious activities. Detection starts with the Start Detection button, stops with Stop Detection, and Return Home navigates back to the main page.



Fig4: Recent Alerts

Recent Alerts Section displays real-time alert notifications generated by the AI system. Each alert shows the type of threat, severity level (HIGH or CRITICAL), date and time of detection, and a brief description such as unauthorized human presence, abnormal posture, or aggressive movement patterns detected.



Fig5: Real-Time Person and Object Detection in CCTV Surveillance

The figure.5 shows real-time object detection where the AI model identifies a person and a cell phone from the CCTV feed, highlighting them with bounding boxes to indicate human presence and object recognition.



Fig.6: Fall Detection and Abnormal Behaviour Identification

The figure.6 shows abnormal behaviour detection, where the system identifies a fall event and labels it as *"Fall Detected"*, indicating a critical physical security or safety incident that requires immediate attention.



Fig7: Alert Messages

Figure.5 shows the alert messages generated by ThreatSentinelGPT during real-time surveillance. Each image is a captured CCTV frame saved when suspicious activity is detected, with bounding boxes indicating identified human presence. These alerts help security personnel visually verify threats such as unauthorized access or abnormal behaviour.

CONCLUSION

ThreatSentinelGPT provides an intelligent, unified security framework for real-time threat detection and automated alert generation. By integrating machine learning, deep learning, and GPT-based intelligence, the system enhances situational awareness, reduces response time, and improves overall security effectiveness across cyber and physical domains.

FUTURE SCOPE

Future enhancements include blockchain-based secure incident logging, advanced biometric authentication, predictive threat analytics, and mobile-based monitoring applications. These improvements will further increase scalability, intelligence, and global applicability of the system.

REFERENCES

1. Ramachandran, V., Kumari, Y. S., & Harini, P. (2016). Image retrieval system with user relevance feedback. *Computer Science*

Engineering, St. Anns College of Engineering, Chirala.

2. Sommer, R., & Paxson, V. (2010). Outside the closed world. IEEE Security & Privacy.
3. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys.
4. Buczak, A. L., & Guven, E. (2016). ML methods for cybersecurity intrusion detection. IEEE Surveys.
5. Stallings, W. (2018). Network Security Essentials. Pearson.
6. Redmon, J., & Farhadi, A. (2018). YOLOv3: An incremental improvement. arXiv.
7. Girshick, R. (2015). Fast R-CNN. ICCV.
8. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
9. Vaswani, A., et al. (2017). Attention is all you need. NeurIPS.
10. Brown, T., et al. (2020). Language models are few-shot learners. NeurIPS.
11. Scarfone, K., & Mell, P. (2007). Guide to intrusion detection systems. NIST.
12. Sultani, W., et al. (2018). Real-world anomaly detection in surveillance videos. CVPR.
13. Ahmad, I., et al. (2020). Security automation using AI. FGCS.
14. Lin, Z., et al. (2023). GPT for cybersecurity intelligence. Computers & Security.
15. Kumar, S., & Lim, J. (2022). Intelligent surveillance systems. Sensors.
16. Behl, A., & Behl, K. (2017). Cyberwar and cyberterrorism. Oxford Press.
17. Zyskind, G., & Nathan, O. (2015). Blockchain-based security logging. IEEE Security.
18. Alrashdi, I., et al. (2021). Smart city surveillance using AI. Sustainable Cities.
19. Xu, X., et al. (2024). Unified cyber-physical security frameworks. Journal of Information Security.
20. Zhang, Y., et al. (2022). AI-driven threat detection systems. IEEE Access.