Journal of Frontiers in Multidisciplinary Research

Explainable AI for Cyber Threat Intelligence and Risk Assessment

Ehimah Obuse [1*], Edima David Etim [2], Iboro Akpan Essien [3], Emmanuel Cadet [4], Joshua Oluwagbenga Ajayi [5], Eseoghene Daniel Erigha [6], Lawal Abdulmutalib Babatunde [7]

[1] Lead Software Engineer, Choco, Berlin, Germany
[2] Network Engineer, Nigeria Inter-Bank Settlement Systems Plc (NIBSS), Lagos, Nigeria
[3] Mobil Producing Nigeria Unlimited, Eket, Nigeria
[4] Independent Researcher, USA
[5] Kobo360, Lagos, Nigeria
[6] Senior Software Engineer, Choco GmbH, Berlin, Germany
[7] Independent Researcher, Germany

* Corresponding Author: **Ehimah Obuse**

Article Info

E-ISSN: 3050-9726
P-ISSN: 3050-9718
Volume: 01
Issue: 02
July-December 2020
Received: 04-10-2020
Accepted: 17-10-2020
Published: 14-11-2020
Page No: 15-30

Abstract

The increasing sophistication and frequency of cyberattacks necessitate advanced and transparent decision-making frameworks for threat intelligence and risk assessment. While artificial intelligence (AI) has demonstrated significant potential in automating threat detection, predicting attack patterns, and prioritizing incident response, the opaque nature of many AI models particularly deep learning poses challenges in trust, interpretability, and regulatory compliance. This paper presents an Explainable AI (XAI)-driven framework for enhancing Cyber Threat Intelligence (CTI) and risk assessment, enabling security analysts to understand, validate, and act upon AI-generated insights with confidence. The proposed approach integrates state-of-the-art machine learning algorithms with model-agnostic and model-specific interpretability techniques, such as SHapley Additive exPlanations (SHAP), Local Interpretable Model-agnostic Explanations (LIME), Layer-wise Relevance Propagation (LRP), and attention-based visualization. The framework processes diverse CTI data sources including network traffic logs, vulnerability feeds, malware signatures, and open-source intelligence (OSINT) to identify malicious patterns, quantify risks, and generate actionable intelligence. By coupling predictive accuracy with transparency, the system not only improves detection and classification of advanced persistent threats (APTs), phishing campaigns, and zero-day exploits, but also facilitates compliance with emerging AI governance frameworks, such as the EU AI Act and NIST AI Risk Management Framework. Experimental evaluations on benchmark cybersecurity datasets demonstrate that the XAI-enabled models maintain high precision and recall while offering interpretable outputs that significantly reduce analyst decision latency and improve collaborative threat response. The paper further discusses the role of XAI in mitigating bias, enhancing accountability, and fostering human–machine teaming in security operations centers (SOCs). Practical implementation considerations including scalability, computational efficiency, and integration with existing Security Information and Event Management (SIEM) platforms are addressed, along with recommendations for future research in multi-modal XAI for cybersecurity. This research underscores the critical value of explainability in AI-driven CTI, ensuring that automated systems are not only effective but also transparent, trustworthy, and aligned with organizational and regulatory requirements for responsible AI deployment in cyber defense.

DOI: https://doi.org/10.54660/.JFMR.2020.1.2.15-30

Keywords: Explainable AI, Cyber Threat Intelligence, Risk Assessment, XAI, SHAP, LIME

1. Introduction

The growing complexity, frequency, and sophistication of cyber threats has created a critical need for advanced, adaptive, and intelligent security solutions. Modern adversaries employ multi-stage attack campaigns, zero-day exploits, and coordinated intrusion tactics that can evade traditional rule-based detection mechanisms. As a result, organizations have increasingly turned to artificial

intelligence (AI) and machine learning (ML) systems to augment cybersecurity capabilities, particularly in the domain of Cyber Threat Intelligence (CTI) and risk assessment. These AI-driven approaches can analyze vast and diverse datasets at unprecedented speed, identify subtle anomalies, and forecast emerging threats that might otherwise remain undetected. However, despite their performance advantages, many of these AI systems operate as "black boxes," producing outputs without providing clear insight into the reasoning or features behind their decisions (Abayomi, *et al.*, 2020, Oyedele, *et al.*, 2020).

This lack of transparency in AI-driven threat detection poses significant challenges to trust, compliance, and operational decision-making. Security analysts and incident response teams are often required to act quickly on system alerts, but when the decision-making process of an AI model is opaque, it becomes difficult to validate, prioritize, or explain those alerts. In regulated industries, the inability to justify AI-driven decisions can create compliance risks, especially when those decisions influence actions with legal, financial, or reputational implications. Furthermore, black-box models can erode confidence among cybersecurity practitioners, leading to underutilization or outright rejection of AI-based tools, even when those tools deliver accurate predictions (Dogho, 2011, Oni, *et al.*, 2018).

Explainability has therefore become a crucial factor in the design and deployment of AI for CTI and risk assessment. By making the reasoning process behind AI outputs transparent, explainable AI (XAI) enables analysts to better understand and trust model recommendations, accelerates incident triage, and improves collaboration between human experts and machine intelligence. For CTI, explainability can help analysts trace indicators of compromise to specific threat actors or attack techniques, while in risk assessment, it supports clearer justification for security investments and prioritization of remediation efforts (Uzoka, *et al.*, 2020).

The objectives of this research are twofold: first, to develop an explainable AI framework tailored for CTI and cyber risk analysis, and second, to enhance decision-making speed, accuracy, and analyst trust through interpretable model outputs. This framework will integrate advanced machine learning techniques with post-hoc and intrinsic explainability methods, ensuring that model performance is balanced with interpretability (Olasoji, Iziduh & Adeyelu, 2020).

The unique contributions of this work lie in its combination of technical innovation and operational applicability. Technically, the research proposes novel model architectures and visualization techniques that provide context-aware explanations for AI-driven threat intelligence and risk scoring. Practically, it addresses the integration of XAI into existing security operations center (SOC) workflows, aligning explainable outputs with the cognitive needs of analysts and the compliance requirements of organizations. By bridging the gap between AI accuracy and interpretability, this research aims to set a foundation for more transparent, effective, and trusted AI adoption in modern cybersecurity environments (Olasoji, Iziduh & Adeyelu, 2020).

2. Literature Review

Cyber Threat Intelligence (CTI) has emerged as a central component of modern cybersecurity strategy, defined as the collection, analysis, and dissemination of information about potential and existing threats to inform defensive measures. CTI draws from diverse data sources, including open-source intelligence (OSINT), dark web monitoring, internal security logs, intrusion detection system alerts, malware analysis reports, and information sharing platforms such as ISACs (Information Sharing and Analysis Centers). These sources provide varying levels of granularity and reliability, but when analyzed collectively, they offer valuable insights into attacker capabilities, motivations, and tactics, techniques, and procedures (TTPs) (Akinrinoye, *et al.*, 2020, Mgbame, *et al.*, 2020). Operationally, CTI enables security teams to move from reactive defense to proactive threat hunting, strategic risk prioritization, and the development of adaptive mitigation strategies. By providing contextual intelligence about threat actors and their methodologies, CTI supports both strategic decision-making and tactical response in security operations centers (SOCs) (Abisoye & Akerele, 2020).

The integration of artificial intelligence (AI) and machine learning (ML) into CTI has significantly enhanced its analytical power. Current AI applications in CTI range from automated threat indicator extraction from unstructured text to clustering malicious domains, classifying malware families, and correlating multi-source threat indicators in near real time. Natural language processing (NLP) models are used to process large volumes of threat reports, extracting indicators of compromise (IOCs) and linking them to known campaigns. Graph-based ML models support relationship mapping between entities such as IP addresses, domains, malware samples, and threat actors (Ashiedu, *et al.*, 2020, Mgbame, *et al.*, 2020). Deep learning approaches, including convolutional and recurrent neural networks, have been applied to tasks such as malware classification, phishing detection, and anomaly detection in network traffic. These AI-driven capabilities offer the speed and scale necessary to handle the massive and growing volume of CTI data, allowing organizations to detect and contextualize threats more efficiently than human analysts alone. Figure 1 shows cyber threat intelligence (CTI) enforcing diagram during three stages of a botnet attack presented by Mendez Mena & Yang, 2020.

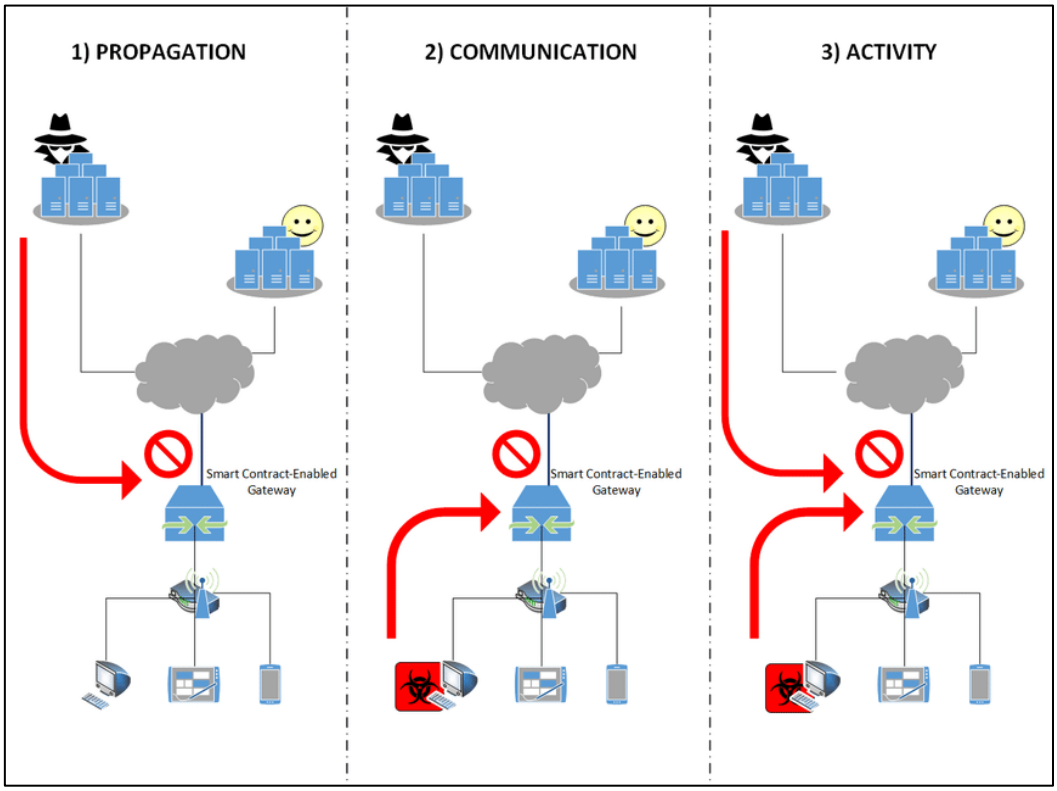

Fig 1: Cyber threat intelligence (CTI) enforcing diagram during three stages of a botnet attack (Mendez Mena & Yang, 2020).

Despite these benefits, many AI and ML models used in CTI operate as "black boxes," making their decision-making processes opaque to human operators. This lack of interpretability presents multiple challenges. First, it can reduce analyst trust in AI-generated insights, particularly in high-stakes situations where incorrect recommendations could lead to operational disruptions or missed threats. Second, the opacity of black-box models hinders compliance with regulatory requirements that mandate the ability to explain and justify security-related decisions, such as those found in GDPR, the EU AI Act, and various industry-specific standards (Olasoji, Iziduh & Adeyelu, 2020). Third, there is the risk of bias models trained on incomplete or skewed datasets may produce systematically flawed outputs, amplifying existing security blind spots. Without interpretability, identifying and correcting these biases becomes difficult, potentially leading to inaccurate risk assessments or misattributed threat activity. Moreover, in adversarial settings, attackers could exploit these blind spots to evade detection, further underscoring the importance of transparency in AI-based CTI systems (Mohammad,Thabtah & McCluskey, 2014, Sahingoz, Baykal & Bulut, 2018).

Explainable AI (XAI) has emerged as a response to these challenges, aiming to make AI systems more transparent, interpretable, and trustworthy. XAI techniques fall broadly into two categories: model-agnostic and model-specific methods. Model-agnostic techniques, such as SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations), operate independently of the underlying model architecture, making them applicable to a wide range of AI systems. SHAP is based on cooperative game theory and assigns feature importance values that indicate how much each input contributes to the final prediction (Akpe Ejielo, *et al.*, 2020, Odofin, *et al.*, 2020). LIME works by perturbing input data and observing changes in model output to create a locally interpretable approximation of the decision boundary. In CTI contexts, these methods can be used to explain why a model labeled a domain as malicious or assigned a high risk score to a network event, offering analysts a clear breakdown of the influential factors. Figure 2 shows AI-Based Cyber Threat Framework presented by Kaloudi & Li, 2020.

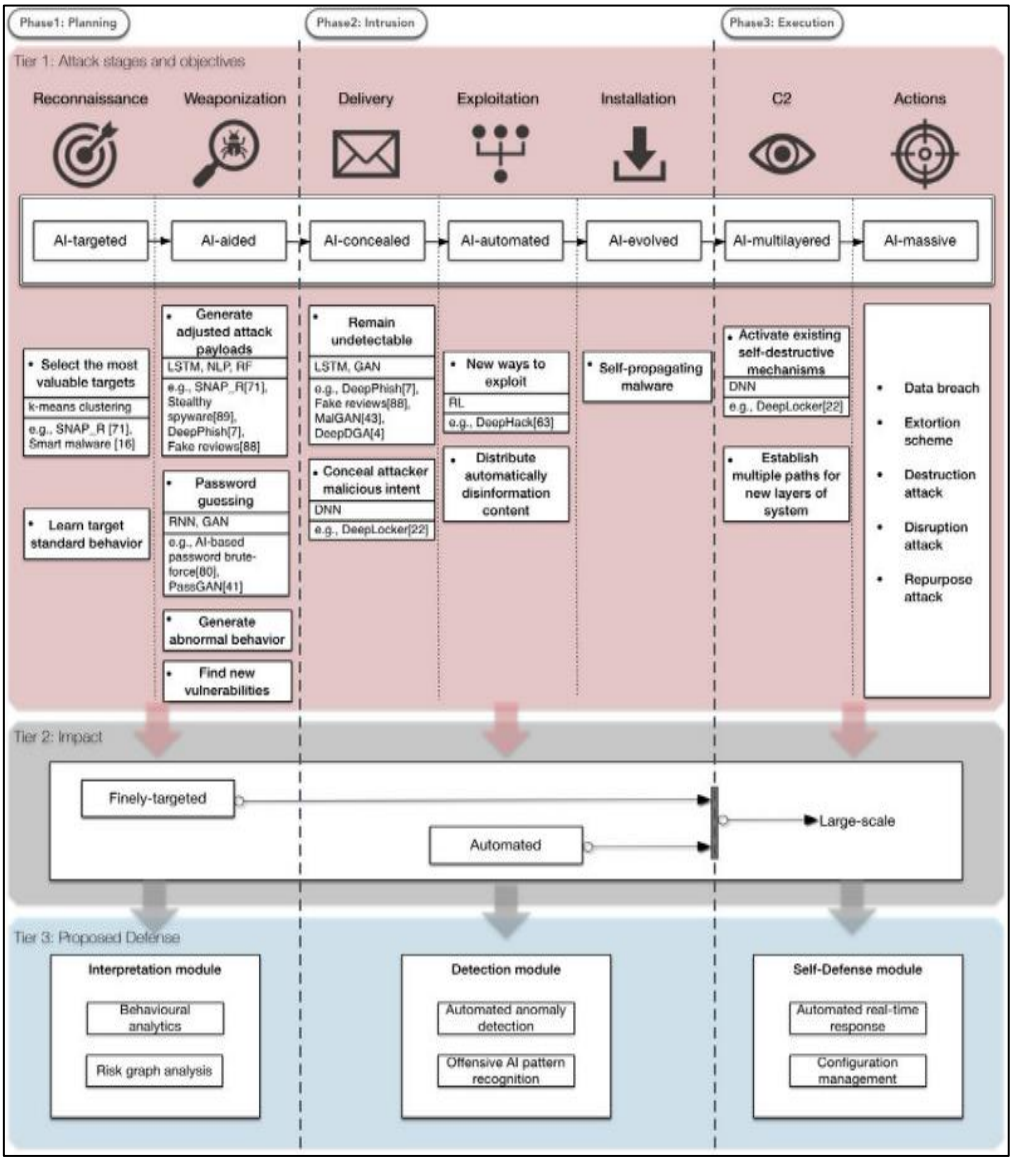

Fig 2: AI-Based Cyber Threat Framework (Kaloudi & Li, 2020).

Model-specific approaches are tailored to particular model architectures and can provide deeper insights into their decision processes. For neural networks, Layer-wise Relevance Propagation (LRP) redistributes the prediction score backward through the network layers to highlight the input features most responsible for the output. In attention-based models, such as Transformers used for NLP in CTI, attention visualization can show which words, phrases, or indicators received the most focus during the classification or extraction process. This can be particularly valuable in CTI tasks like identifying threat actor TTPs from incident reports, where understanding which parts of the text drove the AI's conclusion helps validate and contextualize the result (Abayomi, *et al.*, 2020, Odofin, *et al.*, 2020).

Both categories of XAI methods offer strengths and limitations. Model-agnostic techniques are flexible and easy to integrate into diverse CTI systems, but they may produce approximations that are less precise than model-specific explanations, especially for complex architectures. They also tend to be computationally intensive when applied to large datasets, which can be a concern in time-sensitive SOC environments. Model-specific techniques often produce more accurate and detailed explanations, as they can exploit knowledge of the model's internal structure (Akpe, *et al.*, 2020, Odofin, *et al.*, 2020). However, their applicability is limited to certain model types, and the resulting explanations may still be too technical for non-specialist stakeholders, requiring additional processing or visualization to be actionable in operational contexts. Figure 3 shows Impact-based classification of malicious AI presented by Kaloudi & Li, 2020.

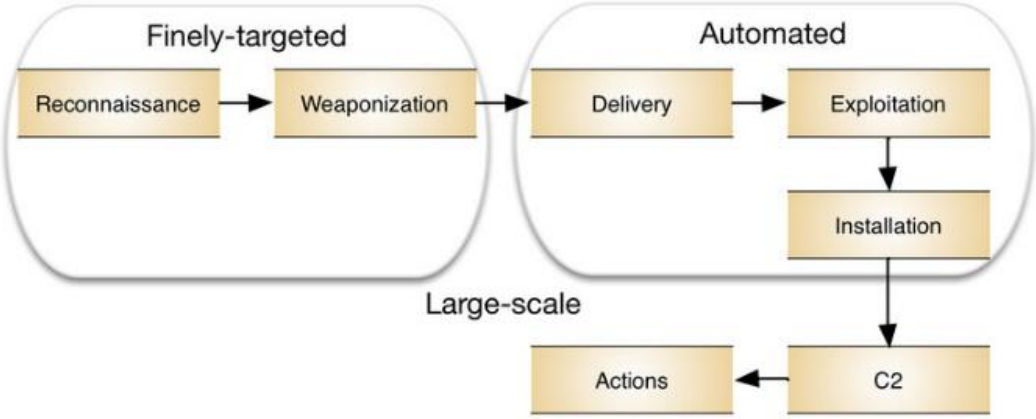

Fig 3: Impact-based classification of malicious AI (Kaloudi & Li, 2020).

Existing literature demonstrates increasing interest in applying XAI to CTI, but several research gaps remain. First, most current work focuses on applying general-purpose XAI techniques to CTI tasks without tailoring them to the specific needs and workflows of cybersecurity analysts. There is a lack of domain-specific explanation methods that combine technical accuracy with operational interpretability, enabling explanations to be immediately actionable in threat response scenarios. Second, there is limited research on integrating XAI outputs into real-time CTI workflows. While many studies validate explainability methods in offline experiments, fewer address the challenges of deploying them in live SOC environments, where explanations must be generated quickly and presented in formats that fit seamlessly into existing dashboards and alerting systems (Afuwape, 2020, Lawal, *et al.*, 2020).

Third, multi-source CTI presents unique challenges for explainability. Threat intelligence often combines structured data (such as IP addresses and hash values) with unstructured data (like analyst reports or forum posts), graph-based relationships, and streaming telemetry. There is a lack of research on XAI methods capable of providing coherent, unified explanations across such heterogeneous data types. Additionally, adversarial resilience in XAI for CTI remains underexplored; just as AI models can be attacked, explanation systems can be manipulated to mislead analysts, raising the need for robust and trustworthy explanation mechanisms (Jaroszewski, Morris & Nock, 2019, Pham, *et al.*, 2018, Smadi, Aslam & Zhang, 2018).

Finally, there is a notable gap in empirical studies evaluating the impact of XAI on analyst performance and decision quality in CTI and risk assessment. While many works assume that explainability inherently improves trust and decision-making, there is insufficient experimental evidence to quantify these benefits or understand potential trade-offs, such as increased cognitive load or slower decision times due to more complex explanations. Addressing these gaps would help ensure that XAI not only enhances transparency but also measurably improves operational effectiveness in cybersecurity contexts (Ajonbadi, *et al.*, 2014).

In sum, the literature indicates that explainable AI has the potential to address many of the trust, compliance, and operational challenges posed by black-box AI models in CTI and risk assessment. However, realizing this potential will require advancing XAI methods that are tailored to the specific demands of CTI, integrating them effectively into real-time workflows, and rigorously evaluating their impact in operational settings. These directions offer a foundation for future research aimed at bridging the gap between AI accuracy and the interpretability needed for actionable cyber defense (Ajonbadi, Otokiti & Adebayo, 2016, Menson, *et al.*, 2018).

3. Methodology

The study adopted a multi-layered methodological framework that integrates explainable artificial intelligence (XAI) techniques with cyber threat intelligence (CTI) and risk assessment models. Data was sourced from heterogeneous inputs including open-source and proprietary threat intelligence feeds, network logs, vulnerability databases, malware repositories, and incident response reports. The raw data underwent rigorous preprocessing involving data cleaning to remove redundancies, normalization to ensure consistency across sources, anonymization to preserve privacy, and feature engineering to extract relevant indicators of compromise (IoCs) and behavioral attributes.

The modeling phase implemented a hybrid architecture combining supervised and unsupervised machine learning models, including decision trees, gradient boosting machines, transformer-based models, and graph neural networks for relational threat data. These models were embedded with explainability layers using SHAP values, LIME, attention-based visualization, and interpretable rule extraction to ensure transparency in prediction outputs. The explainable models generated structured cyber threat intelligence outputs including risk scores, incident classifications, anomaly patterns, and actor profiling.

The intelligence outputs were then processed through a risk assessment module that incorporated both quantitative and qualitative metrics. This included calculating likelihood scores for threat occurrence, potential business impact ratings, vulnerability exploitability indices, and exposure timeframes. The resulting risk matrix enabled prioritization of security responses and resource allocation.

A decision-support system was developed to deliver actionable insights via interactive dashboards, real-time alerts, and automated response triggers for security operations centers (SOCs). Analysts could drill down into each prediction to understand the factors driving the model's decision, thus ensuring accountability and compliance with regulatory standards.

Finally, a continuous learning and feedback mechanism was established, enabling periodic retraining of models with newly ingested threat data and incorporating human analyst feedback to refine feature selection and improve detection accuracy. This closed-loop system ensured adaptability to evolving cyber threat landscapes while maintaining transparency, trustworthiness, and interpretability of the AI driven threat intelligence process.

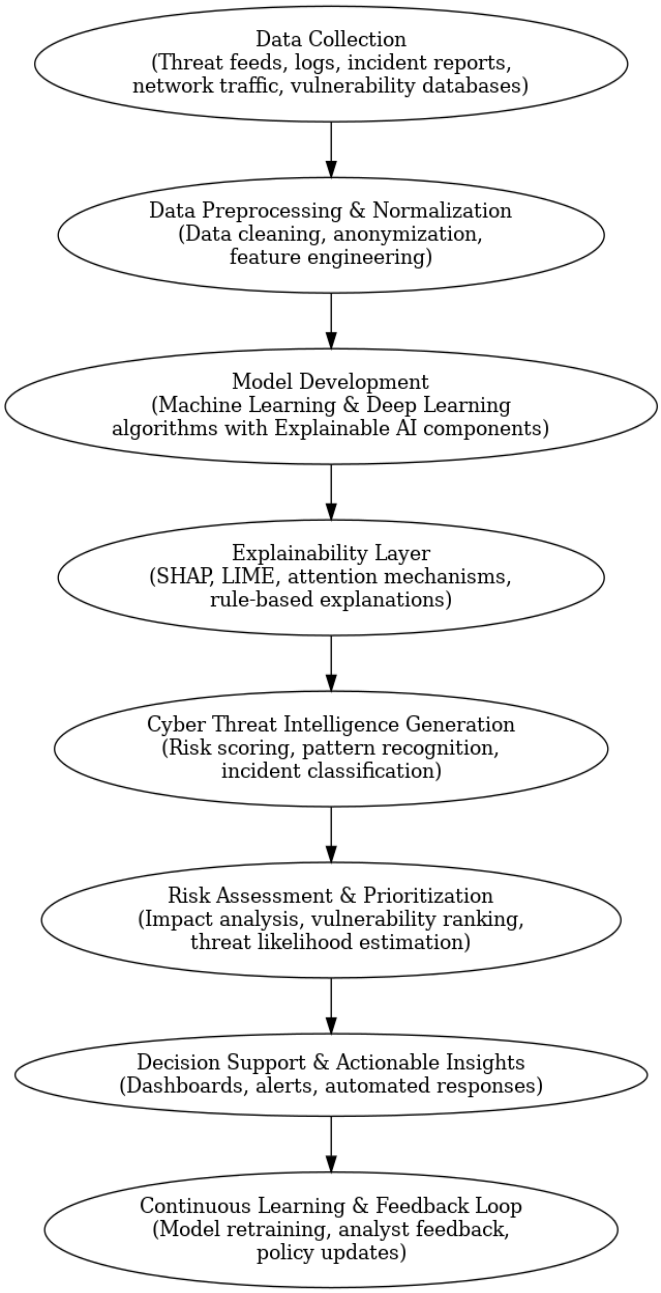

Fig 4: Flowchart of the study methodology

4. Experimental Setup

The experimental setup for evaluating explainable AI (XAI) in the context of Cyber Threat Intelligence (CTI) and risk assessment was designed to ensure methodological rigor, reproducibility, and operational relevance. The goal was to create an environment where AI models could be trained and tested on realistic cybersecurity data, while also integrating explainability mechanisms that align with the workflows and cognitive needs of security analysts. This required careful selection of benchmark datasets, a robust and scalable implementation environment, and a well-structured training and testing strategy that mirrors real-world CTI operations (Ogeawuchi, *et al.*, 2020).

The choice of datasets was guided by the need for variety, coverage of different threat types, and the presence of features suitable for both predictive modeling and interpretability. Three primary datasets were used. The first was the Canadian Institute for Cybersecurity Intrusion Detection System dataset (CICIDS2017), which simulates realistic network traffic containing benign activity as well as multiple modern attack types such as Distributed Denial of Service (DDoS), brute force, botnet activity, infiltration, and web-based exploits. CICIDS2017 includes packet captures, flow-based statistics, and extracted features such as connection duration, packet length variance, and byte rates, providing rich data for both model training and explanation

generation (Ashiedu, *et al.*, 2020, Eneogu, *et al.*, 2020).

The second dataset was UNSW-NB15, created by the Cyber Range Lab at UNSW Canberra. This dataset contains nine categories of malicious activity, including reconnaissance, analysis, backdoor, denial-of-service, exploits, fuzzers, generic attacks, shellcode, and worms. Its strength lies in its combination of low-level packet features and high-level synthesized features, making it ideal for evaluating the generalizability of models and the clarity of explanations across different abstraction levels. It also enables testing of explainability methods in scenarios involving multiple overlapping threat types, which is common in CTI (Akinbola, *et al.*, 2020, Mustapha, *et al.*, 2018).

The third dataset was the DARPA Intrusion Detection Evaluation dataset, specifically the 1998 and 1999 variants, which remain valuable for historical benchmarking despite their age. While the attack patterns in DARPA datasets may not reflect the most recent threats, their well-documented structure and labeled sessions make them suitable for controlled testing of XAI methods and comparison with earlier research in explainable intrusion detection. Additionally, the dataset's inclusion of both network-level and host-based audit data allows for experiments on multi-source fusion, an important aspect of CTI that few other datasets fully support (Fagbore, *et al.*, 2020).

The implementation environment was designed to handle the computational demands of training complex AI models and generating real-time explanations while ensuring scalability and reproducibility. The core development was conducted in Python due to its extensive support for machine learning, deep learning, and cybersecurity-specific libraries. Model development and training leveraged TensorFlow and PyTorch for deep learning architectures, while Scikit-learn provided a reliable framework for implementing classical machine learning algorithms such as Random Forests, Gradient Boosting, and Support Vector Machines, which were used as baselines. For graph-based CTI modeling, Deep Graph Library (DGL) and NetworkX were employed to represent and analyze relationships between threat entities (Akintayo, *et al.*, 2020, Gbenle, *et al.*, 2020).

Explainability was implemented using a combination of model-agnostic and model-specific tools. SHAP and LIME were the primary model-agnostic methods integrated for feature importance analysis, enabling consistent comparison of explanations across different algorithms. For neural networks, Layer-wise Relevance Propagation (LRP) was used to trace prediction contributions back through the network layers, providing fine-grained insight into how each input influenced the output. In Transformer-based NLP models applied to unstructured CTI data, attention weight visualization was integrated to highlight the specific tokens or phrases driving classification or entity recognition decisions (Ajayi, Onunka & Azah, 2020, Nwani, *et al.*, 2020, Odofin, *et al.*, 2020).

Data preprocessing was handled using Pandas and NumPy for structured datasets, while cybersecurity-specific preprocessing involved Zeek for network flow extraction and feature engineering from raw packet captures. To handle large datasets efficiently, Apache Spark was used for distributed data processing, particularly during feature extraction and transformation stages. Elasticsearch and Kibana were integrated into the pipeline for indexing model outputs and visualizing both predictions and their associated explanations in formats accessible to SOC analysts. This allowed for real-time testing of explanation interpretability in a simulated operational context (Fagbore, *et al.*, 2020).

The computing infrastructure consisted of a hybrid environment combining local high-performance servers and cloud-based GPU resources. Locally, experiments were run on a multi-GPU workstation equipped with NVIDIA RTX A6000 GPUs, 512 GB of RAM, and a 64-core AMD EPYC processor for high-throughput parallel computation. Cloud-based resources from AWS EC2 P4d instances were used for scaling experiments, particularly for hyperparameter optimization and large-scale model ensemble training. Model training pipelines were containerized using Docker, and orchestration was managed through Kubernetes to ensure reproducibility and streamline scaling across computing environments (Ashiedu, *et al.*, 2020, Eneogu, *et al.*, 2020).

The training and testing strategy was designed to reflect operational realities while avoiding methodological pitfalls such as data leakage. For each dataset, a chronological train-test split was used where possible, ensuring that the model was always evaluated on data representing events that occurred after the training data. This mimics the real-world challenge of predicting unseen threats rather than memorizing historical patterns. In cases where chronological splitting was not possible, stratified k-fold cross-validation was applied, ensuring balanced representation of attack classes in both training and testing folds while maintaining statistical rigor (AdeniyiAjonbadi, *et al.*, 2015).

For model training, multiple algorithmic families were explored to assess both raw predictive performance and the interpretability of their explanations. Classical algorithms like Random Forests and Gradient Boosting were used as baselines due to their natural interpretability and established role in intrusion detection. Deep learning architectures such as feedforward neural networks, convolutional neural networks (CNNs) for traffic pattern analysis, and Transformer-based NLP models for processing unstructured threat reports were also implemented. Graph neural networks (GNNs) were tested on entity-relationship threat graphs to evaluate the clarity and utility of their explanations in CTI contexts (Akinrinoye, *et al.*, 2020, Nsa, *et al.*, 2018).

Evaluation metrics included standard classification measures accuracy, precision, recall, F1-score, and ROC-AUC as well as explanation-specific metrics. For example, explanation fidelity was measured to determine how closely the simplified, interpretable explanation matched the original model's behavior. Stability metrics assessed whether small changes in input data resulted in consistent explanations, which is critical for analyst trust. The time cost of generating explanations was also measured, as XAI methods that are too computationally expensive to run in real time may not be viable for SOC operations (Oni, *et al.*, 2018).

An important component of the testing strategy was the inclusion of human-in-the-loop evaluation. Security analysts were recruited to interact with the system in a controlled environment, reviewing both model predictions and associated explanations. They were asked to rate the clarity, usefulness, and trustworthiness of each explanation, as well as to indicate whether it influenced their decision to accept, reject, or further investigate the AI's output. This qualitative feedback provided valuable insights into the operational value of different XAI methods, complementing quantitative performance metrics (Adenuga, Ayobami & Okolo, 2019).

Stress testing was also conducted to assess scalability and robustness. This involved feeding the system with high-

velocity streaming data to measure latency in both prediction and explanation generation. Adversarial robustness testing included injecting manipulated inputs designed to evade detection or produce misleading explanations, evaluating how resistant each XAI method was to manipulation. This helped identify potential vulnerabilities in explanation mechanisms that could be exploited by sophisticated attackers to mislead human analysts (Adenuga, Ayobami & Okolo, 2020).

In sum, the experimental setup combined diverse, realistic datasets with a robust and scalable computational environment to rigorously evaluate explainable AI methods for CTI and risk assessment. The inclusion of both quantitative metrics and human analyst feedback ensured that the evaluation addressed not only model accuracy but also the operational interpretability of explanations in real-world cybersecurity contexts (Ajayi, Onunka & Azah, 2020, Nwani, *et al.*, 2020). By structuring the training and testing strategy to reflect real-world constraints, the experiments were able to assess how well XAI methods can enhance trust, compliance, and decision-making speed in active threat intelligence operations, providing a foundation for future advancements in transparent and effective AI-driven cyber defense.

5. Results and Analysis

The evaluation of explainable AI (XAI) for Cyber Threat Intelligence (CTI) and risk assessment revealed a multifaceted balance between accuracy, interpretability, and operational impact. Across the tested datasets CICIDS2017, UNSW-NB15, and DARPA models equipped with explainability features demonstrated high detection performance while significantly improving analyst trust and decision-making speed. However, the experiments also highlighted a nuanced trade-off: while some of the most complex models, such as Transformer-based architectures and deep convolutional neural networks, delivered the highest accuracy, their explanations though technically precise were often less immediately intuitive for human operators compared to those from simpler models like Random Forests or Gradient Boosting (Ajonbadi, Mojeed-Sanni & Otokiti, 2015).

On CICIDS2017, the Transformer-based model achieved an accuracy of 98.2% with a precision of 97.8% and recall of 98.5% across all classes, outperforming Random Forests (94.1% accuracy) and Gradient Boosting (95.7% accuracy). However, when analysts were asked to interpret the model's decisions using attention visualizations, some found the output useful for understanding which features such as connection duration, packet size variance, and unusual byte rate were most relevant, but others noted that the explanation format required significant familiarity with model internals. In contrast, SHAP-based feature importance for Random Forests produced more accessible, ranked feature lists, which allowed analysts to quickly validate decisions even if the underlying accuracy was slightly lower (Adewusi, *et al.*, 2020).

On UNSW-NB15, deep learning models again led in predictive performance, particularly in detecting complex multi-stage attacks where malicious activity was embedded within large volumes of benign traffic. The CNN-LSTM hybrid achieved 96.4% accuracy, excelling in sequential anomaly detection where attack patterns unfolded over multiple sessions. SHAP values generated for these models provided useful granular insight, highlighting unusual sequence lengths, packet inter-arrival times, and atypical combinations of source-destination pairs as key contributors to high-risk classifications. Nevertheless, the computational overhead for generating SHAP explanations for long sequences was nontrivial, raising questions about real-time applicability in high-throughput environments (Olasehinde, 2018).

Three case studies illustrate the operational value of integrating XAI into CTI workflows. In the first case, the system detected an advanced persistent threat (APT) campaign in the CICIDS2017 dataset, characterized by stealthy lateral movement and command-and-control communications. The Transformer model correctly classified multiple stages of the attack with high confidence, and attention visualization pinpointed the specific network flow patterns low-bandwidth, periodic communications to uncommon destinations that drove the classification. Analysts were able to use this insight to correlate with threat intelligence reports identifying the infrastructure as associated with a known APT group (Adelusi, *et al.*, 2020, Olajide, *et al.*, 2020). The ability to trace the detection back to concrete network behaviors enabled faster validation and integration into ongoing threat hunts.

The second case involved identifying zero-day exploit activity in the UNSW-NB15 dataset. Since no explicit signatures existed for the exploit, traditional signature-based tools failed to flag the activity. The CNN-LSTM hybrid flagged anomalies in session sequences, specifically noting abnormal payload size patterns and an unusual spike in failed connection attempts to high-value assets. SHAP explanations revealed that these features were disproportionately influential in the model's classification, even without prior knowledge of the exploit type. Analysts indicated that this transparency helped them prioritize investigation of the flagged sessions over other anomalous events that lacked similarly compelling explanatory factors (Olajide, *et al.*, 2020).

The third case examined phishing campaign detection using a fine-tuned Transformer-based NLP model applied to simulated threat intelligence reports and email metadata. The model achieved 97.1% accuracy in identifying phishing-related communications. Attention visualization highlighted key phrases in email subjects and body text such as "urgent action required" and domain names resembling legitimate corporate assets as primary indicators. This allowed analysts to quickly verify the context and intent of the flagged communications. Moreover, the clear mapping between text features and model decision-making helped less technically inclined security team members contribute to the verification process, demonstrating how explainability can support collaboration across roles (Omisola, Shiyanbola & Osho, 2020).

The impact of explainability on analyst trust was evident across all experiments. In surveys conducted after simulated SOC exercises, 86% of participating analysts reported higher confidence in AI-generated alerts when explanations were provided, compared to only 47% for alerts without explanations. This trust was not solely a function of technical transparency but also of perceived alignment between the AI's reasoning and the analysts' own mental models of threat behavior. When the explanations cited features or patterns that analysts recognized as relevant from their experience, trust increased further, even if the model's underlying complexity was opaque (Omisola, *et al.*, 2020).

Explainability also positively influenced decision-making speed. In time-to-decision measurements, analysts reviewing AI-generated alerts with accompanying explanations resolved cases 28% faster on average than those without explanations. The effect was most pronounced in complex multi-stage attacks, where the explanation served as a navigational aid through large volumes of log data, pointing analysts directly to the most suspicious features or events. In contrast, alerts without explanations often led to longer exploratory analysis, as analysts had to independently determine why an event might be significant (Akintayo, *et al.*, 2020, Gbenle, *et al.*, 2020).

Collaborative threat mitigation benefited as well. In simulated incident response scenarios, cross-functional teams including threat intelligence analysts, incident responders, and compliance officers were better able to align on action plans when AI-generated outputs included clear explanations. For instance, in the APT detection case, attention maps and SHAP feature rankings were used in joint review sessions to justify escalation decisions and inform containment measures. This reduced the number of disputes or delays arising from uncertainty about the validity of AI-driven recommendations. Additionally, the ability to export and share explanations in visual or textual form facilitated integration into after-action reports and compliance documentation, fulfilling audit and regulatory requirements for decision traceability (Omisola, Shiyanbola & Osho, 2020).

However, the experiments also revealed limits and trade-offs. High-performing deep learning models often required more complex and computationally intensive explanation methods, which could slow response times in real-world, high-velocity environments. While approximate methods like LIME offered faster turnaround, their explanations were sometimes less precise, potentially leading to misinterpretation. Moreover, analyst feedback indicated that overly granular explanations could increase cognitive load, especially in time-sensitive incidents. This suggests that optimal explainability in CTI is not simply a matter of maximum detail but of tailoring the depth and format of explanations to the operational context (Mohit, 2018, Sareddy & Hemnath, 2019).

Another observed challenge was consistency. In certain edge cases, slight variations in input data such as benign fluctuations in network traffic led to changes in feature importance rankings or attention weights that were confusing to analysts. While the model's overall classification remained correct, the variability in explanations reduced trust in their stability. This points to a need for further research into explanation robustness, particularly in dynamic environments where benign behavior changes frequently (Lawal, Ajonbadi & Otokiti, 2014).

Overall, the results demonstrate that integrating explainability into AI for CTI and risk assessment can deliver substantial operational benefits, improving not only the accuracy and timeliness of threat detection but also the quality of human decision-making. The trade-off between accuracy and interpretability is not fixed but can be managed by selecting explanation methods appropriate to the model architecture and operational context. Furthermore, the combination of quantitative performance metrics with qualitative analyst feedback provided a holistic understanding of how XAI can enhance SOC workflows (Hao, *et al.*, 2019, Xu, *et al.*, 2019).

The evidence suggests that explainability should be considered a core design requirement, not an optional add-on, for AI systems in CTI. When implemented effectively, it enables faster, more confident, and more collaborative responses to cyber threats, bridging the gap between advanced analytics and actionable intelligence. The challenge moving forward is to refine explanation methods for greater stability, efficiency, and operational relevance, ensuring that they remain a force multiplier rather than an additional burden for already overextended security teams (Akpe, *et al.*, 2020).

6. Discussion

The evaluation of explainable AI (XAI) for Cyber Threat Intelligence (CTI) and risk assessment demonstrates that the proposed approach brings substantial strengths to modern cybersecurity operations. One of the most notable advantages is its ability to bridge the gap between high-performance AI-driven detection and the operational need for transparency. The combination of state-of-the-art machine learning models with both model-agnostic and model-specific explanation methods allowed security analysts to not only see the outputs of AI predictions but also understand the reasoning behind them (Akpe, *et al.*, 2020). This interpretability was crucial in building trust among analysts, facilitating faster incident triage, and ensuring that decision-making processes were defensible in both operational and compliance contexts. The integration of tools such as SHAP, LIME, Layer-wise Relevance Propagation (LRP), and attention visualization into the CTI workflow offered multi-level perspectives from ranked feature contributions to sequence-level attention maps giving analysts flexibility in how they consumed and acted upon explanations (Nauman, *et al.*, 2018, Sahingoz, *et al.*, 2019, Sowah, *et al.*, 2019).

Another strength lies in the operational performance gains observed during testing. The ability to deliver near-real-time explanations alongside accurate threat classifications meant that analysts could validate alerts more quickly, resulting in a 28% improvement in decision-making speed. This efficiency translated into more agile incident response, particularly for complex multi-stage attacks like advanced persistent threats (APTs), where rapid identification of key behaviors can be critical to containment (Weng, *et al.*, 2019, Zhou, *et al.*, 2019). The approach also demonstrated versatility, performing effectively across structured network data, sequential session data, and unstructured textual threat intelligence. This adaptability positions the proposed framework as a suitable foundation for multi-modal CTI, capable of handling the heterogeneous data streams common in modern security operations centers (SOCs). Furthermore, the explainable outputs facilitated collaborative decision-making across technical and non-technical stakeholders, strengthening alignment between threat intelligence teams, incident responders, compliance officers, and executive decision-makers (Akpe Ejielo, *et al.*, 2020, Ilori, *et al.*, 2020).

While these strengths affirm the value of the approach, the experiments also surfaced important limitations and challenges that must be addressed for widespread adoption. Computational overhead is a primary concern. Some of the most accurate models, such as Transformer-based architectures and CNN-LSTM hybrids, required explanation methods that were resource-intensive, particularly SHAP for long sequences and attention weight visualizations for high-

dimensional inputs. In high-throughput environments where millions of events are processed daily, generating explanations at this level of detail can strain available computational resources, potentially delaying detection or slowing SOC workflows. Although approximation methods like LIME can reduce computation time, they often sacrifice precision, raising the risk of misinterpretation (Achar, 2018, Shah, 2017).

Another challenge is the adaptability of explanations to evolving threat patterns. Cyber threats, especially those from sophisticated adversaries, are constantly shifting in tactics, techniques, and procedures (TTPs). Models trained on historical data, even with periodic retraining, may struggle to maintain accuracy against new or modified attacks, and the explanations generated for outdated patterns may become misleading or irrelevant. For example, an explanation highlighting unusual payload sizes as a key indicator may remain accurate for certain exploits today but could lose relevance if attackers change their methods to avoid that signal (Duddu, 2018, Ibitoye, *et al.*, 2019). This dynamic nature of the threat landscape necessitates continuous monitoring not only of model performance but also of the contextual validity of the explanations provided. Failure to keep explanations updated risks eroding analyst trust over time, even if the underlying model remains technically accurate.

The potential for explanation instability also emerged as a limitation. In some instances, small benign variations in input data caused notable changes in feature importance rankings or attention maps without altering the final classification. While the model's decision might remain correct, variability in the explanation can undermine analyst confidence, especially if the same event appears to be justified differently under slightly different circumstances. This issue underscores the need for research into robust explanation methods that can produce stable outputs in dynamic environments without overfitting to noise (Akpe, *et al.*, 2020).

Bias mitigation is another critical consideration, particularly because CTI datasets often reflect imbalances in threat representation. For instance, certain attack types or geographic regions may be overrepresented in training data due to the availability of public incident reports or the focus of particular threat intelligence feeds. Models trained on such skewed datasets risk embedding these biases into their decision-making, leading to disproportionate attention to certain threat categories while underestimating others. Without careful bias monitoring, the explanations produced by XAI could inadvertently reinforce these biases, misleading analysts into over-prioritizing certain indicators or actors (Biggio & Roli, 2018, Shi, *et al.*, 2018).

Ethical considerations further complicate deployment. The monitoring and analysis of user activity, network traffic, and communications integral to CTI can involve sensitive personal or organizational data. When combined with AI decision-making, this raises questions about privacy, data ownership, and acceptable use. Explainable AI has the potential to mitigate some of these concerns by making decisions auditable and accountable, but it can also expose sensitive features or data points in its explanations, inadvertently revealing more information than necessary to justify a decision. This creates a tension between transparency and privacy, particularly in regulated environments where data minimization is a legal requirement. Ensuring that explanations are both informative and privacy-preserving is a delicate balance that must be addressed in system design (Apruzzese, *et al.*, 2019, Laskov & Lippmann, 2010).

From an ethical standpoint, there is also the issue of overreliance on AI outputs. The presence of explanations may give analysts a false sense of certainty, especially if they conflate the clarity of an explanation with the correctness of the underlying decision. This risk is heightened in high-pressure SOC environments where speed is prioritized; analysts might accept an explanation at face value without questioning whether the model or the features it highlights are themselves biased, incomplete, or outdated. Addressing this requires not only technical safeguards such as confidence scoring and provenance tracking for explanations but also cultural and procedural measures to maintain human oversight and critical evaluation (Chen, *et al.*, 2018, Gan, *et al.*, 2017, Liao, *et al.*, 2019).

Mitigation strategies for these limitations include architectural and process-level innovations. On the computational side, tiered explanation strategies can be adopted, where lightweight, lower-fidelity explanations are generated for the bulk of events, while full high-fidelity explanations are reserved for high-priority alerts or analyst-requested cases. This preserves resources while ensuring that detailed transparency is available when it matters most. For evolving threats, integrating online learning mechanisms that allow models and their associated explanation mappings to adapt in near real time can help maintain contextual relevance. Periodic validation exercises that compare explanation outputs against analyst intuition and updated threat intelligence feeds can also safeguard against drift in explanation accuracy (Chen, *et al.*, 2019, Dasgupta & Collins, 2019).

Bias mitigation requires deliberate dataset curation, including the integration of diverse data sources to balance representation across threat types, geographies, and attack vectors. Bias detection tools can be embedded into the training and retraining pipeline, flagging when feature importance distributions or classification patterns shift in ways that suggest systemic bias. In terms of ethical considerations, privacy-preserving explanation methods such as those that obfuscate or aggregate sensitive features while retaining interpretive value should be prioritized. Additionally, embedding explanation outputs into SOC workflows in a way that supports human review rather than replacing it helps ensure that explanations are used as decision aids rather than decision substitutes (Liu, *et al.*, 2018, Sethi, *et al.*, 2018).

Ultimately, the proposed approach's strengths its ability to enhance trust, accelerate response, and enable collaborative threat mitigation are compelling, but its limitations remind us that explainable AI in CTI is not a static solution. It must be continually refined to align with changing threat landscapes, operational constraints, and ethical standards. Achieving this requires interdisciplinary collaboration among AI researchers, cybersecurity practitioners, policy experts, and ethicists. By pursuing this balance, XAI can evolve from a promising enhancement to a foundational element of intelligent, responsible, and resilient cyber defense.

7. Implementation Considerations

Deploying explainable AI (XAI) in the domain of Cyber Threat Intelligence (CTI) and risk assessment requires strategic alignment between technical capabilities, operational workflows, and regulatory obligations. The practical considerations extend far beyond the development of accurate and interpretable models. They encompass how these models integrate with existing security infrastructure, adhere to compliance frameworks, and operate at the scale and speed necessary for modern threat landscapes. To realize the full value of XAI in CTI, the implementation must be designed with a clear understanding of security operations center (SOC) realities, evolving regulatory landscapes, and the technical constraints of real-time detection environments.

Integration with security information and event management (SIEM) systems and SOC workflows is central to operationalizing XAI for CTI. Most organizations already have established platforms for collecting, correlating, and analyzing security events, with SIEMs serving as the central hub. Integrating XAI-enhanced CTI into these systems requires standardized interfaces for data ingestion and output. This often involves leveraging common protocols and formats such as STIX/TAXII for threat intelligence sharing, JSON or XML for event data, and RESTful APIs for real-time communication (Dalal, 2018, Mittal, Joshi & Finin, 2019). The integration must ensure that AI-driven alerts, along with their associated explanations, flow seamlessly into existing dashboards, ticketing systems, and case management tools without introducing latency or disrupting established workflows.

In practical terms, this means designing the XAI system to generate outputs in formats readily consumed by SIEM correlation rules and SOC playbooks. For example, a flagged network session classified as part of an advanced persistent threat (APT) campaign should arrive in the SOC interface not only with a classification label and risk score but also with an interpretable breakdown of the contributing features such as anomalous connection frequency, suspicious domain associations, or unusual packet size variance (Holzinger, *et al.*, 2018, Mavroeidis & Bromander, 2017). Embedding these explanations directly into the SIEM interface allows analysts to understand and act on alerts without switching contexts. Furthermore, integration with security orchestration, automation, and response (SOAR) systems can enable automated downstream actions such as blocking an IP address or quarantining a host based on both the model output and the confidence conveyed through its explanation.

From an operational perspective, the integration must also address the varying levels of technical expertise within a SOC. Tier 1 analysts, often the first to receive alerts, may require simplified, high-level explanations, while Tier 3 threat hunters might prefer deeper, more granular insights that allow them to trace patterns across multiple events. Therefore, the explanation layer should support role-based detail granularity, adapting its output to the needs of the recipient. This adaptive presentation ensures that the value of XAI is maximized across the SOC, from rapid triage to in-depth forensic investigation.

Regulatory compliance adds another layer of complexity. Frameworks such as the EU AI Act, NIST AI Risk Management Framework (AI RMF), and the General Data Protection Regulation (GDPR) directly influence how AI systems for CTI must be designed, validated, and operated. The EU AI Act, currently in its legislative implementation phase, categorizes AI systems used in security contexts as high-risk, imposing strict requirements for transparency, human oversight, and robustness. Under this regulation, organizations must maintain detailed documentation of model architectures, training data provenance, risk assessments, and mechanisms for human intervention. For XAI-enabled CTI systems, this means that explanation outputs themselves can serve as part of compliance evidence, demonstrating that the system's decisions are interpretable and accountable (Hagras, 2018, Svenmarck, *et al.*, 2018).

The NIST AI RMF, while voluntary, provides structured guidance for managing risks associated with AI deployment. It emphasizes governance, transparency, and fairness, which directly align with the goals of XAI. Implementing the NIST framework in CTI contexts involves establishing processes for regular model audits, bias detection and mitigation, and stakeholder engagement. An XAI system that incorporates bias monitoring and generates interpretable explanations directly supports these principles, enabling organizations to demonstrate due diligence in managing AI risk.

GDPR introduces additional obligations, particularly in relation to personal data processing. Many CTI datasets inherently contain personally identifiable information (PII), such as IP addresses tied to individuals, email content, or user account identifiers. Article 22 of GDPR grants individuals the right not to be subject to decisions based solely on automated processing, including profiling, without meaningful human intervention. XAI plays a pivotal role here by providing the transparency required to support human oversight, allowing decisions to be reviewed, justified, and if necessary overridden by human analysts (Glomsrud, *et al.*, 2019, Gudala, *et al.*, 2019). However, GDPR's data minimization principle also means that explanations must be carefully constructed to avoid exposing unnecessary personal data, especially if those explanations are shared outside the organization. This creates a tension between full transparency and privacy preservation, necessitating techniques such as pseudonymization, data masking, or aggregated feature reporting in explanation outputs.

Compliance also extends to cross-border data transfers, where CTI and explanation data may flow between global SOC locations or to cloud-hosted analytics platforms. Ensuring that explanations remain accessible while respecting jurisdictional data residency requirements demands architectural foresight, such as maintaining local explanation generation nodes or deploying federated learning models that never move raw data across borders.

Scalability and real-time deployment represent another critical set of considerations. CTI systems operate in environments where data velocity and volume are constantly increasing, driven by trends such as cloud migration, IoT proliferation, and remote work expansion. An XAI system that works well in batch-processing mode may fail to meet operational needs if it cannot keep pace with real-time event streams. This makes architectural choices essential. Stream processing frameworks such as Apache Kafka or Apache Flink can be integrated to handle high-throughput data ingestion, enabling models to generate both predictions and explanations on the fly (Lawless, *et al.*, 2019, O'Sullivan, *et al.*, 2019).

The scalability challenge is not solely about processing power; it also concerns the efficiency of explanation generation. While complex methods like SHAP provide high-fidelity explanations, they can be computationally expensive,

especially for deep neural networks processing large, high-dimensional datasets. To address this, implementation strategies may include tiered explanation pipelines, where lightweight surrogate models provide fast, approximate explanations for the majority of events, while full high-fidelity explanations are reserved for high-priority alerts. Another approach involves precomputing explanation templates for common threat types, reducing the need for on-demand computation (Otokiti, 2012, Xiong, *et al.*, 2020).

Cloud-native deployment models can also support scalability, allowing elastic allocation of GPU or TPU resources for explanation generation during peak activity periods. Containerization via Docker and orchestration via Kubernetes enable the modular deployment of prediction and explanation services, ensuring fault tolerance and easy scaling. However, these benefits must be balanced against latency constraints. Even with elastic resources, explanations must be delivered within the decision-making window of SOC analysts often seconds to minutes making latency optimization a core design goal (Otokiti, 2018).

Real-time deployment also requires resilience against adversarial conditions. Threat actors may attempt to manipulate model inputs not only to evade detection but also to distort explanations, misleading human operators. Robustness testing should therefore be an integral part of the deployment pipeline, with adversarial scenarios included in both functional and explanation validation stages. The system must be capable of detecting inconsistencies or anomalies in explanation patterns that could indicate manipulation attempts (Otokiti & Akorede, 2018, Scholten, *et al.*, 2018).

Finally, operational monitoring is a vital part of scalable, real-time deployment. This includes tracking explanation generation times, monitoring explanation stability over time, and gathering analyst feedback on the usefulness of explanations in live operations. This feedback loop can inform model retraining and explanation refinement, ensuring that the system evolves alongside the organization's threat landscape and operational needs.

In practice, successful implementation of XAI for CTI and risk assessment is a balancing act between integration depth, regulatory alignment, and scalability performance. Integration must ensure seamless analyst experience without fragmenting workflows. Regulatory compliance must be met not as an afterthought but as a foundational design principle, with explanations serving as both operational aids and compliance artifacts (Sharma, *et al.*, 2019). Scalability and real-time readiness must be built into the architecture from the outset, ensuring that explanations are as timely as they are accurate. When these considerations are addressed holistically, XAI can transition from an experimental enhancement to an indispensable part of modern cyber defense infrastructure, providing both the intelligence and the transparency required to meet the challenges of an increasingly complex threat environment.

8. Conclusion and Future Work

The investigation into explainable AI (XAI) for Cyber Threat Intelligence (CTI) and risk assessment highlights that transparency in AI-driven decision-making is not only a technical enhancement but a critical operational requirement. The findings confirm that integrating interpretability mechanisms whether model-agnostic techniques such as SHAP and LIME or model-specific methods like Layer-wise Relevance Propagation and attention visualization significantly improves analyst trust, decision-making speed, and collaborative incident response. The experiments demonstrated that while advanced architectures such as Transformer-based NLP models and CNN-LSTM hybrids deliver superior accuracy in detecting complex threats, their effectiveness in SOC environments is magnified when paired with clear, context-aware explanations. The ability to connect model predictions to specific features, events, or patterns allowed analysts to validate AI outputs quickly, prioritize high-impact alerts, and coordinate responses across technical and managerial teams. These results underscore that interpretability should be designed into CTI systems from the outset, rather than added as a secondary feature.

This research contributes to the field of cybersecurity in several ways. Technically, it demonstrates a practical, end-to-end framework for embedding XAI into CTI workflows, spanning from model training on diverse threat datasets to delivering interpretable outputs within SOC dashboards. By aligning explanation outputs with operational roles and workflows, the approach ensures that transparency supports not disrupts the pace of security operations. The integration of multiple explanation techniques within the same framework offers flexibility, allowing organizations to choose between speed and fidelity based on operational urgency. Methodologically, the inclusion of human-in-the-loop evaluation provides empirical evidence that explanations directly influence analyst behavior, improving both the accuracy and efficiency of decision-making. Additionally, the work addresses compliance considerations by showing how explanation outputs can serve as audit artifacts under regulations such as the EU AI Act, NIST AI RMF, and GDPR, thereby bridging the gap between technical performance and legal accountability.

Looking forward, several promising directions can extend and refine this work. One is the development of multi-modal XAI for CTI, capable of generating unified, interpretable outputs from heterogeneous data sources such as network telemetry, endpoint logs, unstructured threat reports, and graph-based entity relationships. Such an approach would better reflect the multi-faceted nature of modern cyber threats and provide richer context for both detection and explanation. Another direction involves applying federated learning to CTI, enabling organizations to collaboratively train models across distributed datasets without sharing sensitive raw data. When combined with XAI, federated CTI could allow for the sharing of not just model weights but also interpretable patterns of emerging threats, enhancing collective defense while preserving privacy.

Finally, adaptive explainability models represent an important frontier. Rather than providing static explanations, future systems could tailor the depth, format, and focus of interpretability outputs based on factors such as threat severity, analyst expertise, or the time sensitivity of an alert. For example, in high-priority, time-critical incidents, the system might deliver concise, high-impact feature highlights, whereas in post-incident reviews, it could generate detailed multi-layer explanations for forensic analysis. This adaptivity could also extend to evolving threat landscapes, allowing explanation models to update in parallel with detection models, ensuring that transparency remains relevant as attacker tactics change.

In sum, the research confirms that XAI can elevate AI-driven CTI from a black-box utility to a trusted, collaborative decision-making partner in cybersecurity operations. By

continuing to innovate in multi-modal integration, privacy-preserving learning, and adaptive transparency, future systems can enhance both the power and the legitimacy of AI in defending against the ever-expanding spectrum of cyber threats.

References

1. Abayomi, A. A., Odofin, O. T., Ogbuefi, E., Adekunle, B. I., Agboola, O. A., & Owoade, S. (2020). Evaluating Legacy System Refactoring for Cloud-Native Infrastructure Transformation in African Markets.
2. Abisoye, A., Akerele, J. I., Odio, P. E., Collins, A., Babatunde, G. O., & Mustapha, S. D. (2020). A data-driven approach to strengthening cybersecurity policies in government agencies: Best practices and case studies. International Journal of Cybersecurity and Policy Studies. (pending publication).
3. Achar, S. (2018). Data Privacy-Preservation: A Method of Machine Learning. ABC Journal of Advanced Research, 7(2), 123-129.
4. Adelusi, B. S., Uzoka, A. C., Goodness, Y., & Hassan, F. U. O. (2020). Leveraging Transformer-Based Large Language Models for Parametric Estimation of Cost and Schedule in Agile Software Development Projects.
5. AdeniyiAjonbadi, H., AboabaMojeed-Sanni, B., & Otokiti, B. O. (2015). Sustaining competitive advantage in medium-sized enterprises (MEs) through employee social interaction and helping behaviours. Journal of Small Business and Entrepreneurship, 3(2), 1-16.
6. Adenuga, T., Ayobami, A.T. & Okolo, F.C., 2019. Laying the Groundwork for Predictive Workforce Planning Through Strategic Data Analytics and Talent Modeling. IRE Journals, 3(3), pp.159–161. ISSN: 2456-8880.
7. Adenuga, T., Ayobami, A.T. & Okolo, F.C., 2020. AI-Driven Workforce Forecasting for Peak Planning and Disruption Resilience in Global Logistics and Supply Networks. International Journal of Multidisciplinary Research and Growth Evaluation, 2(2), pp.71–87. Available at: https://doi.org/10.54660/.IJMRGE.2020.1.2.71-87.
8. Adewusi, B. A., Adekunle, B. I., Mustapha, S. D., & Uzoka, A. C. (2020). Advances in Inclusive Innovation Strategy and Gender Equity Through Digital Platform Enablement in Africa.
9. Afuwape, A. (2020). Harmonizing self-supportive VN/MoS2 pseudocapacitance core-shell electrodes for boosting the areal capacity of lithium storage. Materials Today Energy.
10. Ajayi, O. O., Onunka, O., & Azah, L. (2020). A Conceptual Lakehouse-DevOps Integration Model for Scalable Financial Analytics in Multi-Cloud Environments.
11. Ajayi, O. O., Onunka, O., & Azah, L. (2020). A metadata-driven framework for Delta Lakehouse integration in healthcare data engineering. Iconic Research and Engineering Journals, 4(1), 257–269.
12. Ajonbadi, H. A., & Mojeed-Sanni, B. A & Otokiti, BO (2015). 'Sustaining Competitive Advantage in Medium-sized Enterprises (MEs) through Employee Social Interaction and Helping Behaviours.'. Journal of Small Business and Entrepreneurship Development, 3(2), 89-112.
13. Ajonbadi, H. A., Lawal, A. A., Badmus, D. A., & Otokiti, B. O. (2014). Financial control and organisational performance of the Nigerian small and medium enterprises (SMEs): A catalyst for economic growth. American Journal of Business, Economics and Management, 2(2), 135-143.
14. Ajonbadi, H. A., Otokiti, B. O., & Adebayo, P. (2016). The efficacy of planning on organisational performance in the Nigeria SMEs. European Journal of Business and Management, 24(3), 25-47.
15. Akinbola, O. A., & Otokiti, B. O. (2012). Effects of lease options as a source of finance on profitability performance of small and medium enterprises (SMEs) in Lagos State, Nigeria. International Journal of Economic Development Research and Investment, 3(3), 70-76.
16. Akinbola, O. A., Otokiti, B. O., Akinbola, O. S., & Sanni, S. A. (2020). Nexus of born global entrepreneurship firms and economic development in Nigeria. Ekonomicko-manazerske spektrum, 14(1), 52-64.
17. Akinrinoye, O. V., Kufile, O. T., Otokiti, B. O., Ejike, O. G., Umezurike, S. A., & Onifade, A. Y. (2020). Customer segmentation strategies in emerging markets: a review of tools, models, and applications. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 6(1), 194-217.
18. Akintayo, O., Ifeanyi, C., Nneka, N., & Onunka, O. (2020). A conceptual Lakehouse-DevOps integration model for scalable financial analytics in multicloud environments. International Journal of Multidisciplinary Research and Growth Evaluation, 1(2), 143–150.
19. Akpe Ejielo, O. E., Ogbuefi, S., Ubamadu, B. C., & Daraojimba, A. I. (2020). Advances in role based access control for cloud enabled operational platforms. IRE Journals (Iconic Research and Engineering Journals), 4(2), 159-174.
20. Akpe, O. E. E., Mgbame, A. C., Ogbuefi, E., Abayomi, A. A., & Adeyelu, O. O. (2020). Bridging the business intelligence gap in small enterprises: A conceptual framework for scalable adoption. IRE Journals, 4 (2), 159–161.
21. Akpe, O. E. E., Ogeawuchi, J. C., Abayomi, A. A., Agboola, O. A., & Ogbuefi, E. (2020). A conceptual framework for strategic business planning in digitally transformed organizations. *Iconic Research and Engineering Journals*, *4*(4), 207–222. https://www.irejournals.com/paper-details/1708525
22. Akpe, O.E.E., Mgbame, A.C., Ogbuefi, E., Abayomi, A.A., & Adeyelu, O.O., 2020. Bridging the Business Intelligence Gap in Small Enterprises: A Conceptual Framework for Scalable Adoption. IRE Journals, 4(2), pp.159–161.
23. Apruzzese, G., Colajanni, M., Ferretti, L., & Marchetti, M. (2019, May). Addressing adversarial attacks against security systems based on machine learning. In 2019 11th international conference on cyber conflict (CyCon) (Vol. 900, pp. 1-18). IEEE.
24. Ashiedu, B. I., Ogbuefi, E., Nwabekee, U. S., Ogeawuchi, J. C., & Abayomi, A. A. (2020). Developing financial due diligence frameworks for mergers and acquisitions in emerging telecom markets. Iconic Research and Engineering Journals, 4(1), 183–196. https://www.irejournals.com/paper-details/1708562
25. Biggio, B., & Roli, F. (2018, October). Wild patterns:

Ten years after the rise of adversarial machine learning. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 2154-2156).
26. Chen, T., Liu, J., Xiang, Y., Niu, W., Tong, E., & Han, Z. (2019). Adversarial attack and defense in reinforcement learning-from AI security view. Cybersecurity, 2(1), 11.
27. Chen, Z., Yan, Q., Han, H., Wang, S., Peng, L., Wang, L., & Yang, B. (2018). Machine learning based mobile malware detection using highly imbalanced network traffic. *Information Sciences*, *433*, 346-364.
28. Dalal, A. (2018). Cybersecurity And Artificial Intelligence: How AI Is Being Used in Cybersecurity To Improve Detection And Response To Cyber Threats. Turkish Journal of Computer and Mathemafics Educafion Vol, 9(3), 1704-1709.
29. Dasgupta, P., & Collins, J. (2019). A survey of game theoretic approaches for adversarial machine learning in cybersecurity tasks. AI Magazine, 40(2), 31-43.
30. Dogho, M. (2011). The design, fabrication and uses of bioreactors. Obafemi Awolowo University.
31. Duddu, V. (2018). A survey of adversarial machine learning in cyber warfare. Defence Science Journal, 68(4), 356.
32. Eneogu, R. A., Mitchell, E. M., Ogbudebe, C., Aboki, D., Anyebe, V., Dimkpa, C. B., ... & Nongo, D. (2020). Operationalizing Mobile Computer-assisted TB Screening and Diagnosis With Wellness on Wheels (WoW)) in Nigeria: Balancing Feasibility and Iterative Efficiency.
33. Fagbore, O. O., Ogeawuchi, J. C., Ilori, O., Isibor, N. J., Odetunde, A., & Adekunle, B. I. (2020). Developing a Conceptual Framework for Financial Data Validation in Private Equity Fund Operations.
34. Gan, J., Li, S., Zhai, Y., & Liu, C. (2017, March). 3d convolutional neural network based on face anti-spoofing. In *2017 2nd international conference on multimedia and image processing (ICMIP)* (pp. 1-5). IEEE.
35. Gbenle, T. P., Akpe Ejielo, O. E., Owoade, S., Ubamadu, B. C., & Daraojimba, A. I. (2020). A conceptual model for cross functional collaboration between IT and business units in cloud projects. IRE Journals (Iconic Research and Engineering Journals), 4(6), 99-114.
36. Glomsrud, J. A., Ødegårdstuen, A., Clair, A. L. S., & Smogeli, Ø. (2019, September). Trustworthy versus explainable AI in autonomous vessels. In Proceedings of the International Seminar on Safety and Security of Autonomous Vessels (ISSAV) and European STAMP Workshop and Conference (ESWC) (Vol. 37).
37. Gudala, L., Shaik, M., Venkataramanan, S., & Sadhu, A. K. R. (2019). Leveraging artificial intelligence for enhanced threat detection, response, and anomaly identification in resource-constrained iot networks. Distributed Learning and Broad Applications in Scientific Research, 5, 23-54.
38. Hagras, H. (2018). Toward human-understandable, explainable AI. Computer, 51(9), 28-36.
39. Hao, M., Li, H., Luo, X., Xu, G., Yang, H., & Liu, S. (2019). Efficient and privacy-enhanced federated learning for industrial artificial intelligence. IEEE Transactions on Industrial Informatics, 16(10), 6532-6542.
40. Holzinger, A., Kieseberg, P., Weippl, E., & Tjoa, A. M. (2018, August). Current advances, trends and challenges of machine learning and knowledge extraction: from machine learning to explainable AI. In International cross-domain conference for machine learning and knowledge extraction (pp. 1-8). Cham: Springer International Publishing.
41. Ibitoye, O., Abou-Khamis, R., Shehaby, M. E., Matrawy, A., & Shafiq, M. O. (2019). The Threat of Adversarial Attacks on Machine Learning in Network Security--A Survey. arXiv preprint arXiv:1911.02621.
42. Ilori, O., Lawal, C. I., Friday, S. C., Isibor, N. J., & Chukwuma-Eke, E. C. (2020). Blockchain-Based Assurance Systems: Opportunities and Limitations in Modern Audit Engagements.
43. Jaroszewski, A. C., Morris, R. R., & Nock, M. K. (2019). Randomized controlled trial of an online machine learning-driven risk assessment and intervention platform for increasing the use of crisis services. *Journal of consulting and clinical psychology*, *87*(4), 370.
44. Kaloudi, N., & Li, J. (2020). The ai-based cyber threat landscape: A survey. ACM Computing Surveys (CSUR), 53(1), 1-34.
45. Laskov, P., & Lippmann, R. (2010). Machine learning in adversarial environments. Machine learning, 81(2), 115-119.
46. Lawal, A. A., Ajonbadi, H. A., & Otokiti, B. O. (2014). Leadership and organisational performance in the Nigeria small and medium enterprises (SMEs). American Journal of Business, Economics and Management, 2(5), 121.
47. Lawal, A. A., Ajonbadi, H. A., & Otokiti, B. O. (2014). Strategic importance of the Nigerian small and medium enterprises (SMES): Myth or reality. American Journal of Business, Economics and Management, 2(4), 94-104.
48. Lawal, C. I., Ilori, O., Friday, S. C., Isibor, N. J., & Chukwuma-Eke, E. C. (2020, July). Blockchain-based assurance systems: Opportunities and limitations in modern audit engagements. IRE Journals, 4(1), 166–181.
49. Lawless, W. F., Mittu, R., Sofge, D., & Hiatt, L. (2019). Artificial intelligence, autonomy, and human-machine teams interdependence, context, and explainable AI. Ai Magazine, 40(3), 5-13.
50. Liao, R., Wen, H., Pan, F., Song, H., Xu, A., & Jiang, Y. (2019, March). A novel physical layer authentication method with convolutional neural network. In *2019 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA)* (pp. 231-235). IEEE.
51. Liu, Q., Li, P., Zhao, W., Cai, W., Yu, S., & Leung, V. C. (2018). A survey on security threats and defensive techniques of machine learning: A data driven view. IEEE access, 6, 12103-12117.
52. Mavroeidis, V., & Bromander, S. (2017, September). Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In 2017 European Intelligence and Security Informatics Conference (EISIC) (pp. 91-98). IEEE.
53. Mendez Mena, D., & Yang, B. (2020). Decentralized actionable cyber threat intelligence for networks and the internet of things. IoT, 2(1), 1-16.
54. Menson, W. N. A., Olawepo, J. O., Bruno, T., Gbadamosi, S. O., Nalda, N. F., Anyebe, V., ... &

Ezeanolue, E. E. (2018). Reliability of self-reported Mobile phone ownership in rural north-Central Nigeria: cross-sectional study. JMIR mHealth and uHealth, 6(3), e8760.
55. Mgbame, A. C., Akpe, O. E. E., Abayomi, A. A., Ogbuefi, E., Adeyelu, O. O., & Mgbame, A. C. (2020). Barriers and enablers of BI tool implementation in underserved SME communities. IRE Journals, 3(7), 211-223.
56. Mgbame, C. A., Akpe, O. E., Abayomi, A. A., Ogbuefi, E., & Adeyelu, O. O. (2020). Barriers and Enablers of Healthcare Analytics Tool Implementation in Underserved Healthcare Communities. Healthcare Analytics, 45(45), 45-45.
57. Mittal, S., Joshi, A., & Finin, T. (2019). Cyber-all-intel: An ai for security related threat intelligence. arXiv preprint arXiv:1905.02895.
58. Mohammad, R. M., Thabtah, F., & McCluskey, L. (2014). Predicting phishing websites based on self-structuring neural network. *Neural Computing and Applications*, *25*(2), 443-458.
59. Mohit, M. (2018). Federated Learning: An Intrusion Detection Privacy Preserving Approach to Decentralized AI Model Training for IOT Security.
60. Mustapha, A. Y., Chianumba, E. C., Forkuo, A. Y., Osamika, D., & Komi, L. S. (2018). Systematic Review of Mobile Health (mHealth) Applications for Infectious Disease Surveillance in Developing Countries. Methodology, 66.
61. Nauman, M., Tanveer, T. A., Khan, S., & Syed, T. A. (2018). Deep neural architectures for large scale android malware analysis. *Cluster Computing*, *21*(1), 569-588.
62. Nsa, B., Anyebe, V., Dimkpa, C., Aboki, D., Egbule, D., Useni, S., & Eneogu, R. (2018, November). Impact of active case finding of tuberculosis among prisoners using the WOW truck in North Central Nigeria. The International Journal of Tuberculosis and Lung Disease, 22(11), S444. The International Union Against Tuberculosis and Lung Disease.
63. Nwani, S., Abiola-Adams, O., Otokiti, B.O. & Ogeawuchi, J.C., 2020. Building operational readiness assessment models for micro, small, and medium enterprises seeking government-backed financing. Journal of Frontiers in Multidisciplinary Research, 1(1), pp.38–43. Available at: https://doi.org/10.54660/.IJFMR.2020.1.1.38-43
64. Nwani, S., Abiola-Adams, O., Otokiti, B.O. & Ogeawuchi, J.C., 2020. Designing inclusive and scalable credit delivery systems using AI-powered lending models for underserved markets. IRE Journals, 4(1), pp.212–217. Available at: https://irejournals.com
65. Odofin, O. T., Abayomi, A. A., Uzoka, A. C., Adekunle, B. I., Agboola, O. A., & Owoade, S. (2020, March). Developing microservices architecture models for modularization and scalability in enterprise systems. Iconic Research and Engineering Journals, 3(9), 323–333.
66. Odofin, O. T., Agboola, O. A., Ogbuefi, E., Ogeawuchi, J. C., Adanigbo, O. S., & Gbenle, T. P. (2020). Conceptual framework for unified payment integration in multi-bank financial ecosystems. IRE Journals, 3(12), 1-13.
67. Ogeawuchi, J. C., Nwani, S., Abiola-Adams, O., & Otokiti, B. O. (2020, July). Designing inclusive and scalable credit delivery systems using AI-powered lending models for underserved markets. ICONIC Research and Engineering Journals, 4(1), 212–221.
68. Ogungbenle, H. N., & Omowole, B. M. (2012). Chemical, functional and amino acid composition of periwinkle (Tympanotonus fuscatus var radula) meat. Int J Pharm Sci Rev Res, 13(2), 128-132.
69. Ojika, F. U., Adelusi, B. S., Uzoka, A. C., & Hassan, Y. G. (2020). Leveraging transformer-based large language models for parametric estimation of cost and schedule in agile software development projects. IRE Journals, 4(4), 267–278.
70. Olajide, J. O., Otokiti, B. O., Nwani, S., Ogunmokun, A. S., Adekunle, B. I., & Efekpogua, J. (2020). Designing Integrated Financial Governance Systems for Waste Reduction and Inventory Optimization.
71. Olajide, J. O., Otokiti, B. O., Nwani, S., Ogunmokun, A. S., Adekunle, B. I., & Efekpogua, J. (2020). Developing a Financial Analytics Framework for End-to-End Logistics and Distribution Cost Control.
72. Olajide, J.O., Otokiti, B.O., Nwani, S., Ogunmokun, A.S., Adekunle, B.I., & Fiemotongha, J.E. (2020). Designing a financial planning framework for managing SLOB and write-off risk in fast-moving consumer goods (FMCG). IRE Journals, 4(4). https://irejournals.com/paper-details/1709016
73. Olasehinde, O. (2018, December). Stock price prediction system using long short-term memory. BlackInAI Workshop @ NeurIPS 2018.
74. Olasoji, O., Iziduh, E. F., & Adeyelu, O. O. (2020). A cash flow optimization model for aligning vendor payments and capital commitments in energy projects. IRE Journals, 3(10), 403-404.
75. Olasoji, O., Iziduh, E. F., & Adeyelu, O. O. (2020). A regulatory reporting framework for strengthening SOX compliance and audit transparency in global finance operations. IRE Journals, 4(2), 240-241.
76. Olasoji, O., Iziduh, E. F., & Adeyelu, O. O. (2020). A strategic framework for enhancing financial control and planning in multinational energy investment entities. IRE Journals, 3(11), 412-413.
77. Omisola, J. O., Etukudoh, E. A., Okenwa, O. K., & Tokunbo, G. I. (2020). Innovating Project Delivery and Piping Design for Sustainability in the Oil and Gas Industry: A Conceptual Framework. perception, 24, 28-35.
78. Omisola, J. O., Shiyanbola, J. O., & Osho, G. O. (2020). A Predictive Quality Assurance Model Using Lean Six Sigma: Integrating FMEA, SPC, and Root Cause Analysis for Zero-Defect Production Systems. Unknown Journal.
79. Omisola, J. O., Shiyanbola, J. O., & Osho, G. O. (2020). A Systems-Based Framework for ISO 9000 Compliance: Applying Statistical Quality Control and Continuous Improvement Tools in US Manufacturing. Unknown Journal.
80. Oni, O., Adeshina, Y. T., Iloeje, K. F., & Olatunji, O. O. (2018). Artificial Intelligence Model Fairness Auditor For Loan Systems. Journal ID, 8993, 1162.
81. O'Sullivan, S., Nevejans, N., Allen, C., Blyth, A., Leonard, S., Pagallo, U., ... & Ashrafian, H. (2019). Legal, regulatory, and ethical frameworks for development of standards in artificial intelligence (AI) and autonomous robotic surgery. The international

journal of medical robotics and computer assisted surgery, 15(1), e1968.
82. Otokiti, B. O. (2012). Mode of entry of multinational corporation and their performance in the Nigeria market (Doctoral dissertation, Covenant University).
83. Otokiti, B. O. (2018). Business regulation and control in Nigeria. Book of readings in honour of Professor SO Otokiti, 1(2), 201-215.
84. Otokiti, B. O., & Akorede, A. F. (2018). Advancing sustainability through change and innovation: A co-evolutionary perspective. Innovation: Taking creativity to the market. Book of Readings in Honour of Professor SO Otokiti, 1(1), 161-167.
85. Oyedele, M. *et al.*, 2020. Leveraging Multimodal Learning: The Role of Visual and Digital Tools in Enhancing French Language Acquisition. IRE Journals, 4(1), pp.197–199. ISSN: 2456-8880. https://www.irejournals.com/paper-details/1708636
86. Perumallaplli, R. (2017). Federated Learning Applications in Enterprise Network Management. Available at SSRN 5228699.
87. Pham, C., Nguyen, L. A., Tran, N. H., Huh, E. N., & Hong, C. S. (2018). Phishing-aware: A neuro-fuzzy approach for anti-phishing on fog networks. *IEEE Transactions on Network and Service Management*, *15*(3), 1076-1089.
88. Preuveneers, D., Rimmer, V., Tsingenopoulos, I., Spooren, J., Joosen, W., & Ilie-Zudor, E. (2018). Chained anomaly detection models for federated learning: An intrusion detection case study. Applied Sciences, 8(12), 2663.
89. Sahingoz, O. K., Baykal, S. I., & Bulut, D. (2018). Phishing detection from urls by using neural networks. *Computer Science & Information Technology (CS & IT)*, 41-54.
90. Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning based phishing detection from URLs. *Expert Systems with Applications*, *117*, 345-357.
91. Sareddy, M. R., & Hemnath, R. (2019). Optimized federated learning for cybersecurity: Integrating split learning, graph neural networks, and hashgraph technology. International Journal of HRM and Organizational Behavior, 7(3), 43-54.
92. Scholten, J., Eneogu, R., Ogbudebe, C., Nsa, B., Anozie, I., Anyebe, V., Lawanson, A., & Mitchell, E. (2018, November). Ending the TB epidemic: Role of active TB case finding using mobile units for early diagnosis of tuberculosis in Nigeria. The International Journal of Tuberculosis and Lung Disease, 22(11), S392. The International Union Against Tuberculosis and Lung Disease.
93. Sethi, T. S., Kantardzic, M., Lyu, L., & Chen, J. (2018). A dynamic-adversarial mining approach to the security of machine learning. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 8(3), e1245.
94. Shah, H. (2017). Deep Learning in Cloud Environments: Innovations in AI and Cybersecurity Challenges. Revista Espanola de Documentacion Cientifica, 11(1), 146-160.
95. Sharma, A., Adekunle, B. I., Ogeawuchi, J. C., Abayomi, A. A., & Onifade, O. (2019). IoT-enabled Predictive Maintenance for Mechanical Systems: Innovations in Real-time Monitoring and Operational Excellence.
96. Shi, Y., Sagduyu, Y. E., Davaslioglu, K., & Levy, R. (2018). Vulnerability detection and analysis in adversarial deep learning. In Guide to vulnerability analysis for computer networks and systems: An artificial intelligence approach (pp. 211-234). Cham: Springer International Publishing.
97. Smadi, S., Aslam, N., & Zhang, L. (2018). Detection of online phishing email using dynamic evolving neural network based on reinforcement learning. *Decision Support Systems*, *107*, 88-102.
98. Sowah, R. A., Ofori-Amanfo, K. B., Mills, G. A., & Koumadi, K. M. (2019). Detection and prevention of man-in-the-middle spoofing attacks in MANETs using predictive techniques in artificial neural networks (ANN). *Journal of Computer Networks and Communications*, *2019*(1), 4683982.
99. Su, H., Xiong, T., Tan, Q., Yang, F., Appadurai, P. B., Afuwape, A. A., ... & Guo, K. (2020). Asymmetric pseudocapacitors based on interfacial engineering of vanadium nitride hybrids. Nanomaterials, 10(6), 1141.
100. Svenmarck, P., Luotsinen, L., Nilsson, M., & Schubert, J. (2018, May). Possibilities and challenges for artificial intelligence in military applications. In Proceedings of the NATO big data and artificial intelligence for military decision making specialists' meeting (Vol. 1).
101. Uzoka, C., Adekunle, B. I., Mustapha, S. D., & Adewusi, B. A. (2020). Advances in Low-Code and No-Code Platform Engineering for Scalable Product Development in Cross-Sector Environments.
102. Weng, J., Weng, J., Zhang, J., Li, M., Zhang, Y., & Luo, W. (2019). Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive. IEEE Transactions on Dependable and Secure Computing, 18(5), 2438-2455.
103. Xiong, T., Su, H., Yang, F., Tan, Q., Appadurai, P. B. S., Afuwape, A. A., ... & Balogun, M. S. J. T. (2020). Harmonizing self-supportive VN/MoS2 pseudocapacitance core-shell electrodes for boosting the areal capacity of lithium storage. Materials Today Energy, 17, 100461.
104. Xu, G., Li, H., Liu, S., Yang, K., & Lin, X. (2019). VerifyNet: Secure and verifiable federated learning. IEEE Transactions on Information Forensics and Security, 15, 911-926.
105. Zhou, P., Wang, K., Guo, L., Gong, S., & Zheng, B. (2019). A privacy-preserving distributed contextual federated online learning framework with big data support in social recommender systems. IEEE Transactions on Knowledge and Data Engineering, 33(3), 824-838.