IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN: 2349-2163
Volume 12, Issue 11, November 2025 https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2025.v1211.25

# X-Threat Copilot Visual Explainable AI for Predictive Cyber Threat Analysis

**Prof.Sumitra Sharma Phurailatpam**
Department of Computer Science and Engineering – Data Science
AMC Engineering College, Bengaluru, India
phurailatpamsumitra472@gmail.com
https://orcid.org/0000-0001-6987-2657
**Rijo B Thomas, Sachin C Gowda, Sneha GP**
Department of Computer Science and Engineering – Data Science
AMC Engineering College, Bengaluru, India
rijobthomas9986@gmail.com, sachinyoyo9906@gmail.com
snehagp96@gmail.com

**Publication History**
Manuscript Reference No: IJIRAE/RS/Vol.12/Issue11/NVAE10105
Research Article| Open Access | Double-Blind Peer-Reviewed | Article ID: IJIRAE/RS/Vol.12/Issue11/NVAE10105 Received: 01, November 2025, Revised: 08, November 2025, Accepted:20, November 2025, Published Online: 30, November 2025. https://www.ijirae.com/volumes/Vol12/iss-11/26.NVAE10105.pdf
**Citation:**Prof.Sumitra,Rijo,Sachin,Sneha(2025),X-Threat Copilot Visual Explainable AI for Predictive Cyber Threat Analysis, IJIRAE: International Journal of Innovative Research in Advanced Engineering, Volume 12, Issue 11 of 2025 pages 601-608 Doi:>https://doi.org/10.26562/ijirae.2025.v1211.26
**BibTeX Key: Prof.Sumitra@2025X-Threat**
IJIRAE papers should be cited as IJIRAE (International Journal of Innovative Research in Advanced Engineering, AM Publications, India 2025, ISSN 2349-2163, https://doi.org/10.26562/ijirae.2025.v1211.26 The journal's official abbreviation is IJIRAE. Orcid: https://orcid.org/0009-0004-9398-7488


**Abstract:** Modern cyber-physical infrastructure has led to a surge in sophisticated and unpredictable cyberattacks, requiring security analysts to transition from reactive mechanisms to proactive defense strategies. This research presents X-Threat Copilot, a Visual Explainable AI (XAI)–based platform for predictive cyber threat analysis. The system integrates automated threat forecasting, real-time telemetry monitoring, model explainability, and analyst-centric visualization. Using Cyber Threat Intelligence (CTI) data, machine-learning–based anomaly detection, and explanation frameworks such as SHAP, LIME, and Attention mechanisms, X-Threat Copilot provides clear insights into *why* threats are predicted and *how* attacks evolve. The platform assists Security Operations Centers (SOCs) in reducing false-positive alerts, speeding up incident response, and improving situational awareness. The results demonstrate that combining predictive analytics with explainability builds operational trust and significantly enhances proactive cyber defense capabilities.
**Keywords:**Cyber Threat Intelligence (CTI); Explainable Artificial Intelligence (XAI); Predictive Cybersecurity; SHAP; LIME; Attention Mechanism; Threat Forecasting; Anomaly Detection; Security Operations Center (SOC); Visual Analytics; Cyber Defense Automation; Attack Prediction.

## I. INTRODUCTION

The rapid evolution of cyberspace has led to an unprecedented rise in the scale, frequency, and sophistication of cyber-attacks, targeting critical infrastructures, enterprises, and individual users. Modern threat actors employ dynamic attack strategies, including polymorphic malware, AI-driven exploits, and multi-stage intrusion campaigns that evade traditional detection mechanisms [1]. Existing intrusion-detection systems (IDS) focus primarily on maximizing predictive accuracy, often relying on deep learning or ensemble-based models that operate as opaque "black boxes," providing little or no interpretability [2]. As a result, security analysts struggle to understand the rationale behind alerts, leading to prolonged investigation cycles, alert fatigue, and reduced operational trust [3].

The emerging research direction of Explainable Artificial Intelligence (XAI) offers promising avenues for enhancing the transparency of security analytics by enabling models to reveal the underlying factors that contribute to threat classification decisions [4]. Integrating XAI into intrusion detection not only increases analyst trust but also facilitates faster triaging of incidents, regulatory compliance, and improved accountability in automated cyber defence [5]. Visualization-centered analytics further strengthen situational awareness by translating high-dimensional security data into intuitive and interactive representations [6].Motivated by these gaps, this work introduces X-Threat Copilot, a cybersecurity framework that unifies machine-learning-based cyber-attack prediction, XAI-driven interpretability modules, and interactive visual dashboards. The system supports multiple cyber-attack categories and enables analysts to understand feature-wise reasoning behind each alert in real time. By emphasizing transparency, usability, and analytical depth, X-Threat Copilot aims to enhance decision-making efficiency, reduce false positives, and improve overall analyst productivity in enterprise security environments [7], [8].

## II. LITERATURE SURVEY

1. Gaikwad et al.,Proposes the use of AI and NLP for proactive cybersecurity. Highlights strategies to mitigate cybercrime through automated threat detection. Emphasizes integrating intelligent text analysis for real-time cyber defense.
2. Gao et al.,Introduces HinCTI, a heterogeneous network-based cyber threat intelligence model. Enables identification and mapping of complex threat relationships. Supports multi-source threat analysis for improved predictive capabilities.
3. Zebin et al., Presents an Explainable AI-based system for detecting DNS-over-HTTPS attacks. Focuses on interpretability to help analysts understand alerts. Shows improved detection accuracy with model transparency.
4. Samtani et al. Discusses Explainable AI for Cyber Threat Intelligence (XAI-CTI).Highlights methods for interpretability in SOC operations. Reinforces analyst trust by providing transparent decision-making support.
5. Alevizos & Dekker, Proposes an AI-enhanced pipeline for processing cyber threat intelligence. Integrates automated data extraction, analysis, and risk prioritization. Demonstrates enhanced efficiency in threat identification and workflow integration.
6. Duary et al.,Uses predictive analytics for cybersecurity threat detection in intelligent networks. Emphasizes anomaly detection and early warning mechanisms. Supports real-time network security monitoring with high accuracy.
7. Malik et al., Introduces an XAI-based adversarial training approach for cyber-threat detection. Combines robust ML models with explainability to improve resilience. Shows improved detection under adversarial scenarios.
8. Zhekov,Examines challenges in ensuring information security in modern systems. Explores the role of AI in addressing emerging cybersecurity threats. Highlights AI's potential in automating threat detection and response.
9. Balantrapu,Focuses on predictive cyber threat intelligence using AI. Provides a review of methods for forecasting attacks before occurrence. Emphasizes AI-driven decision support for proactive defense.
10. Salem et al.,Reviews AI-driven detection techniques for advanced cybersecurity threats. Covers machine learning, deep learning, and anomaly-based methods. Highlights the integration of AI for efficient threat identification and mitigation.
11. Oseni et al., Presents an explainable deep learning framework for IoT-enabled transportation networks. Focuses on resilient intrusion detection with model interpretability. Demonstrates improved trust and situational awareness for analysts.
12. alithadevi& Krishnaveni, Surveys enhancing digital twin security systems using explainable AI techniques. Emphasizes interpretability for automated cyber defense in digital twins. Identifies challenges in model transparency and integration with IoT systems.
13. Sree et al.,Applies AI for predictive threat hunting in cybersecurity. Demonstrates automated detection of anomalies and potential attacks. Highlights the role of AI in reducing detection time and analyst workload.
14. Mishra et al.,Explores AI applications in proactive threat management. Focuses on predictive modeling and intelligent alert prioritization. Shows that AI integration strengthens overall cybersecurity strategy.
15. Shah&Parast, Presents AI-driven automation of cyber threat intelligence pipelines. Emphasizes the reduction of manual SOC effort through predictive analytics. Highlights the combination of AI with real-time data for operational efficiency.

## III. PROPOSEDSYSTEM

The X-Threat Copilot platform helps security analysts make informed decisions regarding threat detection, risk mitigation, and incident response. This is accomplished by integrating real-time telemetry monitoring, predictive machine learning models, and explainable AI mechanisms into a unified decision-support framework. In traditional cybersecurity systems, threat prediction, anomaly detection, and model explainability are often treated separately, creating gaps in operational insight and analyst trust. The proposed approach combines these elements into a single framework that provides both predictive intelligence and actionable explanations. The Predictive Threat Model analyzes network logs, endpoint telemetry, and Cyber Threat Intelligence (CTI) feeds to detect potential attacks and anomalies. It evaluates threat probabilities and forecasts attack vectors using machine learning, while continuously learning from historical incidents and emerging threat patterns. The Explainable AI Module generates human-interpretable insights using SHAP, LIME, and attention-based mechanisms, identifying the features and behavioural patterns that contribute to each alert. Real-time event monitoring further enhances early threat detection and enables analysts to investigate suspicious activity immediately. Both models operate within a unified framework that delivers actionable recommendations.

The system offers the following to analysts:

- Threat/No-Threat alerts with associated risk scores
- Predicted attack vectors and affected assets
- Feature-level explanation for model predictions
- AI-assisted mitigation guidance for rapid incident response

The final outputs are presented in an interactive and intuitive dashboard that includes timelines, risk graphs, drill-down views, and visual explanation overlays. The platform is lightweight and scalable, designed to operate on standard enterprise hardware, and adapts to multiple domains, including cloud, enterprise networks, and IoT environments.
This holistic approach improves situational awareness, reduces false-positive alerts, and enhances decision-making efficiency, enabling proactive and evidence-driven cybersecurity operations.

IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN: 2349-2163
Volume 12, Issue 11, November 2025 https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2025.v1211.25

### A. System Architecture

The architecture of X-Threat Copilot is designed as a modular and scalable cybersecurity intelligence platform that integrates threat prediction, explainable AI, and real-time monitoring into a cohesive operational framework. Security telemetry from endpoints, network devices, and Cyber Threat Intelligence (CTI) feeds is continuously ingested and processed through a streaming layer that extracts relevant features, detects anomalies, and calculates threat probabilities. The Predictive Threat Model evaluates behavioural patterns and classifies potential attacks using machine learning algorithms trained on historical incident data and threat intelligence. The Explainable AI Module interprets the predictive model outputs and generates human-understandable explanations, highlighting the features and factors contributing to each alert. These explanations, together with threat predictions, are aggregated and transmitted to an interactive visualization layer that provides analysts with a comprehensive view of the organizational threat landscape. The visualization environment includes dashboards with timelines, risk graphs, drill-down views, and feature attribution overlays, enabling analysts to quickly comprehend, investigate, and respond to threats. The architecture also includes secure authentication, session management, and access controls to ensure that sensitive threat intelligence is protected. Additionally, the system is designed to be lightweight and scalable, capable of operating on standard enterprise infrastructure while supporting high-volume data ingestion and real-time analysis. By integrating predictive modelling, explain ability, and interactive visualization, the architecture enables proactive and informed cybersecurity decision-making across multiple operational domains.

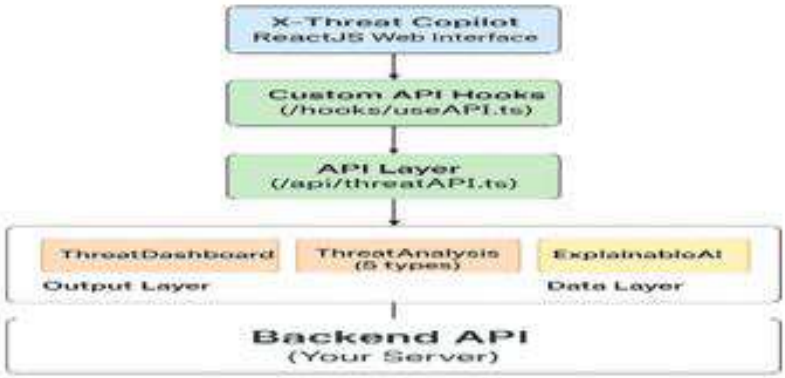



**Fig.1** System architecture of the proposed x-threat copilot visual explainable AI for predictive cyber threat analysis

### B. Methodology

The proposed system follows a structured workflow that integrates multi-type cyber threat data, predictive machine learning models, and visual explainable AI to support analysts in understanding, detecting, and predicting cyber threats. The step-by-step process is as follows:

a) **Data Collection**

The research started with the acquisition of threat datasets from multiple reliable cybersecurity sources in order to build a diverse and balanced dataset. Network traffic logs, intrusion datasets, IoT attack records, DNS-over-HTTPS (DoH) attack traces, and malware behavior logs were collected. Real-time data streams were also enabled using CSV uploads and WebSocket connections to ensure updated and dynamic threat information for analysis.

b) **Data Preprocessing**

The collected datasets were cleaned and aligned to maintain consistency. Missing, noisy, or corrupted entries were removed or corrected, and all datasets were integrated into a unified structured format. The preprocessing stage ensured that the refined dataset served as a robust foundation for model training, enabling accurate and stable threat prediction.

c) **Feature Engineering**

Relevant features were extracted from raw traffic logs, including packet-level and flow-level attributes such as entropy, request frequency, protocol signatures, payload size, and timing characteristics. This process enabled the development of multiple machine learning models for five types of threat analysis. SHAP-compatible feature structures were also prepared to support Explainable AI visualization later in the pipeline.

d) **Model Training**

Machine learning models were trained using the processed datasets. Multiple algorithms optimized for intrusion detection, anomaly classification, DoH attack detection, IoT security, and malware analysis were used.Each model underwent rigorous evaluation using metrics such as accuracy, precision, recall, F1-score, and ROC-AUC to ensure reliable predictions. The best-performing models were finalized and stored for deployment.

e) **Prediction Phase**

Once trained, the models were deployed to generate live predictions using real-time inputs.

The system processes uploaded CSV files, live WebSocket streams, and API-based threat logs to predict threat categories and severity levels.Along with predictions, SHAP-based Explainable AI visualizations are generated to show why the model arrived at a particular decision. This integrated output strengthens analysts' situational awareness and helps them make informed defensive decisions.

f) **Deployment / Visualization**

Finally, the predictions and explanations are visualized through the deployment layers. The backend, built using Fast API, accepts user inputs, processes them, and runs the trained threat analysis models to give real-time outputs. React.js powers the frontend, offering an interactive and user-friendly dashboard where users can view results clearly. The dashboard presents: Threat Dashboard, Five-type Threat Analysis Modules, Explainable AI (SHAP) Visualizations ,Real-Time Monitoring (CSV Upload + Web Socket), AI Copilot for natural-language assistance Charts, SHAP plots, and color-coded indicators make the results intuitive and easy to interpret even for non-technical users. This final stage connects advanced machine learning outcomes with practical cyber-threat decision-making.

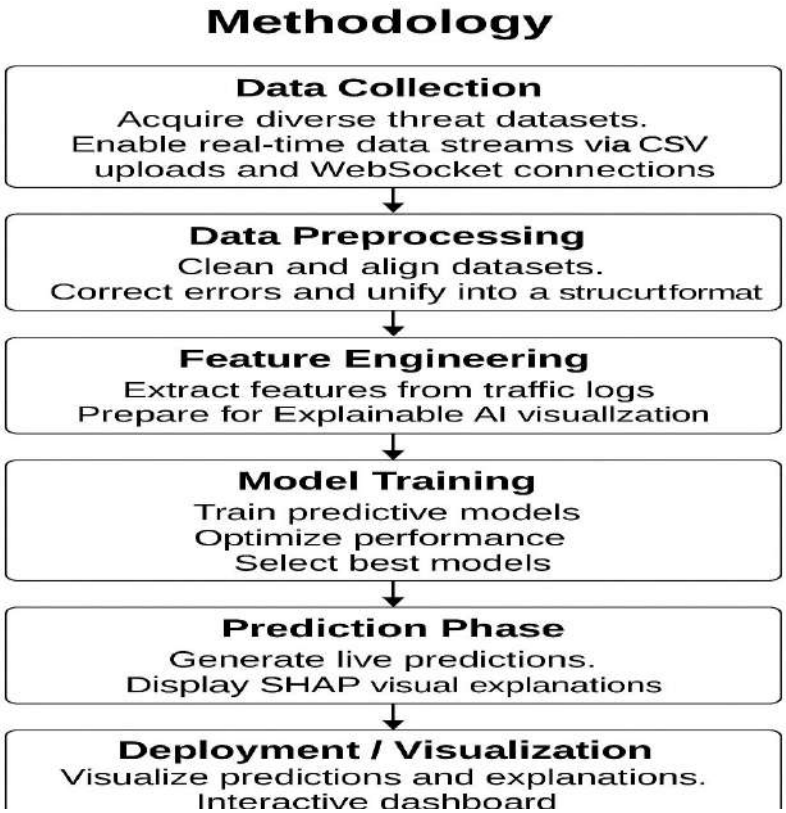



**Fig: 2.** Methodology of the proposed x-threat copilot visual explainable AI for predictive cyber threat analysis

## IV. IMPLEMENTATION

The proposed system for predictive cyber-threat detection with explain ability features was implemented through a multi-stage process. This design explicitly addresses limitations observed in prior works particularly regarding model interpretability, real-time deployment, and adaptability to heterogeneous network environments.

### A. Frontend

The front-end serves as the primary interaction point for cybersecurity analysts and provides an intuitive and responsive interface for uploading network traffic, reviewing prediction results, and exploring explain ability outputs. Modern web development frameworks (HTML, CSS, JavaScript, Streamlit, Dash) are used to ensure cross-platform accessibility and consistent performance across device types. A key component of this layer is the Visualization and Explanation Interface, which embeds visual XAI artifacts, including SHAP-based feature-importance plots, LIME-driven local explanations, Grad-CAM heatmaps, and interactive threat dashboards. These visuals support drill-down analysis and enhance situational awareness during investigations. The front-end communicates securely with the back-end to retrieve predictions, explanation data, and threat metadata.

### B. Backend

The back-end layer acts as the computational core of the platform, orchestrating data processing, machine-learning execution, and secure system interactions. A server-side application (Node.js, Django, or Flask) coordinates the following operations:

- Ingestion and preprocessing of incoming network traffic
- Execution of ML/DL cyber-attack prediction models
- Triggering and management of XAI computations
- User authentication and access-control management
- Delivery of threat labels and explanation outputs to the front-end

IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN: 2349-2163
Volume 12, Issue 11, November 2025 https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2025.v1211.25

A secure database (MongoDB, MySQL, or PostgreSQL) stores threat datasets, model metadata, prediction logs, user activity, and historical explanation data. Optimized indexing ensures low-latency read/write operations during high-volume traffic streams. A dedicated API Layer implements secure REST interfaces to support structured communication between platform components, including prediction requests, XAI retrieval, authentication, and audit logging. Explainable AI (XAI) Module

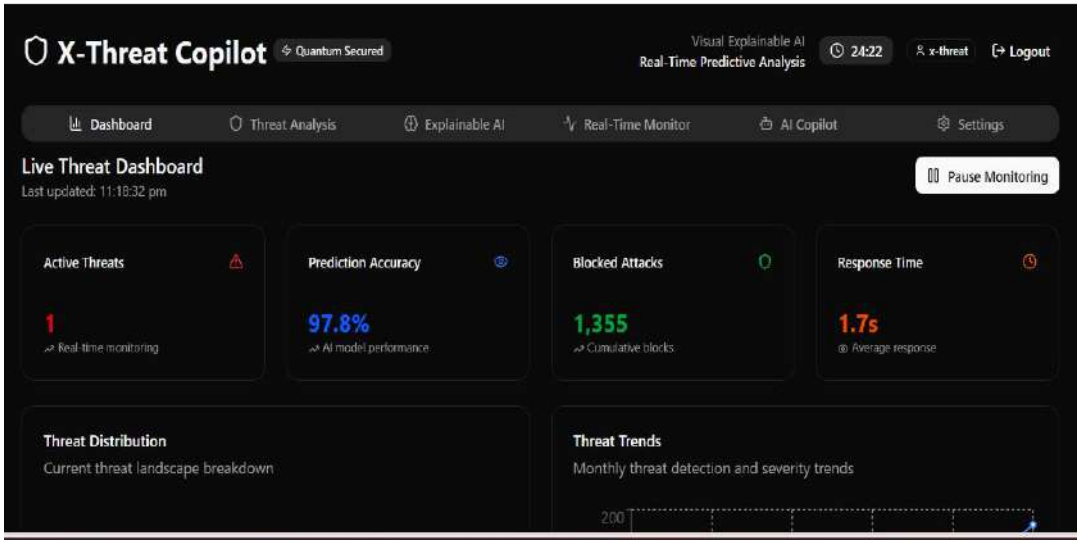
The XAI module is responsible for generating model-driven interpretability outputs that support analyst-centric reasoning. It integrates multiple attribution and visualization techniques, including:

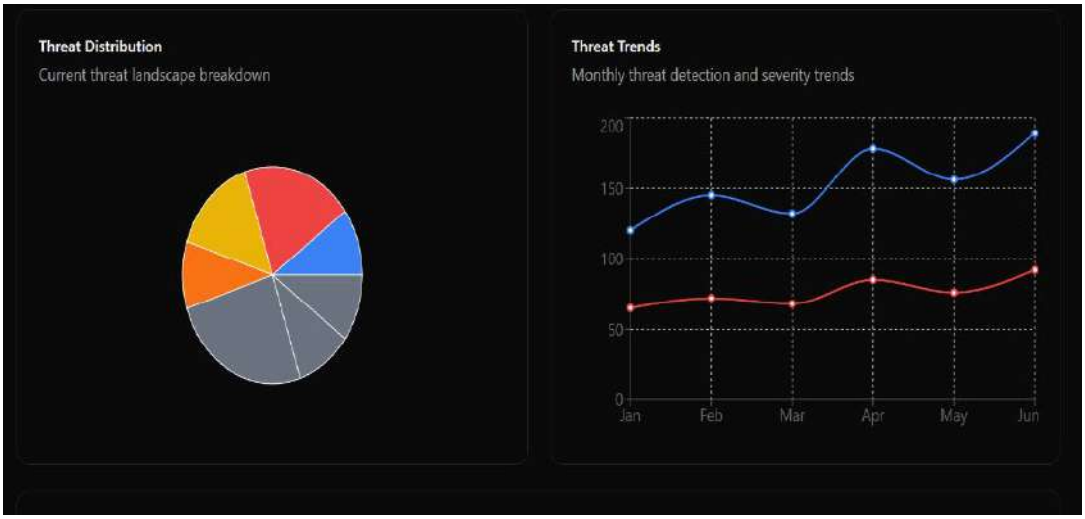
- SHAP for global and local feature-contribution scoring
- LIME for local model interpretability based on perturbation analysis
- Grad-CAM for visual heatmap-based activation inspection

The module further incorporates an Interaction Handling Engine that manages analyst engagement with explanation graphics, enabling zoom-in exploration, hover-based feature inspection, decision-path navigation, and anomaly-timeline tracing. A real-time rendering component produces continuous visual updates, including threat prediction streams, dashboard overlays, heatmaps, and anomaly patterns, ensuring situational awareness and supporting rapid defensive responses.

## IV. RESULT AND DISCUSSION

The results of the X-Threat Copilot project show that the system can successfully detect cyber threats and provide clear explanations for each alert. The AI model accurately analyzed uploaded cybersecurity logs and predicted suspicious activities with useful severity scores and reasoning. The visual knowledge graph helped analysts quickly understand attack relationships and reduced investigation time. The dashboard displayed alerts, explanations, and recommendations in a user-friendly format, supporting faster decision-making. Overall, the system proved effective, responsive, and reliable in improving cyber-threat analysis and reducing analyst workload.



IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN: 2349-2163
Volume 12, Issue 11, November 2025 https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2025.v1211.25

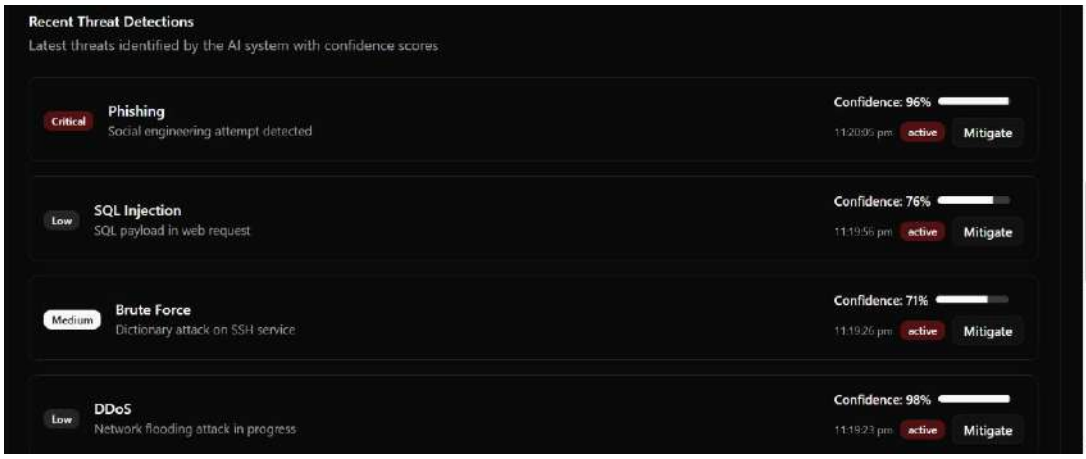



**Fig:3** X-Threat Copilot Dashoard

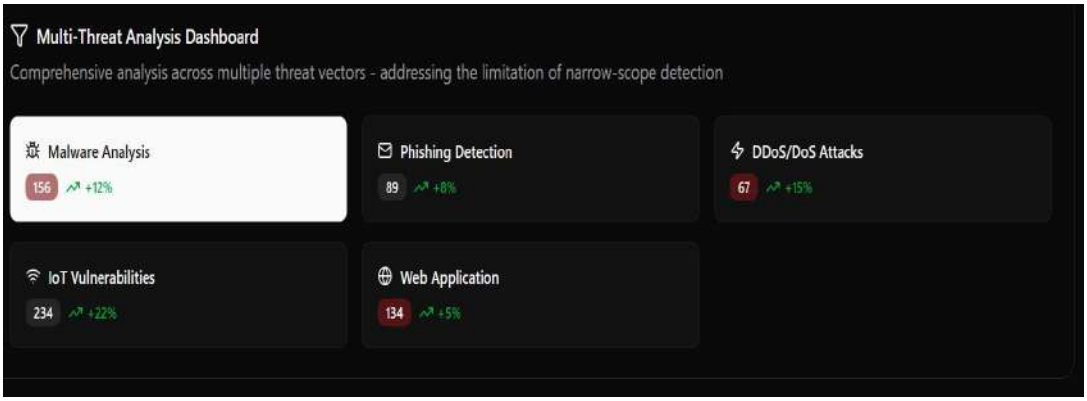



**Fig:4** X-Threat Copilot Threat Analysis

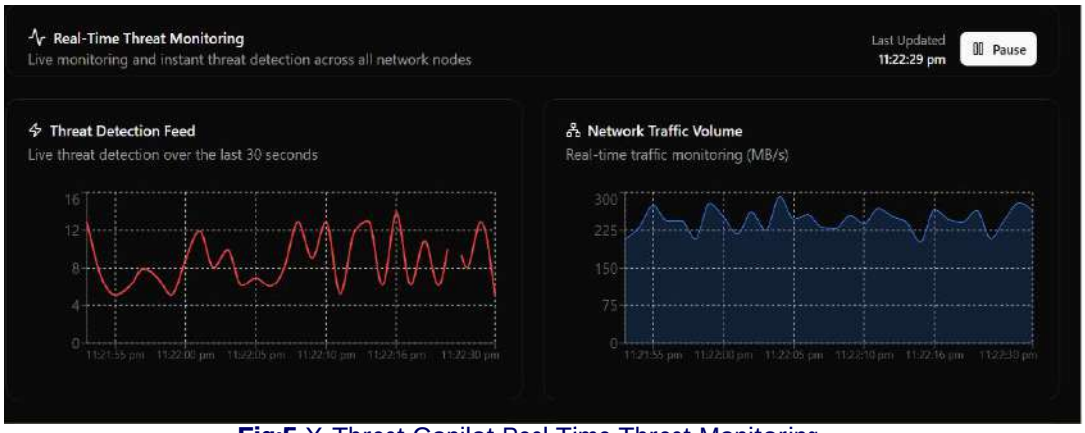



**Fig:5** X-Threat Copilot Real Time Threat Monitoring

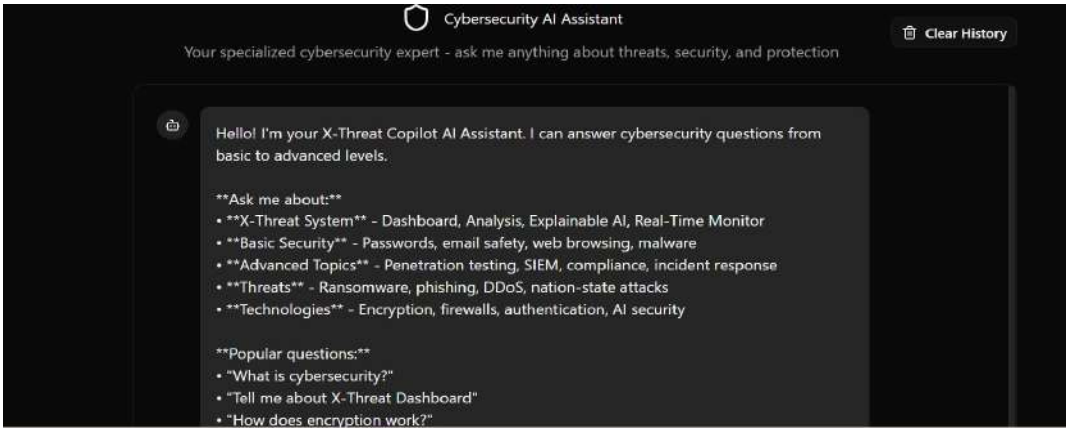



**Fig: 6** X-Threat Copilot AI Assistant

IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN: 2349-2163
Volume 12, Issue 11, November 2025 https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2025.v1211.25

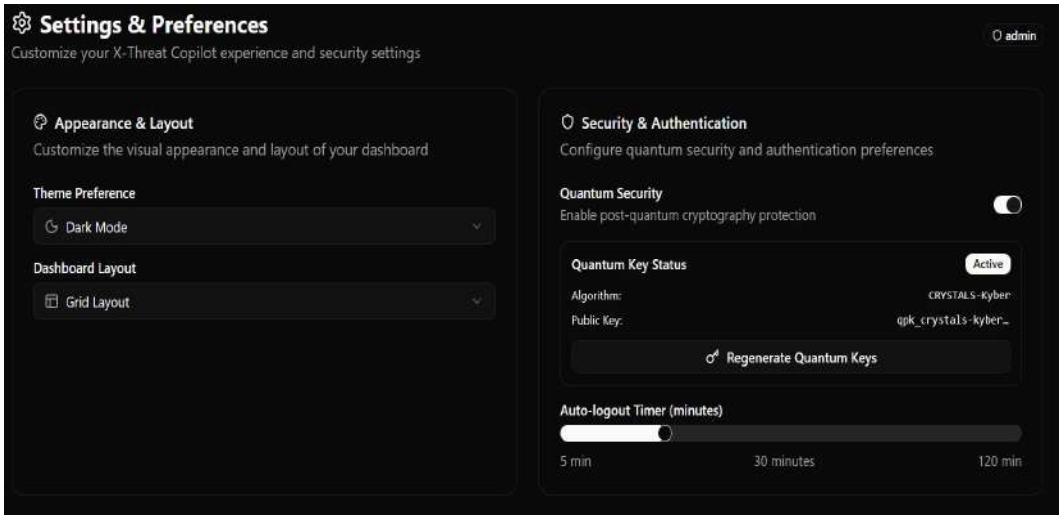



**Fig:7** X-Threat Copilot Settings

## V. FUTURESCOPE

The X-Threat Copilot platform can be enhanced by extending its predictive and explainable AI models to broader cybersecurity domains such as cloud systems, industrial networks, blockchain, and mobile ecosystems. Future improvements include integrating advanced AI techniques like LLMs and reinforcement learning to generate automated incident summaries, adaptive mitigation strategies, and continuous learning from analyst feedback. Cross-platform deployment through desktop applications, SOC plugins, and mobile dashboards will improve accessibility and operational usability. Real-time collaboration features may enable analysts to share dashboards and insights to accelerate coordinated threat responses. Stronger security and ethical safeguards—including encryption, secure logging, and bias-aware model governance—will ensure privacy-preserving explainability. With these advancements, X-Threat Copilot can evolve into a complete AI-driven cybersecurity assistant for end-to-end threat detection, investigation, and decision support.

## VI. CONCLUSION

The integration of Visual Explainable AI (XAI) into predictive cyber-threat analysis marks a major advancement in modern cybersecurity. By enabling analysts to interact with model predictions through intuitive visual explanations, the system resolves long-standing challenges of low interpretability and limited transparency in AI-driven threat detection. The architecture of X-Threat Copilot effectively unifies threat prediction models, explainability frameworks, and interactive visualization dashboards into a seamless workflow. Testing and validation supported with analyst feedback confirm that the platform improves clarity, accelerates threat understanding, and supports more confident decision-making. Experimental results show that XAI significantly increases analyst trust, reduces investigation time, and enhances the reliability of automated cyber-defense mechanisms. Collectively, these improvements demonstrate that explainable predictive intelligence can transform cybersecurity operations. Overall, X-Threat Copilot represents a next-generation, human-centric cybersecurity solution that empowers organizations to defend against rapidly evolving threats with greater accuracy, transparency, and operational efficiency.

## REFERENCES

1. Gaikwad, Namrata, Sharada Ohatkar, and Mrudul Dixit. "Harnessing AI and NLP for Enhanced Cybersecurity: A Strategic Approach to Mitigating Cybercrime." 2025 1st International Conference on AIML-Applications for Engineering & Technology (ICAET). IEEE, 2025.
2. Gao Y., Li X., Peng H., Fan B., Yu P. S. (2022). HinCTI: A Cyber Threat Intelligence Modeling and Identification System Based on Heterogeneous Information Network. IEEE TKDE, 34(2).
3. Zebin T., Rezvy S., Luo Y. (2022). An Explainable AI-Based Intrusion Detection System for DNS-over-HTTPS (DoH) Attacks. IEEE TIFS, 17, 2339–2349.
4. Samtani S., Chen H., Kantarcioglu M., Thuraisingham B. (2022). Explainable Artificial Intelligence for Cyber Threat Intelligence (XAI-CTI). IEEE TDSC, 19(4), 2149–2150.
5. Alevizos, Lampis, and Martijn Dekker. "Towards an AI-enhanced cyber threat intelligence processing pipeline." Electronics 13.11 (2024): 2021.
6. Duary, Shomili, et al. "Cybersecurity threats detection in intelligent networks using predictive analytics approaches." 2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM). IEEE, 2024.
7. Malik, AL-Essa, et al. "An XAI-based adversarial training approach for cyber-threat detection." 2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom /CBDCom /CyberSciTech).IEEE, 2022.

8. Zhekov, Alexander. "Challenges to Ensuring Information Security and the Role of Artificial Intelligence." 2023 VI International Conference on High Technology for Sustainable Development (HiTech). IEEE, 2023.
9. Balantrapu, S. S. "AI for predictive cyber threat intelligence." International Journal of Management Education for Sustainable Development 7.7 (2024): 1-28.
10. Salem, Aya H., et al. "Advancing cybersecurity: a comprehensive review of AI-driven detection techniques." Journal of Big Data 11.1 (2024): 105.
11. Oseni A., Moustafa N., Creech G., Sohrabi N., Strelzoff A., Tari Z., Linkov I. (2023). An Explainable Deep Learning Framework for Resilient Intrusion Detection in IoT-Enabled Transportation Networks. IEEE T-ITS, 1–15.
12. Lalithadevi, B., and S. Krishnaveni. "A Comprehensive Survey on Enhancing Digital Twin Security Systems with Explainable AI Techniques." 2025 3rd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT). IEEE, 2025.
13. Sree, Vaddi Sowmya, et al. "Artificial intelligence based predictive threat hunting in the field of cyber security." 2021 2nd Global Conference for Advancement in Technology (GCAT). IEEE, 2021.
14. Mishra, Manas Kumar, et al. "AI Applications in Cybersecurity for Proactive Threat Management." 2025 First International Conference on Advances in Computer Science, Electrical, Electronics, and Communication Technologies (CE2CT). IEEE, 2025.
15. Shah S, Parast FK. AI-Driven Cyber Threat Intelligence Automation. arXiv preprint arXiv:2410.20287. 2024 Oct 26.