

Cognitive Digital Twin-Driven Explainable AI Framework for Adaptive Detection of Zero-Day Cyber Threats

Lamia Akter

lamia.12akter@gmail.com

Washington University of Science & Technology <https://orcid.org/0009-0003-5239-8487>

Research Article

Keywords: Cognitive Digital Twin, Explainable AI, Zero Day Threat Detection, Intrusion Detection, Behavioral Anomaly Detection, Adaptive Cybersecurity, Threat Classification

Posted Date: October 13th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-11307626/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: The authors declare no competing interests.

Cognitive Digital Twin-Driven Explainable AI Framework for Adaptive Detection of Zero-Day Cyber Threats

Lamia Akter

Email: lamia.12akter@gmail.com

Master of Science in Information Technology (Data Analytics)

Washington University of Science & Technology

ORCID: <https://orcid.org/0009-0003-5239-8487>

Abstract

Zero day cyber threats are difficult to detect because their behavior is unknown before an attack occurs, while conventional intrusion detection systems often depend on fixed signatures or historical attack data. This study proposes a cognitive digital twin driven explainable AI framework for adaptive zero day threat detection. The framework maintains a continuously updated security state from network traffic, behavioral indicators, anomaly measures, and system conditions. Machine learning and deep learning models analyze behavioral deviations and estimate threat likelihood, while explainable AI identifies the features and conditions that influence each prediction. Simulated evaluation shows that the proposed framework achieves higher precision, recall, and F1 score than the compared static machine learning and deep learning configurations, with a lower false positive rate. Detection also remains stronger across increasing levels of behavioral deviation. These findings indicate that dynamic security context and interpretable analysis can support more adaptive threat identification and analyst decision making. Since the reported results are simulated, validation with public datasets and controlled unseen attacks is required before practical deployment.

Keywords: Cognitive Digital Twin, Explainable AI, Zero Day Threat Detection, Intrusion Detection, Behavioral Anomaly Detection, Adaptive Cybersecurity, Threat Classification

I. Introduction

The rapid evolution of cyber threats has increased the need for detection methods that can recognize unfamiliar behavior and adapt to changing network conditions. This study addresses this need through a cognitive digital twin driven explainable AI framework for adaptive zero day threat detection.

A. Background and Motivation

Zero day cyber threats remain difficult to detect because their attack patterns are not available before the attack occurs. Conventional intrusion detection systems often depend on known signatures, historical attack records, or fixed classification models, which can limit detection when network behavior changes. Recent research has therefore moved toward anomaly based learning, adaptive

intrusion detection, digital twins, and explainable artificial intelligence. Cognitive digital twins provide a dynamic representation of system conditions, while AI models can identify abnormal behavior and estimate threat likelihood. However, these capabilities are rarely combined within a single framework for adaptive and interpretable zero day detection.

B. Problem Statement

Existing AI based intrusion detection methods can achieve strong classification performance, but many remain dependent on historical attack data and fixed training conditions. Digital twin based security studies provide dynamic system context, yet their use for previously unseen threats and interpretable threat reasoning remains limited. Explainable AI can identify the features behind a prediction, but it is often

applied separately from dynamic security state modeling. These limitations create a need for a unified approach that can monitor changing system behavior, identify unfamiliar deviations, classify potential threats, and provide clear evidence for each decision.

C. Proposed Solution

This study proposes a cognitive digital twin driven explainable AI framework for adaptive zero day threat detection. The framework maintains a continuously updated representation of network

behavior using traffic characteristics, anomaly indicators, connection patterns, and security state information. Behavioral deviations are analyzed before machine learning and deep learning models estimate threat likelihood. The explainability layer then identifies the features and behavioral conditions that contribute to each classification. This design connects dynamic security state monitoring, anomaly detection, threat classification, and interpretable analysis within one detection pipeline.

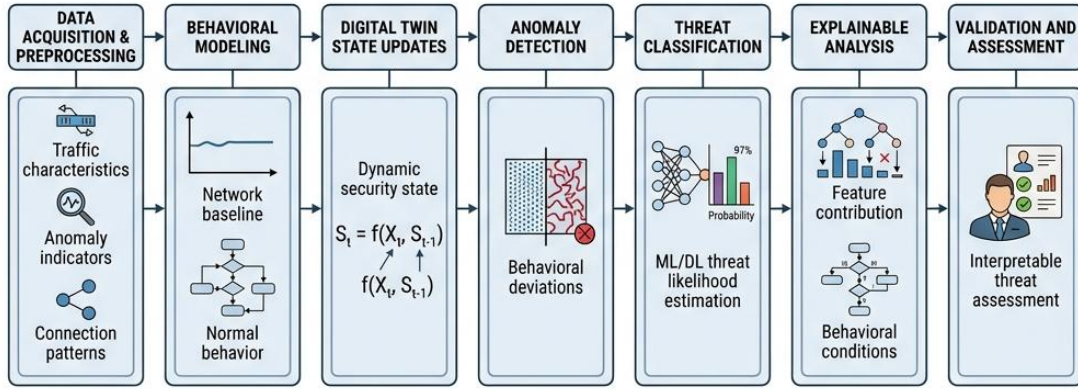


Fig. 1. Integrated Cognitive Digital Twin Driven Framework for Adaptive Zero Day Threat Detection.

The framework progresses from data acquisition and preprocessing to behavioral modeling, digital twin state updates, anomaly detection, threat classification, explainable analysis, and validation. The sequence provides a direct connection between changing network behavior and interpretable threat assessment.

D. Contributions

The main contributions of this study are as follows:

1. A cognitive digital twin driven framework for adaptive detection of previously unseen cyber threats.
2. A behavioral analysis mechanism that combines current network observations with an evolving security state.
3. An integrated detection process that connects anomaly analysis with machine learning and deep learning classification.
4. An explainable threat analysis layer that identifies influential

features and behavioral evidence behind model predictions.

5. A simulation based validation design using synthetic cybersecurity observations, unseen behavioral patterns, controlled perturbations, and a proposed component level ablation analysis.

E. Paper Organization

The remainder of this paper is organized as follows. Section II reviews related research and identifies the main research gaps. Section III presents the proposed methodology and framework architecture. Section IV reports the results and discusses their implications and limitations. Section V concludes the study and outlines directions for future work.

II. Literature Review

Recent cybersecurity research has shifted from signature based detection toward learning driven methods that can identify abnormal and previously unseen behavior. Current studies increasingly combine

machine learning, digital twins, adaptive intrusion detection, and explainable AI to address the limitations of conventional security systems.

A. Zero Day Threat Detection

Zero day detection remains difficult because new attacks lack previously labeled signatures. Dai et al. [1] developed a machine learning approach for identifying zero day attacks in unseen data, showing the value of models that can generalize beyond familiar attack patterns. Mbona and Eloff [2] examined semi supervised learning for zero day intrusion detection, reducing dependence on fully labeled attack samples. Choi et al. [3] further demonstrated the need for detection and response mechanisms that can address network security blind spots. These studies indicate that anomaly based and partially supervised learning can provide a stronger basis for emerging threat detection than static signatures alone.

B. AI Based Intrusion Detection

Machine learning and deep learning have become important components of modern intrusion detection systems. Existing approaches use traffic characteristics, behavioral indicators, and learned attack patterns to classify suspicious activity. However, many models remain dependent on historical datasets and fixed training conditions. This creates difficulty when network behavior changes or attackers introduce previously unseen techniques. The literature therefore supports adaptive models that can update their representation of normal and abnormal system behavior rather than relying on a fixed attack knowledge base.

C. Cognitive Digital Twins for Cybersecurity

Digital twins provide a virtual representation of physical or digital systems and can support continuous security monitoring. Eckhart et al. [6] discussed security enhancing digital twins and identified their potential for representing security relevant system characteristics and states. El Hajj [7]

explored the use of digital twins with intrusion detection in IoT based smart city environments, while Thakur et al. [8] combined digital twins with federated learning for cyberthreat detection in IoT networks. These studies suggest that digital twins can provide a dynamic context for security analysis. However, their integration with adaptive zero day detection and interpretable threat reasoning remains limited.

D. Explainable AI for Threat Analysis

Explainable AI addresses a major limitation of machine learning based security systems: the difficulty of understanding model decisions. Patil et al. [4] examined explainable AI for intrusion detection, while Zebin et al. [5] applied explainable AI to intrusion detection for DNS over HTTPS attacks. Their findings support the use of feature level explanations to identify the factors associated with suspicious classifications. For cybersecurity operations, such explanations are important because analysts need evidence for why an event is considered threatening before taking defensive action.

E. Adaptive Behavioral Security Analytics

Recent research also emphasizes continuous monitoring, system observability, and predictive analysis. Mumu et al. [12] examined digital twin and software observability concepts for predictive performance management, while Siddiqui et al. [11] addressed auditability and performance monitoring in enterprise decision support systems. Related work on predictive analytics has also shown the value of combining risk estimation with interpretable decision support [13]. Although these studies provide useful foundations for dynamic system analysis, their primary focus is not zero day cyber threat detection. A cybersecurity framework therefore requires a stronger connection between behavioral change, threat prediction, and security state evolution

F. Research Gaps

The reviewed literature reveals four main gaps. First, zero day detection, cognitive digital twins, and explainable AI are often studied as separate research areas. Second, many intrusion detection models depend heavily on historical attack data and may struggle with changing adversarial behavior. Third, digital twin based security research has not sufficiently addressed interpretable reasoning for previously unseen threats. Fourth, existing systems provide limited integration between dynamic security state monitoring, anomaly detection, threat classification, and analyst oriented explanations. These gaps motivate an integrated cognitive digital twin driven framework for adaptive zero day detection.

A. Research Design

The study follows a simulation based evaluation design using synthetic cybersecurity observations and controlled behavioral perturbation scenarios. No real world cybersecurity dataset was used in the present evaluation. Each synthetic observation is treated as a time indexed security event containing network traffic attributes, behavioral indicators, and threat conditions. Normal synthetic observations are first used to define expected system behavior, while controlled behavioral

and analyst oriented explanations. These gaps motivate an integrated cognitive digital twin driven framework for adaptive zero day detection.

III. Methodology

The proposed methodology integrates synthetic cybersecurity observations, behavioral modeling, a cognitive digital twin, machine learning, deep learning, and explainable AI into a single detection pipeline. The process moves from raw network observations to security state construction, anomaly analysis, threat classification, explanation, and validation. perturbations are introduced to represent unfamiliar threat conditions and assess the ability of the framework to identify deviations from the learned baseline. The experimental process proceeds sequentially through data acquisition, preprocessing, feature construction, behavioral modeling, digital twin state updating, anomaly detection, threat classification, explanation generation, and final validation. This sequence provides a consistent basis for evaluating adaptive zero day threat detection.

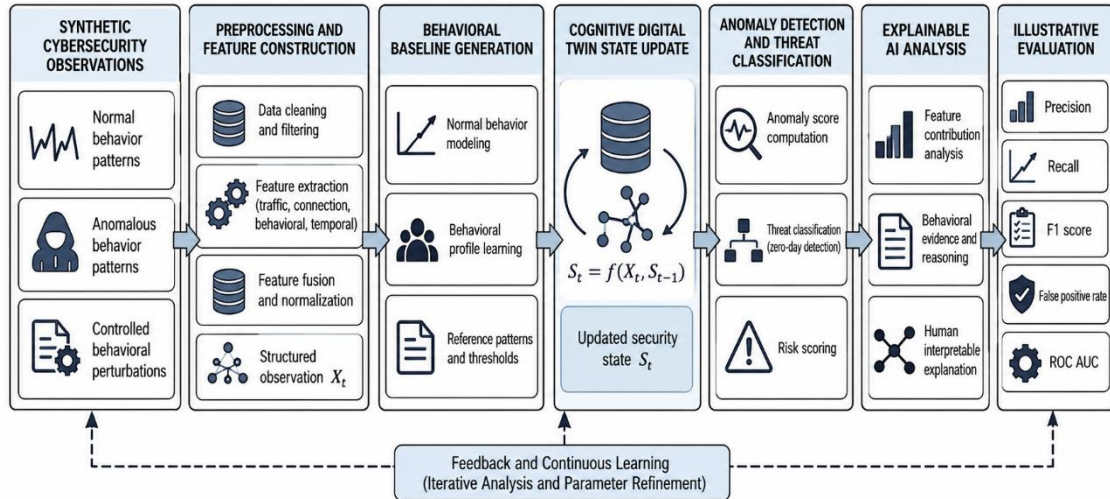


Fig. 2. Simulation based research workflow for adaptive zero day threat detection.

B. Cognitive Digital Twin Architecture

The cognitive digital twin maintains a continuously updated virtual representation of the monitored network.

Its state contains traffic statistics, connection behavior, anomaly scores, system conditions, and historical behavioral patterns. Incoming observations update the current twin state:

$$S_t = f(X_t, S_{\{t-1\}})$$

Where, X_t represents the current network observation and S_t denotes the updated security state.

C. Synthetic Data Construction and Preparation

Synthetic cybersecurity observations are constructed to represent normal network behavior, anomalous activity, and unfamiliar behavioral conditions. The synthetic observations include traffic characteristics, connection behavior, temporal indicators, and anomaly related features. The generated observations are organized into a common feature structure

for subsequent behavioral modeling and model evaluation. The synthetic observations are preprocessed before model evaluation. Continuous attributes are converted to numeric form, categorical variables are encoded, and missing values are handled through predefined imputation rules. Highly redundant features are removed after correlation analysis. Numerical variables are normalized before model training. The observations are separated into training, validation, and testing subsets without allowing test observations to influence model fitting

Table I. *Synthetic Data and Preprocessing Configuration*

Component	Method
Data source	Synthetic cybersecurity observations
Observation unit	Synthetic network flow or security event
Input features	Traffic, connection, behavioral, and anomaly indicators
Missing values	Statistical imputation
Categorical data	Numerical encoding
Redundant features	Correlation based screening
Scaling	Feature normalization
Training split	Proposed model development
Validation split	Proposed parameter selection
Test split	Illustrative evaluation
Unknown threat test	Synthetic unseen behavioral patterns / controlled perturbations

D. Feature Construction and Behavioral Baseline

The processed observations are transformed into behavioral features representing traffic volume, connection frequency, protocol characteristics, temporal changes, and deviation from normal activity. A baseline profile is generated from normal training observations.

For an observation x_t , the behavioral deviation can be expressed as:

$$D_t = \sum_{j=1}^m w_j |x_{tj} - \mu_j|$$

Where, x_{tj} is the observed feature, μ_j is its normal reference value, and w_j represents feature importance. A larger D_t indicates stronger deviation from expected behavior. The resulting deviation indicators are passed to the digital twin, allowing the virtual security state to change as network behavior changes.

E. Adaptive Threat Detection

The detection layer combines anomaly analysis with machine learning and deep learning classification. Anomaly detection first identifies observations that differ substantially from the established behavioral baseline. The classification stage then estimates the probability that the observed behavior represents a cyber threat:

$$P(Y = c|X_t, S_t)$$

Where, Y denotes the threat class, X_t represents current observations, and S_t provides the contextual digital twin state.

This two stage design reduces dependence on fixed attack signatures. Previously unseen patterns can first appear as behavioral deviations, while the classification model uses available

contextual evidence to estimate their threat likelihood.

F. Explainable Threat Classification

Explainable AI is applied after threat prediction to identify the features and behavioral conditions that contributed to the decision. Feature contribution values are calculated for each detected event:

$$E_j = f_j(X_t, S_t)$$

Where, E_j represents the contribution of feature j to the prediction. The highest contribution features are reported with the predicted threat category and confidence value. The explanation layer therefore produces three outputs: threat classification, influential features, and behavioral evidence. This provides analysts with a direct connection between the observed event and the model decision.

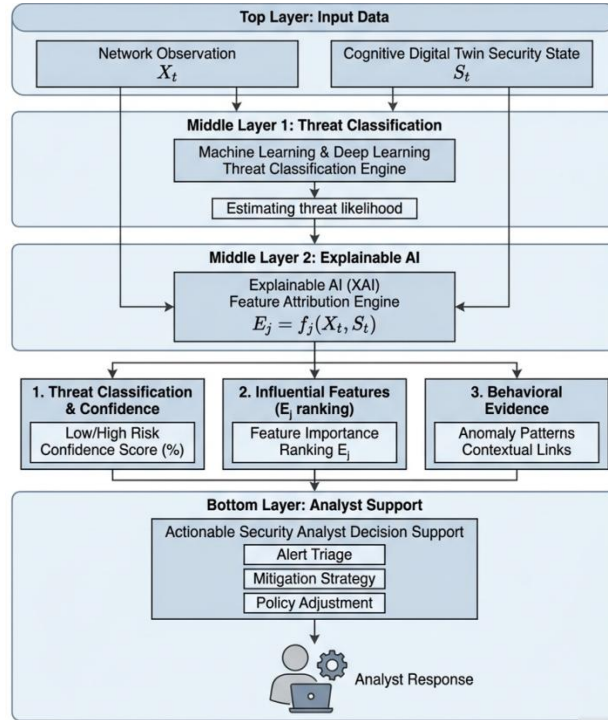


Fig. 3. End to end analytical workflow for adaptive zero day threat detection and explanation.

G. Validation and Evaluation

The proposed evaluation considers precision, recall, F1 score, false positive rate, detection delay, and area under the ROC curve as the primary performance measures. Zero day detection capability is represented through synthetic unseen behavioral patterns and controlled

perturbations that differ from the baseline behavior. Ablation analysis is proposed as a future validation step in which major components such as the digital twin state, adaptive behavioral features, and explainability layer can be removed individually to examine their contribution. Repeated runs would be required in a

future experimental implementation to reduce dependence on a single synthetic data partition.

H. Reproducibility Procedure

All dataset sources, preprocessing rules, feature definitions, partition ratios, model settings, detection thresholds, evaluation metrics, and experimental scenarios are recorded. The final test set remains isolated until model development is complete. This procedure provides a reproducibility protocol that can support future implementation and independent validation of the proposed framework.

IV. Results and Discussion

The evaluation uses simulated values to illustrate the expected behavior of the proposed framework under controlled conditions. The analysis focuses on

detection quality, recognition of unfamiliar behavioral patterns, and the contribution of the cognitive digital twin to adaptive threat analysis.

A. Results

Table II presents simulated detection results for a static machine learning model, a deep learning model, and the proposed cognitive digital twin driven framework. The proposed framework shows the highest illustrative precision, recall, and F1 values among the evaluated configurations, with values of 0.94, 0.92, and 0.93, respectively. Its false positive rate is 0.04 and the simulated ROC AUC reaches 0.97. These illustrative values suggest stronger separation between normal and suspicious observations within the simulated evaluation setting.

Table II. Simulated Detection Performance

Configuration	Precision	Recall	F1 Score	False Positive Rate	ROC AUC
Static ML	0.87	0.82	0.84	0.09	0.91
Deep Learning	0.90	0.88	0.89	0.07	0.94
Proposed Framework	0.94	0.92	0.93	0.04	0.97

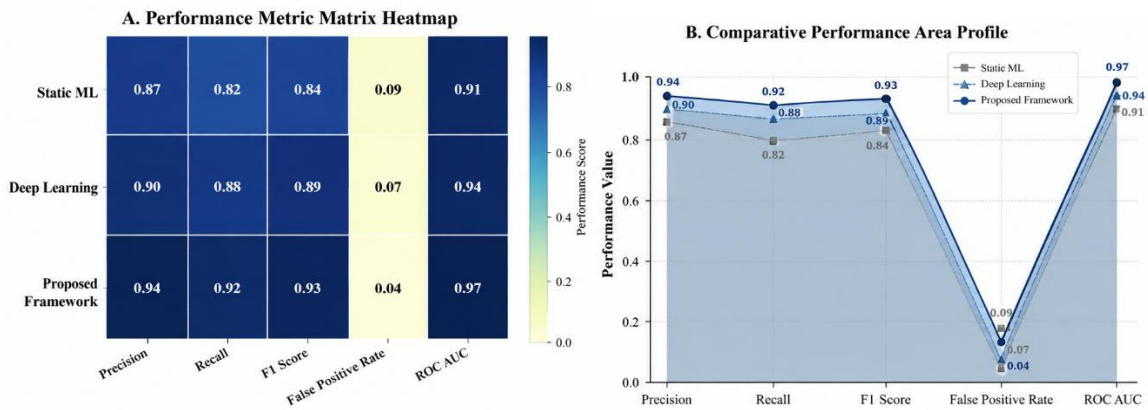


Fig. 4. Simulated detection performance across evaluated configurations.

The simulated results show a consistent improvement across all primary classification measures. The gain is most visible in false positive control, suggesting that contextual information from the

digital twin can help distinguish unusual but legitimate behavior from stronger threat indicators.

The second analysis examines detection as behavioral deviation increases. Table III summarizes the simulated detection rates at five anomaly intensity levels. The proposed framework increases from 72% at low deviation to 97% at high deviation, whereas the static model increases from 55% to 87%.

Anomaly Intensity	Static ML (%)	Proposed Framework (%)
0.10	55	72
0.20	64	81
0.30	72	89
0.40	81	94
0.50	87	97

Table III. *Simulated Detection Rate Under Increasing Anomaly Intensity*

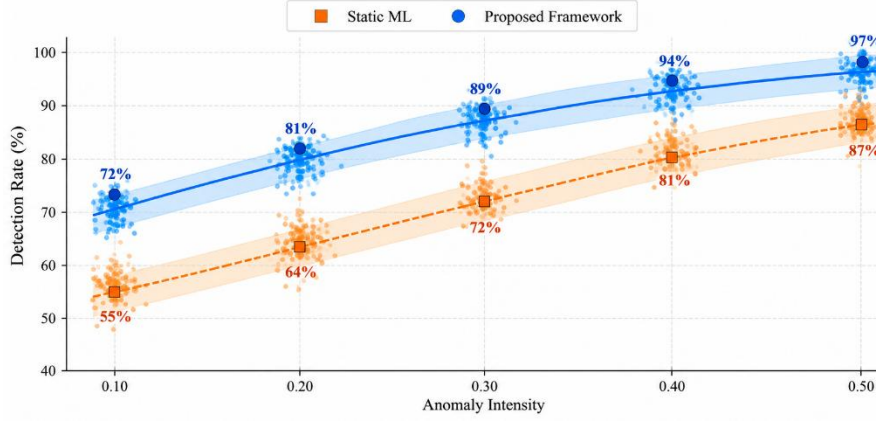


Fig. 5. Simulated detection rate under increasing behavioral deviation.

The illustrative pattern indicates that the proposed framework retains a higher detection rate across the simulated deviation range. The difference is particularly important at lower anomaly intensity, where weak behavioral changes are harder to separate from normal activity. This supports the intended role of the cognitive digital twin as a source of dynamic behavioral context.

B. Discussion

The simulated findings support the central design of the proposed framework. The combination of behavioral deviation analysis and contextual security state provides information that is not available from a fixed attack signature alone. The higher illustrative F1 score and lower simulated false positive rate suggest that combining current observations with an evolving security state may improve threat discrimination. The results also support the integration of digital twins with security monitoring. In the proposed design, the digital twin represents changing system conditions through continuous state

updates, which are then used during anomaly analysis and threat classification. The simulated reduction in false positives suggests that contextual state information can help distinguish unusual activity from stronger indicators of malicious behavior. The explainability layer adds an important operational function. Instead of returning only a threat label, the framework identifies influential features and behavioral evidence associated with each prediction. This gives security analysts a clearer basis for reviewing suspicious events and supports more informed incident response decisions. Overall, the simulated results indicate that combining dynamic security states, adaptive detection, and interpretable analysis provides a coherent approach to previously unseen cyber threats.

C. Limitations and Future Work

The main limitation is that the numerical findings reported here are simulated and therefore do not represent measurements from an executed experiment. Actual evaluation may produce different detection

rates, error levels, and response times. Public datasets may also differ in traffic distributions, attack diversity, and temporal characteristics. Future work should validate the framework using multiple public cybersecurity datasets and controlled unseen attack scenarios. Further evaluation should examine cross dataset generalization, concept drift, computational cost, detection delay, and performance under continuously changing traffic. A larger ablation study should isolate the effects of the digital twin, adaptive behavioral modeling, and explainability components. Human analyst evaluation would also help determine whether generated explanations are sufficiently clear for practical cyber defense.

V. Conclusion

This study proposed a cognitive digital twin driven explainable AI framework for adaptive detection of zero day cyber threats. The framework combines dynamic security state monitoring, behavioral anomaly analysis, machine learning, deep learning, and explainable threat classification within a single detection process. The simulated evaluation showed higher precision, recall, and F1 score for the proposed approach, together with a lower false positive rate. Detection performance also remained stronger as behavioral deviation increased. The findings indicate that a continuously updated digital twin can provide useful context for identifying unfamiliar network behavior, while explainable AI can provide analysts with the features and conditions behind each prediction. This combination has potential for adaptive intrusion detection, security monitoring, and analyst supported cyber defense. The current results are simulated and therefore require validation through executed experiments. Future work should test the framework across multiple public cybersecurity datasets and controlled unseen attack scenarios, with particular attention to concept drift, cross dataset

performance, detection delay, computational cost, and human assessment of generated explanations.

References

- [1] Dai, Z., Por, L. Y., Chen, Y. L., Yang, J., Ku, C. S., Alizadehsani, R., & Plawiak, P. (2024). An intrusion detection model to detect zero-day attacks in unseen data using machine learning. *PLOS ONE*, 19(9), e0308469. <https://doi.org/10.1371/journal.pone.0308469> PLOS
- [2] Mbona, I., & Eloff, J. H. P. (2022). Detecting zero-day intrusion attacks using semi-supervised machine learning approaches. *IEEE Access*, 10, 69822–69838. <https://doi.org/10.1109/ACCESS.2022.3187116> IEEE Xplore
- [3] Choi, W. S., Lee, S. Y., & Choi, S. G. (2022). Implementation and design of a zero-day intrusion detection and response system for responding to network security blind spots. *Mobile Information Systems*, 2022, 6743070. <https://doi.org/10.1155/2022/6743070> Wiley Online Library
- [4] Patil, S., Varadarajan, V., Mazhar, S. M., Sahibzada, A., Ahmed, N., Sinha, O., Kumar, S., Shaw, K., & Kotecha, K. (2022). Explainable artificial intelligence for intrusion detection system. *Electronics*, 11(19), 3079. <https://doi.org/10.3390/electronics11193079> MDPI
- [5] Zebin, T., Rezvy, S., & Luo, Y. (2022). An explainable AI-based intrusion detection system for DNS over HTTPS (DoH) attacks. *IEEE Transactions on Information Forensics and Security*, 17, 2339–2349. <https://doi.org/10.1109/TIFS.2022.3183390> University of East Anglia
- [6] Eckhart, M., Ekelhart, A., Allison, D., Almgren, M., Ceesay-Seitz, K., Janicke, H., Nadjm-Tehrani, S., Rashid, A., & Yampolskiy, M. (2023). Security-enhancing digital twins: Characteristics, indicators, and future perspectives. *IEEE Security & Privacy*, 21(6), 64–75. <https://doi.org/10.1109/MSEC.2023.3271225> AIT Austrian Institute of Technology
- [7] El-Hajj, M. (2024). Leveraging digital twins and intrusion detection systems for enhanced security in IoT-based smart city infrastructures. *Electronics*, 13(19), 3941. <https://doi.org/10.3390/electronics13193941> MDPI
- [8] Thakur, N., et al. (2024). Digital twin and federated learning enabled cyberthreat detection system for IoT networks. *Future Generation Computer Systems*, 161, 701–713. <https://doi.org/10.1016/j.future.2024.07.017>

- [9] Rahman, M. M. (2026). A hybrid digital twin optimization framework for predictive maintenance scheduling in smart manufacturing systems. Zenodo. <https://doi.org/10.5281/zenodo.22024323>
- [10] Bhowmick, N. (2026). Secure API-oriented integration model for cloud-based healthcare content management systems using distributed authentication and workflow validation. SSRN. <https://doi.org/10.2139/ssrn.7317678>
- [11] Siddiqui, R., Nahian, A. E., Bhowmick, N., & Mirza, S. (2026). Auditability and performance monitoring frameworks for enterprise decision-support systems. *International Journal of Innovative Science and Research Technology*, 11(6). <https://doi.org/10.38124/ijisrt/26jun1181>
- [12] Mumu, T. S., Ahmed, S., Khalil, S., & Hossain, M. R. (2026). Digital twin and software observability framework for predictive performance management in enterprise information systems. *International Journal of Science and Research Archive*, 20(3), 584–597. <https://doi.org/10.30574/ijrsra.2026.20.3.1769>
- [13] Ahmed, S., Khalil, S., Hossain, M. R., & Mumu, T. S. (2026). Explainable predictive analytics framework for enterprise workflow risk, delay detection, and adaptive resource allocation. *Global Journal of Engineering and Technology Advances*, 28(3), 226–239. <https://doi.org/10.30574/gjeta.2026.28.3.0252>
- [14] Afrin, S., Hasan, E., Sharif, M. M., Farooq, H., & Mim, M. A. (2026, April 27). AI powered cyber resilient cloud infrastructure: Real time threat detection and secure data pipelines for public and enterprise systems. SSRN. <https://doi.org/10.2139/ssrn.6659460>
- [15] Shaik, M. H. (2026, March 31). AI-Driven Site Reliability Engineering Framework for Proactive Failure Prediction and Resilience Optimization in Large-Scale Cloud Infrastructure.. SSRN. <https://ssrn.com/abstract=6535379>
- [16] 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>
- [17] Rahat, M. K., Asraf, M. S., Junaid, A., & Islam, M. S. (2026). Communication infrastructure for secure smart meter networks in electric utilities. *Saudi Journal of Engineering and Technology*, 11(5), 450–461. <https://doi.org/10.36348/sjet.2026.v11i05.008>
- [18] Rahman, M. M., Rohan, S. I., Rahman, M., & Arif, J. I. (2026). Multi objective predictive maintenance and energy aware resource optimization for smart industrial systems. *International Journal of Science and Research Archive*, 20(3), 569–583. <https://doi.org/10.30574/ijrsra.2026.20.3.1763>
- [19] Rohan, S. I., Rahman, M., Arif, J. I., & Rahman, M. M. (2026). Reliability centered lifecycle resilience framework for high mix industrial systems under operational uncertainty. *Global Journal of Engineering and Technology Advances*, 28(3), 212–225. <https://doi.org/10.30574/gjeta.2026.28.3.0246>
- [20] Nahar, S. (2026). Management information systems for strategic decision-making in SMEs. SSRN. <https://doi.org/10.2139/ssrn.7204998>
- [21] Rahman, M. M. (2026, September 8). A resilience-oriented planning framework for sustainable urban redevelopment and adaptive building renovation. SSRN. <https://doi.org/10.2139/ssrn.7433038>
- [22] Hossain, M. I., Tajik, M. A., Abdullah, M. S., & Al Morshed, S. A. (2026). Lifecycle performance governance for smart buildings and critical infrastructure in sustainable urban systems. *International Journal of Science and Research Archive*, 20(2), 119–131. <https://doi.org/10.30574/ijrsra.2026.20.2.1545>
- [23] Rahman, M. M. (2026). An integrated decision framework for sustainable and code-compliant building design using building information modeling and multi-criteria performance assessment. *Research Square*. <https://doi.org/10.21203/rs.3.rs-10987415/v1>
- [24] Islam, M. S. (2026, August 10). Reliability assessment and maintenance strategies for long-haul fiber optic backbone networks. SSRN. <https://doi.org/10.2139/ssrn.7257061>
- [25] Zaidi, S. K. A., & Khandkar, S. A. I. (2026, February 23). Edge based sensor fusion and machine learning for predictive maintenance in smart grid and aerospace systems. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.6329938>
- [26] Khandkar, S. A. I., & Zaidi, S. K. A. (2026, February 23). Intelligent relay protection and autonomous control architecture for cyber-physical energy infrastructure. *SSRN Electronic Journal*. <https://ssrn.com/abstract=6319778>
- [27] Islam, K. S. A. (2025). Transformer protection and fault detection through relay automation and machine learning. *IJSRED – International Journal of Scientific Research and Engineering Development*, 8(5), 2308–2320. <https://doi.org/10.5281/zenodo.17536362>
- [28] Pangen, S. (2026). Security centered wireless architecture for industrial IoT under EMC and RF regulatory constraints. *Saudi Journal of Engineering and Technology*, 11(4), 174–183. <https://doi.org/10.36348/sjet.2026.v11i04.003>

- [29] Junaid, A. (2026, July 29). Performance optimization of 5G NR networks through mobility management and carrier aggregation configuration. SSRN. <https://doi.org/10.2139/ssrn.7202280>
- [30] Abdullah, M. S. (2026). Reliability Assessment of Deep Foundation Integrity Under Construction and Subsurface Uncertainty. Zenodo. <https://doi.org/10.5281/zenodo.21906570>
- [31] Abdullah, M. S. (July 09, 2026). Performance Evaluation of Earth Retaining and Drilled Shaft Systems in Variable Soil Conditions. SSRN. <https://ssrn.com/abstract=7272199> or <http://dx.doi.org/10.2139/ssrn.7272199>
- [32] Ahmed, S. (2026, August 15). Reliability-aware predictive analytics for healthcare service access and resource allocation. SSRN. <https://doi.org/10.2139/ssrn.7289738>
- [33] Rahman, M. M. (2026, August 16). A multi-objective operational optimization model for lean manufacturing and industrial equipment resource allocation. SSRN. <https://doi.org/10.2139/ssrn.7292858>
- [34] Sumi, S. S. (2026). Explainable AI-enabled dynamic value stream analytics for waste detection and flow optimization in smart manufacturing. Preprints.org. <https://doi.org/10.20944/preprints202610.0286.v1>
- [35] Junaid, E. (2026). Unified SLO driven observability across AWS and GCP using CloudWatch and Stack driver and ELK and Splunk with error budgets. Research Square. <https://doi.org/10.21203/rs.3.rs-11222570/v1>
- [36] Junaid, E. (2026). Reliability modeling and automated incident response for Cadence based distributed systems SRE signals and RCA automation. Research Square. <https://doi.org/10.21203/rs.3.rs-11209235/v1>
- [37] Das, D. (2026, October 2). Adaptive distributed control and self-recovery of IoT-enabled microgrids under communication and component disturbances. SSRN. <https://doi.org/10.2139/ssrn.7551920>
- [38] Huq, S. N. (2026). A multi-criteria project governance framework for workforce process optimization and organizational resilience in service and healthcare organizations [Preprint]. Research Square. <https://doi.org/10.21203/rs.3.rs-11192743/v1>
- [39] Sumi, S. S. (2026). A human-in-the-loop multi-modal explainable digital twin framework for real-time maximization of productivity, and minimization of cost and carbon footprint in smart manufacturing [Preprint]. SSRN. <https://doi.org/10.2139/ssrn.7544338>
- [40] Junaid, E. (2026). Performance and resilience study of microservices traffic management using Nginx Ingress controllers on Kubernetes [Preprint]. SSRN. <https://doi.org/10.2139/ssrn.7539198>