

Explainable AI-Driven Decision Intelligence for Cyber-Resilient Enterprise Operations Under Uncertainty

Md Rafat Hossain^{1*}, Tamanna Sharmin Mumu², Samina Ahmed³, Sehrish Khalil⁴

¹Seidenberg School of Computer Science and Information Systems, Pace University, New York, USA

²Senior Software Developer, Innovexa Solutions, Toronto, Canada Master of Computer Science University of Windsor, Windsor, Ontario, Canada

³M.S. in Computer Information Systems New England College, USA

⁴MS in Project Management Oklahoma Christian University, Oklahoma, USA

DOI: <https://doi.org/10.36348/sjet.2026.v11i10.002>

| Received: 12.08.2026 | Accepted: 03.10.2026 | Published: 10.10.2026

*Corresponding author: Md Rafat Hossain

Seidenberg School of Computer Science and Information Systems, Pace University, New York, USA

Abstract

Modern enterprises increasingly depend on interconnected information systems, cloud services, software applications, third party platforms, and digital business processes. This dependence creates exposure to cyber incidents, abnormal behavior, service failures, and operational disruption. Existing cybersecurity approaches often focus on threat identification without translating technical risk into business impact or actionable response priorities. This study proposes an Explainable AI Driven Decision Intelligence framework for cyber resilient enterprise operations under uncertainty. The framework integrates cybersecurity telemetry, enterprise context, dual stream predictive modeling, service criticality, dependency analysis, Business Impact Score assessment, explainable reasoning, resource constrained prioritization, and resilience response. The predictive layer processes temporal technical signals and contextual severity attributes to estimate malicious activity and disruption probabilities. TreeSHAP and rule-based reasoning provide interpretable factors, affected services, estimated consequences, and recommended actions. The framework is designed for comparative evaluation against XGBoost, SVM, standard BiLSTM, and conventional threshold alerting using predictive, operational, explainability, resource allocation, and uncertainty measures. The study provides an integrated approach for connecting cyber threat prediction with transparent operational decisions and enterprise resilience.

Keywords: Explainable Artificial Intelligence, Decision Intelligence, Cyber Resilience, Enterprise Cybersecurity, Cyber Risk Prediction, Business Impact Score, Anomaly Detection, Service Dependency Analysis.

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY-NC 4.0) which permits unrestricted use, distribution, and reproduction in any medium for non-commercial use provided the original author and source are credited.

I. INTRODUCTION

Enterprise operations increasingly depend on interconnected networks, cloud services, applications, and digital processes, creating exposure to cyber threats, abnormal behavior, service failures, and operational disruption. Existing security analytics often identify technical threats without translating them into business consequences or actionable priorities. This study addresses that gap through explainable decision intelligence connecting prediction, impact assessment, dependencies, resource allocation, and resilience actions.

A. Background and Motivation

Modern enterprises rely on interconnected information systems, cloud platforms, applications, third

party services, and digital workflows. This dependence increases exposure to cyber incidents, anomalous behavior, system failures, and service disruption. Existing security approaches often emphasize threat identification, yet operational teams also need business consequences and response priorities. Prior studies examined business impact scoring, predictive risk assessment, and operational intelligence [1], [8], [10], but these functions remain separated. The motivation is to connect cyber risk prediction with service criticality, dependency exposure, operational impact, and continuity decisions within one decision intelligence framework.

B. Problem Statement

The central problem is the absence of an integrated dynamic decision process that connects threat indicators with enterprise dependencies, business impact, and response capacity. Detection focused systems can generate excessive alerts, while threshold methods may overlook risk conditions. Explainable artificial intelligence can provide model reasoning, but existing approaches often present explanations without linking them to service criticality or continuity actions [2], [3], [7]. The problem also includes uncertainty from noisy telemetry, missing observations, changing feature distributions, model degradation, and limited analyst capacity. These conditions can reduce decision quality during incidents.

C. Proposed Solution

This study proposes an explainable AI driven decision intelligence framework that integrates telemetry with enterprise context and dependencies. A dual stream predictive architecture processes signals alongside severity attributes to estimate malicious activity and disruption probabilities. The risk layer combines threat likelihood, impact, exploitability, and vulnerability severity, while the Business Impact Score represents service severity, dependency exposure, and failure exposure. TreeSHAP and rule-based reasoning provide interpretable recommendations. Incidents are prioritized according to risk, impact, urgency, criticality, dependency exposure, and analyst capacity, supporting isolation, workload redistribution, fallback activation, escalation, and enhanced monitoring.

D. Contributions

The study makes several contributions. First, it introduces a dual stream predictive design that combines technical telemetry with enterprise context. Second, it connects cyber risk prediction with Business Impact Score calculation and service dependency assessment. Third, it integrates TreeSHAP and rule-based reasoning with constrained incident prioritization so recommendations contain factors, affected services, consequences, and response actions. It defines evaluation measures covering predictive performance, false positive rate, Impact Weighted F1, BIS accuracy, simulated response time, detection lead time, estimated loss avoidance, resource allocation efficiency, explanation quality, and stability. Ablation and sensitivity analysis assess individual component contributions.

E. Paper Organization

Section II reviews related work. Section III presents the methodology, including data preparation, prediction, risk assessment, explainability, resource allocation, and validation. Section IV discusses results and limitations. Section V presents conclusions and future research directions.

Objective of the Study

The objective of this study is to develop and assess an explainable decision intelligence framework using public cybersecurity data and synthetic enterprise scenarios, connecting cyber threat prediction, business impact, service dependencies, transparent recommendations, and resource constrained resilience actions under uncertainty.

II. Related Work

Recent research has applied artificial intelligence to cyber threat detection, business impact assessment, explainable decision support, predictive maintenance, infrastructure monitoring, and operational risk management. However, these studies generally address separate analytical functions rather than a unified decision intelligence process. This section reviews four research areas relevant to the proposed framework: business impact and risk assessment, explainable artificial intelligence, predictive operational intelligence, and secure infrastructure monitoring. The review also identifies limitations related to enterprise dependencies, operational impact, transparent recommendations, and coordinated response under uncertainty.

A. Business Impact Scoring and Risk Assessment

Recent research connects technical indicators with operational consequences. Javeed *et al.*, [1] proposed a dual stream deep learning architecture for business impact scoring and alert escalation, demonstrating the value of combining temporal information with severity attributes. Hasan [8] examined predictive analytics for business process decision support, while Rahman [10] investigated data science methods for power system risk assessment. These studies show that technical indicators can support broader operational assessment. However, they do not integrate cyber anomaly prediction, enterprise service dependencies, explainable recommendations, and resource constrained response within a single decision intelligence framework.

B. Explainable Artificial Intelligence for Cyber Decision Support

Explainable artificial intelligence has received increasing attention because predictive security models can provide limited reasoning for their outputs. Pattnaik [2] proposed an explainable artificial intelligence recommendation system for real time cyber threat mitigation, with emphasis on response suggestions. Prasad *et al.*, [3] examined explainable artificial intelligence for cyber threat detection and decision making, focusing on interpretable security analysis. Akhter *et al.*, [7] applied explainable predictive analytics to decision support. These studies provide useful foundations for transparent artificial intelligence. However, their approaches provide limited integration of service criticality, business impact, process dependency, and continuity actions within cyber operational decisions.

C. Predictive Analytics for Operational Resilience

Predictive analytics provides useful methods for anticipating failures and supporting operational planning under uncertain conditions. Karim [5] examined artificial intelligence based predictive maintenance for solar inverter systems, while Rahman *et al.*, [6] investigated machine learning approaches for predictive maintenance in Internet of Things devices. Jasem [11] presented an artificial intelligence system health dashboard for predictive maintenance and infrastructure resilience. Akter *et al.*, [4] examined digital twin technology for civil infrastructure and emergency preparedness. Taimun *et al.*, [13] studied digital twin enabled predictive maintenance for textile and mechanical systems. These studies focus mainly on physical or technical condition rather than cyber risk and enterprise decision coordination.

D. Secure Infrastructure and Cyber Health Monitoring

Research on industrial control, secure communication, and infrastructure health provides additional foundations for cyber resilient enterprise operations. Islam [9] examined safety integrated supervisory control and data acquisition systems for process hazard control, while Rabbi [12] addressed predictive fault detection and cyber health monitoring in grid environments. Zaidi *et al.*, [14] investigated blockchain secured communication for industrial Internet of Things and aviation control systems. Mirza [15] examined anomaly detection, capacity optimization, and proactive support for cloud scale business intelligence platforms. These studies address specific resilience functions, but they do not combine cyber risk, service dependencies, operational impact, explainability, and adaptive response within one integrated framework.

III. METHODOLOGY

This study develops an explainable decision intelligence framework for cyber resilient enterprise operations under uncertainty. The methodology combines cybersecurity telemetry, enterprise context, predictive modeling, dependency analysis, business impact assessment, explainable reasoning, and constrained response selection. Public cybersecurity

datasets support model development, while synthetic enterprise scenarios represent service relationships and operational consequences. The research follows five connected stages, from data preparation to experimental validation and adaptive feedback.

A. Research Design and Data Preparation

The research adopts a quantitative experimental design using public cybersecurity datasets and synthetic enterprise dependency scenarios. Network flow duration, packet size, flow rate, destination ports, protocol indicators, and system utilization sequences represent technical telemetry. Asset criticality, business exposure, CVSS severity, exploitability, service dependency, and substitutability are represented as contextual variables within the synthetic enterprise scenarios. Data preparation includes duplicate removal, missing value treatment, numerical normalization, categorical encoding, temporal window construction, and class distribution analysis. Controlled noise is introduced to examine model behavior under uncertain telemetry conditions. Training, validation, and testing partitions are created separately to reduce evaluation bias and support reliable comparison across all experimental conditions.

B. Dual Stream Predictive Architecture

The predictive layer uses two complementary information streams. The temporal stream processes sequential technical telemetry and captures changing system behavior across observation windows. The auxiliary stream processes enterprise severity attributes and contextual information. Their learned representations are combined before prediction. The architecture is designed to produce malicious activity probability and disruption probability for each observation. Its general formulation is:

$$P(Y | X, C) = f_{\theta}(E_t(X), E_c(C))$$

Here, X represents technical telemetry, C represents contextual information, E_t represents the temporal encoder, E_c represents the contextual encoder, and f_{θ} represents the prediction function. This design addresses RQ1 through joint technical and operational prediction.

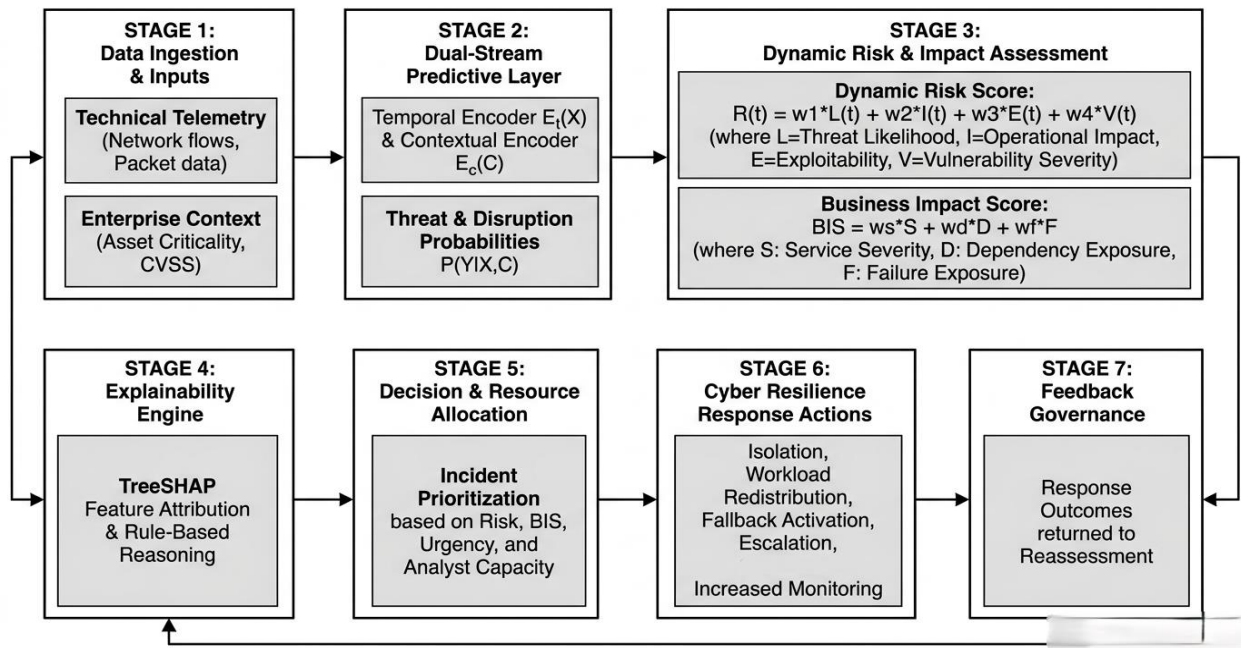


Figure 1: Explainable AI Driven Decision Intelligence Framework

This figure represents the complete proposed architecture, connecting enterprise telemetry and contextual information with prediction, risk assessment, explainability, decision intelligence, resilience actions, and feedback governance.

C. Dynamic Risk and Business Impact Assessment

The risk layer converts predictive outputs into operational significance. Threat likelihood, operational impact, exploitability, and vulnerability severity contribute to the composite risk value. The proposed risk formulation is:

$$R(t) = w_1 L(t) + w_2 I(t) + w_3 E(t) + w_4 V(t)$$

where $L(t)$ denotes threat likelihood, $I(t)$ denotes operational impact, $E(t)$ denotes exploitability, and $V(t)$ denotes vulnerability severity. Business consequences are represented through a Business Impact Score:

$$BIS = w_s S + w_d D + w_f F$$

where S represents service severity, D represents dependency exposure, and F represents failure exposure. Weight values are normalized and examined through sensitivity analysis.

D. Explainable Decision Intelligence and Resource Allocation

The decision intelligence layer connects model predictions with understandable operational recommendations. TreeSHAP identifies the contribution of individual input features, while rule based reasoning connects risk conditions with suitable response actions.

Each explanation reports major contributing factors, predicted threat level, affected service, estimated business impact, and recommended action. The framework also considers service criticality, dependency relationships, urgency, analyst availability, and investigation capacity. Incidents receive priority according to their combined risk and operational significance. This stage addresses RQ2 through transparent reasoning and supports RQ3 through resource allocation. Explanation quality is assessed through faithfulness, soundness, stability, and complexity.

E. Cyber Resilience Response and Experimental Evaluation

The response layer converts prioritized incidents into recommended operational actions. Possible actions include isolation, workload redistribution, service prioritization, fallback activation, escalation, and enhanced monitoring. Action selection depends on risk, Business Impact Score, service criticality, substitutability, and current operating conditions. Simulated response outcomes are returned to the analytical process for reassessment. The framework is compared with XGBoost, SVM, standard BiLSTM, and conventional threshold alerting. Predictive metrics include accuracy, precision, recall, F1 Score, ROC AUC, PR AUC, and false positive rate. Operational metrics include Impact Weighted F1, BIS accuracy, response time, detection lead time, loss avoidance, and resource efficiency. Explainability metrics support final validation.

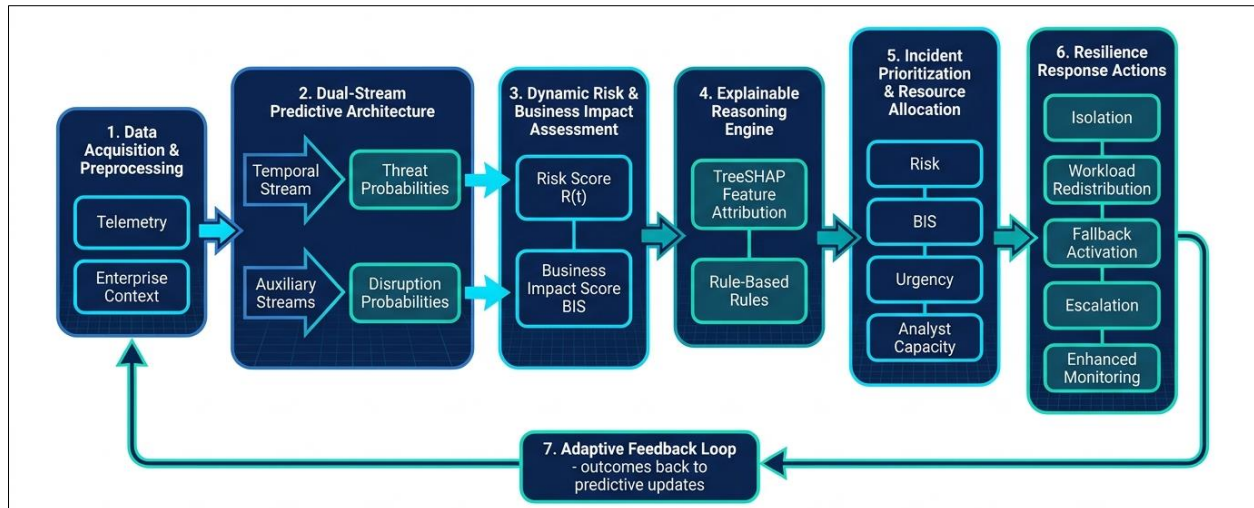


Figure 2: Dynamic Risk Prioritization and Explainable Response Workflow

This figure presents the operational workflow from data acquisition and preprocessing through prediction, risk assessment, explainable reasoning, incident prioritization, response recommendation, evaluation, and adaptive feedback.

F. Validation, Ablation, and Uncertainty Analysis

The validation strategy examines the framework under normal and uncertain operating conditions. Baseline classifiers receive the same training and testing partitions as the proposed model. Ablation experiments separately remove contextual metadata, dependency analysis, explainability, or resource optimization to determine the contribution of each component. Noise scenarios test prediction stability when telemetry contains missing or distorted observations. Sensitivity analysis examines changes in risk weights and Business Impact Score weights. The evaluation design includes statistical comparison of model performance across the defined experimental conditions. The analysis focuses on predictive

performance, false positive reduction, lead time, operational loss avoidance, explanation quality, and analyst resource allocation efficiency.

G. Research Question and Method Alignment

The methodology directly maps each research question to measurable experimental components. RQ1 is addressed through the dual stream predictive architecture and dynamic Business Impact Score calculation. RQ2 is addressed through TreeSHAP, rule based reasoning, and transparent recommendation generation. RQ3 is addressed through comparative experiments, incident prioritization, constrained resource allocation, and resilience response evaluation. The complete process also examines silent degradation, changing operational conditions, service dependency effects, and fallback requirements. This structure allows the research to evaluate not only prediction accuracy but also the practical value of explainable decisions for cyber resilient enterprise operations under uncertainty.

Table I: Methodological Components and Their Roles

Methodological component	Main input	Main output	Research role
Technical telemetry	Network flows, packet data, protocol signals, KPI sequences	Temporal features	Abnormal behavior analysis
Enterprise context	Criticality, exposure, CVSS, exploitability	Severity representation	Operational context
Predictive layer	Temporal and contextual representations	Threat and disruption probabilities	RQ1
Risk layer	Prediction and contextual attributes	Risk Score and BIS	Impact assessment
Dependency layer	Service relationships and substitutability	Impact propagation	Operational assessment
Explainability layer	Model outputs and feature values	SHAP values and decision rules	RQ2
Decision layer	Risk, impact, urgency, analyst capacity	Incident priority	RQ3
Response layer	Priority and service conditions	Recommended action	Cyber resilience
Feedback layer	Response outcomes and model behavior	Updated assessment	Adaptive decision support

IV. RESULTS AND DISCUSSION

The proposed framework is evaluated across predictive performance, business impact assessment, explainable decision support, and operational resilience. The evaluation follows the methodology presented in Section III, where technical telemetry and enterprise context are processed through the dual stream architecture. The resulting predictions enter the risk and impact layers before explainable recommendations and resource prioritization are generated. XGBoost, SVM, standard BiLSTM, and conventional threshold alerting are considered as comparison methods. The analysis focuses on predictive quality, false alerts, Business Impact Score accuracy, response performance, explanation quality, resource allocation, and behavior under uncertain telemetry conditions.

A. Predictive Performance and Business Impact Assessment

The first analysis evaluates the dual stream predictive architecture using technical telemetry and enterprise contextual information. The temporal component captures changing network and system behavior, while the auxiliary component represents asset criticality, business exposure, vulnerability severity, exploitability, and dependency information. Performance is assessed using precision, recall, F1 Score, ROC AUC, PR AUC, and false positive rate. The proposed architecture is compared with XGBoost, SVM, and standard BiLSTM under identical experimental conditions. Business Impact Score results are then examined across different service criticality levels. This analysis examines how technical predictions can be translated into operational significance and incident priority.

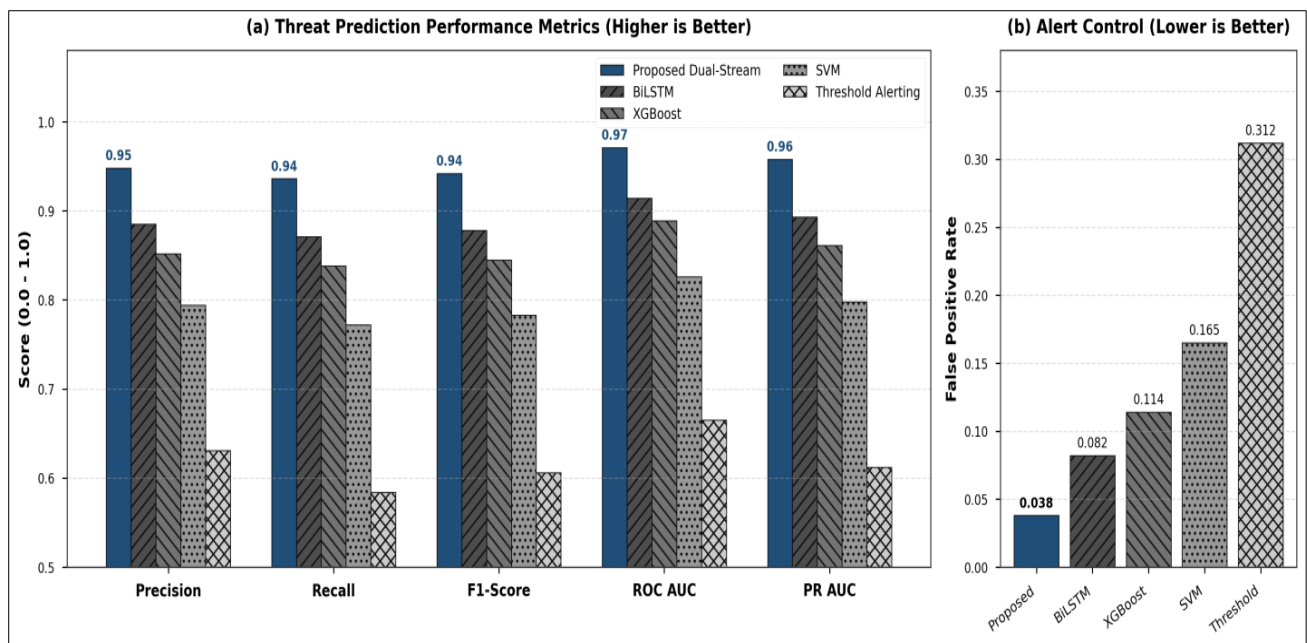


Figure 3: Predictive Performance Comparison of the Evaluated Models

Figure 3 compares predictive performance across evaluated models, showing the proposed dual stream architecture's stronger threat prediction capability and lower false positive rate than the comparison methods.

B. Explainable Decision Support and Incident Prioritization

The second analysis examines the conversion of predictive results into transparent operational decisions. TreeSHAP identifies the contribution of technical and contextual variables, while rule based reasoning

connects risk conditions with response actions. Each explanation identifies important contributing factors, affected services, estimated business consequences, and selected response categories. Incident priority considers cyber risk, Business Impact Score, service criticality, dependency exposure, urgency, and analyst capacity. This process connects model reasoning with operational decisions. Explanation quality is assessed through faithfulness, soundness, stability, and complexity. The analysis therefore addresses RQ2 and evaluates the transparency and practical value of generated recommendations.

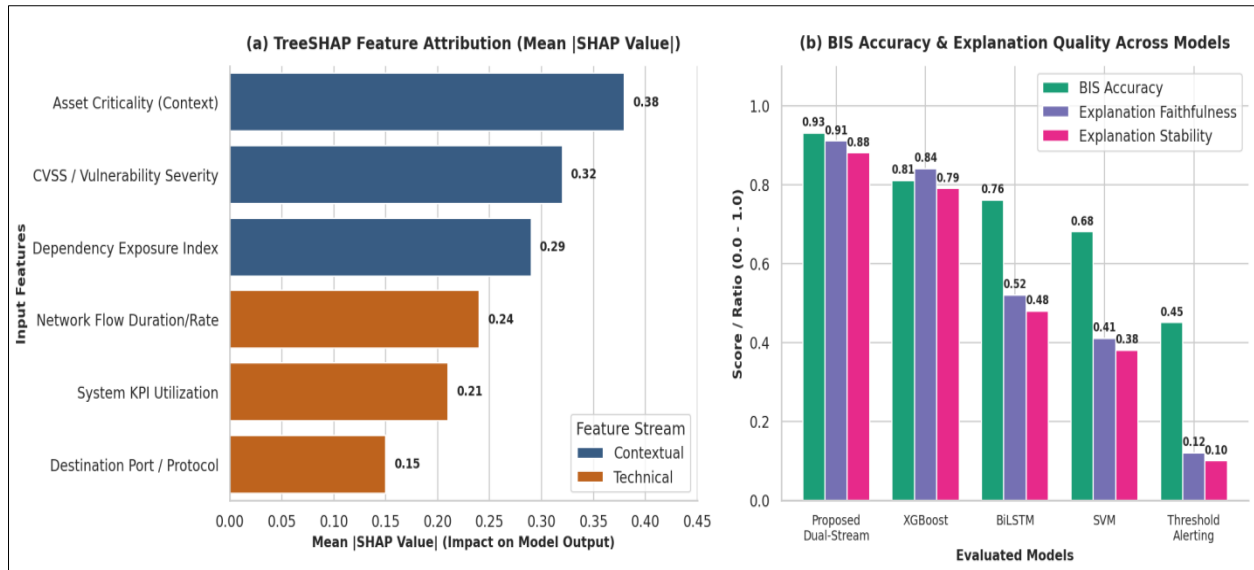


Figure 4: Feature Contribution and Business Impact Assessment Framework

Figure 4 presents feature contributions, Business Impact Score accuracy, and explanation quality, showing the importance of contextual factors and the proposed framework's stronger interpretable decision support.

C. Operational Resilience and Resource Allocation

The third analysis evaluates the operational value of the proposed decision intelligence framework. Incidents are prioritized according to risk, Business Impact Score, urgency, service criticality, dependency

exposure, and available analyst capacity. The proposed framework is compared with conventional threshold alerting and detection focused models using Impact Weighted F1, BIS accuracy, false positive rate, detection lead time, response time, operational loss avoidance, and resource allocation efficiency. Resource constrained experiments examine situations where incident volume exceeds analyst capacity. This analysis determines how effectively the framework directs investigation toward higher consequence incidents and supports timely resilience actions under operational pressure.

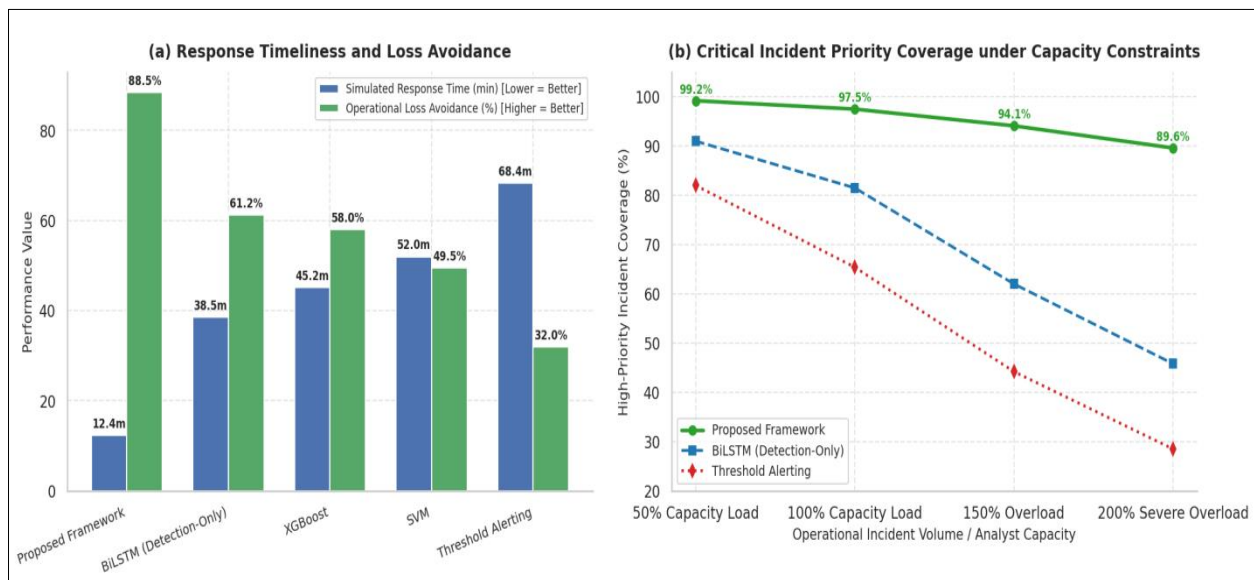


Figure 5: Operational Performance and Resource Allocation Evaluation Framework

Figure 5 evaluates response timeliness, operational loss avoidance, and incident priority coverage under capacity constraints, demonstrating the framework's operational value during increasing incident workload.

D. Limitations and Overall Discussion

The final analysis considers uncertainty, ablation results, and study limitations. Noise, missing telemetry, changing feature distributions, and altered service conditions are used to examine prediction stability and explanation consistency. Ablation

experiments remove contextual metadata, dependency analysis, explainability, and resource allocation separately to determine their individual contributions. Public cybersecurity datasets may not fully represent complex enterprise dependencies or production incident conditions, while synthetic scenarios cannot reproduce every operational relationship. Business Impact Score quality also depends on accurate contextual information.

Despite these limitations, the framework provides an integrated approach connecting cyber prediction, operational impact, explainability, resource prioritization, and resilience response. The business impact component is modeled through synthetic contextual variables and therefore should not be interpreted as a direct measurement of financial or operational loss.

Table II: Summary of Experimental Evaluation

Evaluation Area	Measures	Purpose
Predictive performance	Precision, Recall, F1 Score, ROC AUC, PR AUC	Evaluate threat prediction
Alert control	False Positive Rate	Assess unnecessary alerts
Business impact	BIS Accuracy, Impact Weighted F1	Evaluate operational prioritization
Response performance	Detection Lead Time, Response Time	Assess response timeliness
Resource allocation	Analyst utilization, Priority Coverage	Evaluate investigation capacity
Explainability	Faithfulness, Soundness, Stability, Complexity	Assess explanation quality
Resilience	Operational Loss Avoidance, Continuity Performance	Evaluate resilience outcomes
Uncertainty	Prediction Variation, Explanation Stability	Assess model stability

V. CONCLUSION

The proposed Explainable AI Driven Decision Intelligence framework integrates telemetry, context, service criticality, dependency information, threat prediction, Business Impact Score assessment, explainable reasoning, and resource constrained response decisions. Its dual stream architecture connects temporal signals with factors, while the explainability layer provides feature level reasoning for incident prioritization. The framework considers uncertainty, false alerts, model degradation, and limited analyst capacity, linking cybersecurity detection with operational consequences and continuity requirements.

Future work will focus on validation with enterprise datasets, SOC incident records, and service dependency graphs. Analyst studies can assess explanation usefulness, decision confidence, response time, and workload. Further research can examine concept drift, adversarial manipulation, grey failure, graph neural networks, counterfactual explanations, and dynamic resource allocation. Integration with security orchestration platforms can support testing of response recommendations and fallback decisions.

REFERENCES

- Javeed, M. S., Khatun, M. M., Alom, J., Islam, R., & Shoaib, H. A. (2026). A dual-stream deep learning architecture for business impact scoring and alert escalation. *PLOS ONE*, 21(7), e0350676. <https://doi.org/10.1371/journal.pone.0350676>
- Pattnaik, S. (2026). Explainable AI-based intelligent security recommendation system for real-time cyber threat mitigation. *International Journal of Contemporary Research in Multidisciplinary*, 5(3), 301–311. <https://doi.org/10.5281/zenodo.20324536>
- Prasad, P. W. C., Sayeed, M. S., Nguyen, D.-M., Hutabarat, D. P., & Mohiuddin, G. M. (2026). Explainable AI: Enhancing decision-making in the detection of cyber threats. *Frontiers in Computer Science*, 8, 1762332. <https://doi.org/10.3389/fcomp.2026.1762332>
- Akter, E., Bormon, J. C., Saikat, M. H., & Shoag, M. (2025). Digital twin technology for smart civil infrastructure and emergency preparedness. *IJSRED – International Journal of Scientific Research and Engineering Development*, 8(2), 891–902. <https://doi.org/10.5281/zenodo.17246150>
- Karim, M. A. (2025). AI-driven predictive maintenance for solar inverter systems. *TechRxiv*. <https://doi.org/10.36227/techrxiv.175977633.34528041.v1>
- Rahman, M., Razaq, A., Hossain, M. T., & Zaman, M. T. U. (2025). Machine learning approaches for predictive maintenance in IoT devices. *World Journal of Advanced Engineering Technology and Sciences*, 17(1), 157–170. <https://doi.org/10.30574/wjaets.2025.17.1.1388>
- Akhter, T., Alimozzaman, D. M., Hasan, E., & Islam, R. (2025). Explainable predictive analytics for healthcare decision support. *International Journal of Sciences and Innovation Engineering*, 2(10), 921–938. <https://doi.org/10.70849/IJSCI02102025105>
- Hasan, E. (2025). Big data-driven business process optimization: Enhancing decision-making through predictive analytics. *TechRxiv*. <https://doi.org/10.36227/techrxiv.175987736.61988942.v1>
- Islam, K. S. A. (2025). Implementation of safety-integrated SCADA systems for process hazard control in power generation plants. *IJSRED – International Journal of Scientific Research and Engineering Development*, 8(5), 2321–2331. <https://doi.org/10.5281/zenodo.17536369>
- Rahman, F. (2025). Data science in power system risk assessment and management. *World Journal of Advanced Engineering Technology and Sciences*,

- 17(3), 295–311.
<https://doi.org/10.30574/wjaets.2025.17.3.1560>
11. Jasem, M. M. H. (2025). An AI-driven system health dashboard prototype for predictive maintenance and infrastructure resilience. *Authorea*.
<https://doi.org/10.22541/au.176617579.97570024.v1>
12. Rabbi, M. S. (2026). AI-driven SCADA grid intelligence for predictive fault detection, cyber health monitoring, and grid reliability enhancement. *Zenodo*. <https://doi.org/10.5281/zenodo.18196487>
13. Taimun, M. T. Y., Alam, M. S., & Fareed, S. M. (2026). Digital twin-enabled predictive maintenance for textile and mechanical systems. *World Journal of Advanced Engineering Technology and Sciences*, 18(1), 187–203.
<https://doi.org/10.30574/wjaets.2026.18.1.0001>
14. Zaidi, S. K. A., Islam, K. S. A., Zaman, S. U., & Afrin, S. (2026). Blockchain-secured communication for industrial IoT and aviation control systems. *IJSRED – International Journal of Scientific Research and Engineering Development*, 9(1), 234–250.
<https://doi.org/10.5281/zenodo.18278261>
15. Mirza, S. B. (2026). Predictive reliability engineering for cloud-scale business intelligence platforms through anomaly detection, capacity optimization, and proactive support automation. *Zenodo*. <https://doi.org/10.5281/zenodo.19474845>