



A Systematic Review of Machine Learning Applications in Cybersecurity Threat Detection and Classification (2018–2026)

Maishar Mostari Zenia¹;

[1]. Master of Science in Cybersecurity, Southeast Missouri State University, Cape Girardeau, MO, USA; Email: mzenia1s@semo.edu

Doi: [10.63125/6kg7kg75](https://doi.org/10.63125/6kg7kg75)

Received: 19 March 2026; **Revised:** 21 April 2026; **Accepted:** 19 May 2026; **Published:** 10 June 2026

Abstract

This study addresses the growing difficulty organizations face in detecting and classifying increasingly sophisticated cybersecurity threats when conventional signature-based and rule-based mechanisms are challenged by previously unseen attacks, changing malicious behavior, high-volume security data, and complex cloud and enterprise infrastructures. The purpose of the research is to systematically examine machine-learning applications in cybersecurity threat detection and classification and quantitatively determine how major machine-learning capabilities contribute to Cybersecurity Threat Detection and Classification Performance. The study combines a systematic review of 82 eligible studies published between 2018 and 2026 with a quantitative, cross-sectional, case-study-based empirical design focused on cybersecurity-oriented enterprise, network, and cloud-enabled organizational environments where machine learning is used for security monitoring and threat management. The empirical sample comprised cybersecurity analysts, information-security specialists, network-security engineers, SOC professionals, IT security personnel, machine-learning practitioners, and cybersecurity managers. Of 320 questionnaires distributed, 301 were returned and 286 usable responses were retained, yielding an 89.4% usable response rate. The key explanatory variables were ML-Based Automated Threat Detection, Intelligent Feature Learning and Pattern Recognition, Real-Time Anomaly and Intrusion Detection, and ML-Based Threat Classification Capability, with Cybersecurity Threat Detection and Classification Performance serving as the dependent variable. Data were analyzed using descriptive statistics, Cronbach's alpha, KMO and Bartlett's tests, Pearson correlation, multiple regression, ANOVA, standardized beta coefficients, tolerance, VIF, and Durbin-Watson diagnostics. The findings showed that Cybersecurity Threat Detection and Classification Performance recorded $M = 4.18$, $SD = 0.53$, while Real-Time Anomaly and Intrusion Detection achieved $M = 4.16$, $SD = 0.55$. All four predictors were significantly associated with performance, with Real-Time Anomaly and Intrusion Detection showing the strongest correlation, $r = .74$, followed by ML-Based Threat Classification Capability, $r = .71$, ML-Based Automated Threat Detection, $r = .69$, and Intelligent Feature Learning and Pattern Recognition, $r = .63$, all $p < .001$. The regression model achieved $R = .834$, $R^2 = .696$, adjusted $R^2 = .692$, $F(4, 281) = 160.84$, $p < .001$, explaining 69.6% of the variance. Real-Time Anomaly and Intrusion Detection emerged as the strongest predictor, $\beta = .31$, followed by ML-Based Threat Classification Capability, $\beta = .28$, ML-Based Automated Threat Detection, $\beta = .24$, and Intelligent Feature Learning and Pattern Recognition, $\beta = .18$. All five hypotheses were supported. These findings imply that organizations should prioritize real-time anomaly recognition, accurate threat classification, automated detection, and intelligent feature learning as complementary capabilities for improving cybersecurity performance across enterprise and cloud environments.

Keywords

Machine Learning; Cybersecurity Threat Detection; Real-Time Anomaly Detection; Threat Classification; Intelligent Feature Learning;

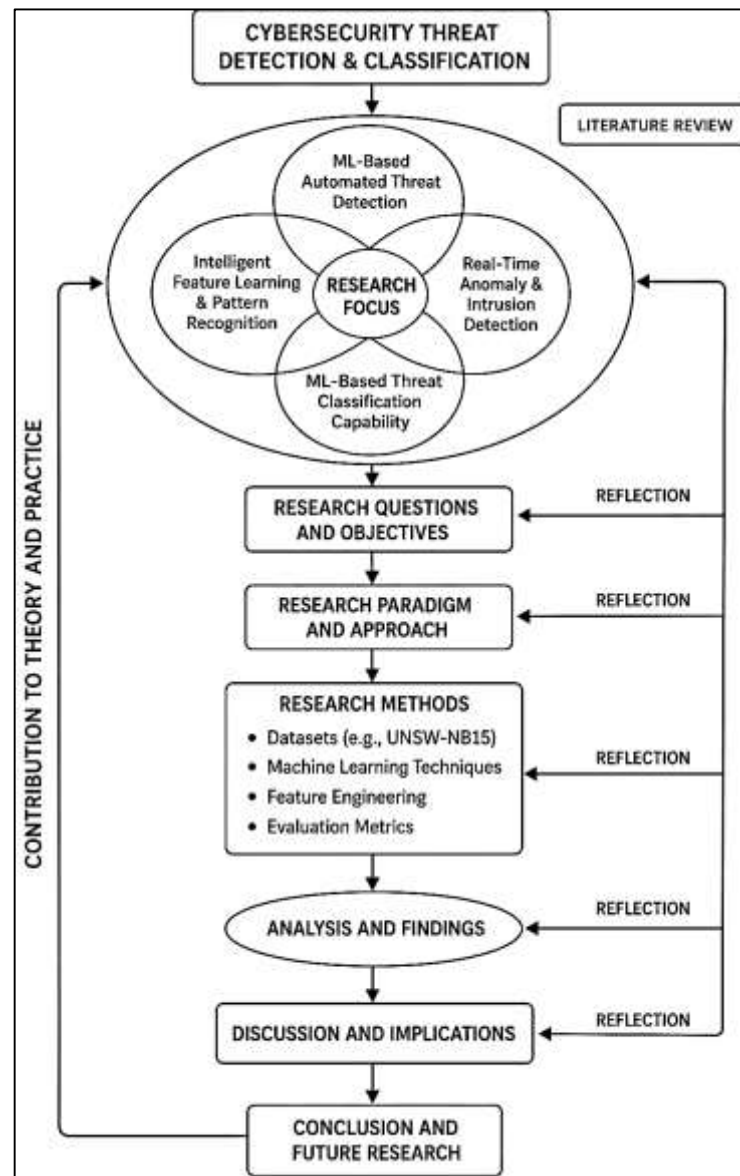
INTRODUCTION

Cybersecurity can be defined as the coordinated application of technologies, computational mechanisms, organizational processes, analytical techniques, and protective controls intended to preserve the confidentiality, integrity, availability, authenticity, and authorized use of digital systems, networks, software, devices, and information resources against malicious interference and unauthorized access. Within cybersecurity, a threat represents an event, behavior, action, or computational activity capable of exploiting vulnerabilities and disrupting legitimate digital operations. Threat detection refers to the systematic identification of malicious, suspicious, or anomalous activities within computing environments, whereas threat classification refers to the assignment of identified activities to defined categories such as malware, phishing, ransomware, denial-of-service attacks, botnets, intrusions, insider threats, or other forms of malicious behavior. Machine learning represents a computational approach through which algorithms identify statistical structures and patterns within data and use those learned relationships to make predictions or classifications without relying exclusively on manually programmed decision rules. The relationship between machine learning and cybersecurity has emerged from the understanding that malicious and legitimate activities can often be represented as classification, anomaly-detection, feature-learning, and pattern-recognition problems. Early applications demonstrated that support vector machines and artificial neural networks could learn patterns from network data and differentiate intrusive activities from legitimate behavior (Chen et al., 2005; Zhang & Shen, 2005). Machine-learning methods were also introduced to reduce false-positive alarms generated by intrusion-detection systems, since large numbers of incorrect security alerts can make the identification of genuine attacks increasingly difficult for cybersecurity analysts (Pietraszek & Tanner, 2005). Anomaly-based cybersecurity systems subsequently received considerable research attention because they establish profiles of expected behavior and identify substantial deviations that could represent malicious activities (Garcia-Teodoro et al., 2009; Patcha & Park, 2007). The international significance of these capabilities has increased as financial institutions, governments, telecommunications networks, healthcare systems, industrial organizations, educational institutions, cloud platforms, and critical infrastructures have become interconnected through digital technologies. Machine-learning approaches offer mechanisms for analyzing substantial volumes of network traffic and system information in environments where continuous manual inspection is not operationally practical. Various classifiers, clustering techniques, neural networks, Bayesian approaches, evolutionary algorithms, and hybrid models have consequently been examined for intrusion and threat detection (Liao et al., 2013; Tsai et al., 2009). Cybersecurity classification also differs from conventional closed-world machine-learning applications because attackers deliberately modify their behaviors and because operational network conditions can change over time (Sommer & Paxson, 2010). The learning mechanism itself can also become a target because adversaries may manipulate training observations or exploit weaknesses in classification boundaries (Barreno et al., 2010).

The development of data-driven cybersecurity has progressively placed machine learning at the center of automated threat detection because modern security systems must perform two related functions: distinguishing malicious events from legitimate activities and determining the specific category to which a detected attack belongs. Network anomaly-detection research has established that malicious behavior can be represented through packet-level information, network-flow attributes, temporal relationships, behavioral indicators, statistical characteristics, and other forms of digital evidence that can be processed through computational learning models (Bhuyan et al., 2014). The effectiveness of such models is closely associated with the datasets from which they learn because training and evaluation data determine which forms of legitimate and malicious behavior are represented during model development. The introduction of the UNSW-NB15 dataset reflected growing recognition that intrusion-detection research required datasets containing realistic legitimate traffic together with multiple categories of contemporary cybersecurity attacks rather than relying exclusively on older benchmark data (Moustafa & Slay, 2015). Research synthesizing data-mining and machine-learning approaches has identified supervised classification, unsupervised clustering, association methods, decision trees, support vector machines, neural networks, random forests, Bayesian techniques, evolutionary algorithms, and hybrid approaches as major computational strategies for cybersecurity

intrusion detection (Buczak & Guven, 2016). Feature representation forms another central component of this process because network connections, executable files, URLs, application activities, system calls, protocols, and security logs may contain large numbers of variables, not all of which contribute equally to separating benign and malicious activities. Machine-learning systems therefore depend on feature selection, feature extraction, or representation-learning mechanisms capable of transforming raw cybersecurity observations into informative representations. Deep-learning research on malware system-call sequences demonstrated that convolutional and recurrent structures can capture both local characteristics and sequential behavior associated with malicious software (Kolosnjaji et al., 2016).

Figure 1: Systematic Research Framework for Machine Learning-Based Cybersecurity Threat Detection and Classification



Machine-learning classification has also been applied to malicious URLs by extracting lexical, structural, and related characteristics that distinguish harmful online resources from legitimate websites (Vanhoenshoven et al., 2016). Malware-detection research has similarly demonstrated that feature extraction and classification are interconnected processes because the accuracy with which malicious software is categorized depends heavily on the quality and discriminative value of the attributes supplied to a learning algorithm (Ye et al., 2017). Phishing-detection research has extended these principles to web environments by using machine-learning methods to identify fraudulent

websites from characteristics available at the client side, reducing dependence on static blacklist approaches alone (Jain & Gupta, 2018). Broader cybersecurity research has consequently treated machine learning as an analytical architecture encompassing data preprocessing, feature generation, feature learning, behavioral analysis, anomaly recognition, and classification rather than as a single algorithmic technique (Xin et al., 2018). These processes are especially relevant to the present study because automated threat detection, intelligent feature learning and pattern recognition, real-time anomaly and intrusion detection, and ML-based threat classification represent related dimensions through which machine-learning applications can be examined within cybersecurity environments.

The period from 2018 onward represented an important phase in the application of machine learning to cybersecurity threat detection and classification because deep-learning and representation-learning techniques became increasingly incorporated into network security, malware analysis, botnet identification, phishing detection, and intrusion-detection architectures. Deep learning allows computational models to form hierarchical representations from input data, enabling cybersecurity systems to identify complex nonlinear patterns without depending entirely on extensive manually engineered feature sets. Deep-learning-based network intrusion research demonstrated that representation-learning architectures could transform network data into discriminative internal features and use these representations to separate normal from malicious traffic (Shone et al., 2018). Similar approaches were applied within Internet of Things environments, where large numbers of connected devices created distinctive cybersecurity challenges related to botnets, compromised devices, unauthorized communications, and abnormal network behavior. Deep autoencoder models demonstrated the capacity to learn profiles of normal IoT traffic and identify anomalous behavior generated by compromised devices, providing an unsupervised mechanism for detecting botnet activity (Meidan et al., 2018). The development of cybersecurity datasets also became closely linked to machine-learning evaluation because meaningful comparison between classifiers requires traffic containing multiple attack types and representative normal activity. Research on contemporary intrusion-detection datasets incorporated benign traffic alongside attack categories and evaluated network features according to their usefulness for machine-learning-based classification (Sharafaldin et al., 2018). Data-driven cybersecurity research further expanded the analytical scope beyond individual alerts toward the processing of heterogeneous security information for the characterization and prediction of cybersecurity incidents (Sun et al., 2019). Reviews of machine learning in cybersecurity identified intrusion detection, malware recognition, critical-infrastructure security, and identification of unknown or zero-day malicious activities among the major application areas of learning-based cybersecurity systems (Handa et al., 2019). Phishing detection has similarly been formulated as a machine-learning classification problem in which URL characteristics, linguistic attributes, and computational features are evaluated by classifiers to identify potentially fraudulent web resources (Sahingoz et al., 2019). Deep-learning applications have included convolutional neural networks, recurrent neural networks, autoencoders, deep belief networks, generative architectures, and related models applied across malware, intrusion, spam, insider-threat, botnet, and false-data-injection detection tasks (Berman et al., 2019). Experimental applications have also demonstrated that deep neural networks can distinguish multiple categories of network attacks within large-scale intrusion-detection datasets (Vinayakumar et al., 2019). Dataset characteristics remain central to these evaluations because publicly available network-security datasets differ in attack distributions, feature structures, capture environments, traffic characteristics, labeling procedures, and realism (Ring et al., 2019). Comparative research has therefore increasingly evaluated deep-learning architectures together with the datasets and cybersecurity conditions under which reported detection and classification performance is obtained (Ferrag et al., 2020).

Machine-learning-based cybersecurity threat detection and classification also require consideration of detection accuracy, classification reliability, computational efficiency, data representativeness, class distribution, generalization capability, and resistance to deliberate adversarial manipulation. Overall classification accuracy alone may provide an incomplete representation of cybersecurity performance because security datasets often contain unequal distributions of benign and malicious observations, while some attack classes occur much less frequently than others. A classifier can therefore report high aggregate accuracy while failing to detect important minority attack categories. Cybersecurity studies

consequently employ multiple performance measurements, including precision, recall, F1-score, detection rate, false-positive rate, false-negative rate, receiver operating characteristic measures, confusion matrices, and class-specific performance indicators. Deep-learning research has emphasized that cybersecurity datasets are frequently characterized by high dimensionality, heterogeneous variables, extensive data volumes, and complex relationships among attack behaviors, characteristics that support the application of representation-learning methods capable of extracting nonlinear structures from security data (Dixit & Silakari, 2021; Li et al., 2021). Cybersecurity machine learning nevertheless operates within an adversarial environment in which attackers may intentionally modify observable properties in order to avoid detection, manipulate training information, probe decision boundaries, or influence the predictions generated by defensive models. Research in adversarial machine learning has demonstrated that classifiers can be affected through strategically constructed inputs and has distinguished between different attack mechanisms according to the adversary's knowledge, objectives, influence, and stage of interference with a learning system (Biggio & Roli, 2018; Tonay, 2026). These concerns are particularly important for systems responsible for classifying observations as legitimate, malicious, anomalous, phishing-related, malware-related, intrusion-related, or members of more specific threat families. Data representativeness introduces another methodological issue because classification models trained on limited, artificially generated, or outdated datasets may report strong benchmark performance without reproducing the conditions encountered in operational cybersecurity networks (Ring et al., 2019; Rony & Md, 2026). Malicious URL detection illustrates this issue because classifiers may use lexical, structural, host-based, content-based, or contextual features, while differences in dataset construction and feature-selection procedures can substantially affect reported results (Aljabri et al., 2022). Comparative research has evaluated conventional classifiers such as support vector machines, random forests, decision trees, and k-nearest-neighbor algorithms for identifying malicious URLs, demonstrating that algorithm selection and feature representation jointly determine classification performance (Abad et al., 2023; Sadia, 2026). Research published in 2024 continued to examine malicious URL detection as a machine-learning classification problem by comparing multiple learning methods and evaluating their capacity to differentiate harmful digital resources from legitimate ones (Reyes-Dorta et al., 2024). These performance dimensions provide an empirical basis for examining how different machine-learning capabilities relate to overall cybersecurity threat detection and classification performance.

A systematic examination of machine-learning applications in cybersecurity threat detection and classification requires integration of the algorithms employed, cybersecurity threats examined, datasets utilized, feature-learning strategies adopted, performance criteria reported, and operational functions performed by learning systems. The existing literature encompasses supervised approaches such as support vector machines, decision trees, random forests, k-nearest-neighbor methods, Bayesian classifiers, and artificial neural networks, together with unsupervised and deep-learning approaches such as clustering, autoencoders, convolutional neural networks, recurrent neural networks, and other representation-learning architectures (Buczak & Guven, 2016; Xin et al., 2018). These approaches have been applied to distinct but interconnected security problems involving malware detection and categorization, network intrusion detection, botnet identification, phishing recognition, malicious URL classification, abnormal traffic identification, and detection of previously unrecognized patterns of malicious behavior (Berman et al., 2019; Nishat, 2026; Ye et al., 2017). The diversity of these applications indicates that cybersecurity threat detection can be examined through several complementary machine-learning capabilities. ML-based automated threat detection represents the ability of computational systems to identify potentially malicious events with limited dependence on continuous manual analysis. Intelligent feature learning and pattern recognition represent the capacity to extract, select, or construct discriminative characteristics from raw cybersecurity observations. Real-time anomaly and intrusion detection refers to the identification of unusual or malicious activities as network and system events occur. ML-based threat classification capability represents the ability of learning algorithms to assign identified malicious events to appropriate categories or attack families. Research examining deep-learning intrusion detection has demonstrated the connection between feature learning and classification by incorporating both processes within integrated detection architectures (Ferrag et al., 2020; Badrul, 2026). Reviews of cybersecurity machine learning have similarly documented

considerable variation in algorithms, preprocessing procedures, datasets, feature representations, attack categories, and evaluation methodologies across published studies (Dixit & Silakari, 2021; Chowdhury, 2026). More recent reviews have continued to identify methodological diversity across machine-learning-based cybersecurity research, particularly in relation to datasets, security domains, algorithms, and performance assessment procedures (Pervaz, 2026; Vourganas & Michala, 2024). Within the present study, these established research dimensions provide the basis for systematically examining machine-learning applications reported in cybersecurity threat detection and classification while organizing ML-Based Automated Threat Detection, Intelligent Feature Learning and Pattern Recognition, Real-Time Anomaly and Intrusion Detection, and ML-Based Threat Classification Capability as measurable explanatory constructs associated with Cybersecurity Threat Detection and Classification Performance.

Background of the Study

Cybersecurity has become a central concern for governments, businesses, financial institutions, healthcare organizations, educational institutions, technology companies, critical infrastructure operators, and individual users because digital systems are increasingly exposed to sophisticated and rapidly evolving forms of malicious activity. The expansion of cloud computing, Internet of Things devices, mobile technologies, online financial services, remote-working platforms, artificial intelligence, and interconnected organizational networks has created extensive opportunities for digital transformation while simultaneously increasing the volume, complexity, and diversity of cybersecurity threats. Traditional security mechanisms have largely depended on predefined signatures, static rules, manual monitoring, and previously identified attack characteristics. Such approaches can remain useful for detecting known threats, yet their effectiveness becomes limited when organizations encounter previously unseen attacks, rapidly changing malicious behaviors, encrypted traffic, highly dynamic network activities, or sophisticated attack strategies specifically designed to evade conventional detection mechanisms. Machine learning has consequently emerged as an important computational approach for strengthening cybersecurity threat detection and classification because learning algorithms can analyze large volumes of security data, discover patterns, identify anomalies, differentiate legitimate from malicious activities, and classify identified threats into meaningful categories. Machine-learning applications in cybersecurity include malware detection, phishing identification, intrusion detection, botnet detection, ransomware recognition, malicious URL classification, denial-of-service detection, anomaly identification, and behavioral threat analysis. These applications employ diverse learning methods, including support vector machines, decision trees, random forests, k-nearest-neighbor algorithms, artificial neural networks, clustering methods, deep neural networks, convolutional neural networks, recurrent neural networks, autoencoders, ensemble models, and other intelligent computational techniques. The period between 2018 and 2026 is particularly important for studying this area because cybersecurity research during this timeframe has increasingly incorporated advanced machine-learning and deep-learning architectures, new cybersecurity datasets, improved feature-learning mechanisms, real-time anomaly detection, and more sophisticated classification approaches. Within this research context, four capabilities are particularly relevant: ML-Based Automated Threat Detection, Intelligent Feature Learning and Pattern Recognition, Real-Time Anomaly and Intrusion Detection, and ML-Based Threat Classification Capability. These capabilities collectively represent important dimensions through which machine learning can strengthen Cybersecurity Threat Detection and Classification Performance. Therefore, examining the development, application, effectiveness, and statistical relationships associated with these capabilities provides a structured basis for understanding the role of machine learning in contemporary cybersecurity threat-management environments.

Problem Statement

The increasing sophistication of cybersecurity threats has created major challenges for organizations attempting to identify, analyze, and classify malicious activities accurately and rapidly. Modern attacks can change their behavioral characteristics, exploit unknown vulnerabilities, imitate legitimate network behavior, target different technological environments, and generate large quantities of complex security data that are difficult to evaluate manually. Conventional signature-based and rule-based security mechanisms are often dependent on previously identified threat patterns, which can reduce

their effectiveness when malicious activities are new, highly adaptive, or deliberately modified to evade established detection rules. Machine learning has been widely introduced to address these challenges through automated threat identification, intelligent pattern recognition, anomaly detection, and attack classification. However, the existing literature contains substantial variation in the machine-learning algorithms employed, datasets selected, threat categories examined, features used, experimental environments considered, and performance metrics reported. Some studies emphasize intrusion detection, while others concentrate on malware, phishing, malicious URLs, botnets, ransomware, or other individual attack types. The reported effectiveness of machine-learning techniques also differs across datasets and cybersecurity environments, making it difficult to determine which capabilities most consistently contribute to broader cybersecurity threat detection and classification performance. Furthermore, many studies assess isolated algorithms or individual security applications without examining the combined relationships among automated threat detection, intelligent feature learning, real-time anomaly and intrusion detection, and threat classification capability within a unified analytical framework. This fragmentation limits the ability to understand how different machine-learning capabilities interact with overall cybersecurity detection performance. There is therefore a need for a systematic examination of machine-learning applications between 2018 and 2026 together with a quantitative empirical evaluation of the principal ML capabilities associated with cybersecurity threat detection and classification. The present research addresses this problem by integrating systematic literature analysis with a cross-sectional, case-study-based quantitative assessment using a structured five-point Likert-scale instrument, descriptive statistics, reliability and validity testing, Pearson correlation analysis, multiple regression modeling, ANOVA, and hypothesis testing.

Purpose and Objectives of the Study

The primary purpose of this study is to systematically examine machine-learning applications in cybersecurity threat detection and classification between 2018 and 2026 and quantitatively evaluate the principal machine-learning capabilities associated with effective Cybersecurity Threat Detection and Classification Performance. The study is designed to integrate evidence from the published cybersecurity literature with empirical perceptions obtained from professionals operating within relevant cybersecurity and information-technology environments. Specifically, the research seeks to identify the major machine-learning algorithms, models, datasets, security applications, and threat categories that have characterized cybersecurity detection and classification research during the selected review period. It further aims to assess the extent to which ML-Based Automated Threat Detection contributes to the identification of suspicious and malicious activities within digital environments. Another objective is to evaluate the role of Intelligent Feature Learning and Pattern Recognition in extracting and recognizing security-relevant characteristics from network traffic, system activities, malicious software, URLs, and other cybersecurity data. The study also seeks to examine whether Real-Time Anomaly and Intrusion Detection is significantly associated with improved cybersecurity threat detection and classification performance by enabling organizations to identify abnormal behaviors and potentially malicious activities as they occur. A further objective is to determine the influence of ML-Based Threat Classification Capability on the accurate categorization of detected cyber threats into meaningful attack classes. In addition, the research aims to establish the individual and combined statistical relationships between these four machine-learning capabilities and Cybersecurity Threat Detection and Classification Performance through Pearson correlation and multiple regression analyses. The study also seeks to assess the reliability and validity of the proposed research constructs and determine whether the empirical evidence supports the formulated hypotheses. Through these objectives, the research establishes a structured quantitative framework for evaluating how major machine-learning capabilities relate to the effectiveness of contemporary cybersecurity threat detection and classification systems.

Research Hypotheses

The research hypotheses have been developed to statistically examine the relationships between the selected machine-learning capabilities and Cybersecurity Threat Detection and Classification Performance. The first hypothesis, H1, proposes that ML-Based Automated Threat Detection has a significant positive effect on Cybersecurity Threat Detection and Classification Performance, based on the assumption that automated identification of malicious activities can strengthen the speed and

effectiveness of security monitoring. The second hypothesis, H2, proposes that Intelligent Feature Learning and Pattern Recognition has a significant positive effect on Cybersecurity Threat Detection and Classification Performance, reflecting the importance of extracting discriminative security characteristics and recognizing complex attack patterns from large and heterogeneous datasets. The third hypothesis, H3, states that Real-Time Anomaly and Intrusion Detection has a significant positive effect on Cybersecurity Threat Detection and Classification Performance, as timely recognition of abnormal network or system behavior can support the identification of both known and unfamiliar attack patterns. The fourth hypothesis, H4, proposes that ML-Based Threat Classification Capability has a significant positive effect on Cybersecurity Threat Detection and Classification Performance because accurate categorization of malicious events can support the differentiation of attack types and improve the analytical quality of cybersecurity detection systems. The fifth hypothesis, H5, proposes that ML-Based Automated Threat Detection, Intelligent Feature Learning and Pattern Recognition, Real-Time Anomaly and Intrusion Detection, and ML-Based Threat Classification Capability collectively have a significant predictive effect on Cybersecurity Threat Detection and Classification Performance. These hypotheses establish the statistical structure of the quantitative component of the study and allow each explanatory construct to be examined independently as well as collectively. Their evaluation will be conducted through descriptive statistics, Pearson correlation analysis, multiple regression modeling, ANOVA, standardized regression coefficients, significance testing, and relevant diagnostic measures using the data collected through the five-point Likert-scale research instrument.

Significance of the Research

- i. Academic significance: The study contributes to the academic literature by systematically organizing machine-learning applications in cybersecurity threat detection and classification across the 2018-2026 period. It brings together research concerning different algorithms, cybersecurity threats, datasets, feature-learning approaches, anomaly-detection techniques, and classification mechanisms within a common analytical structure.
- ii. Methodological significance: The research combines a systematic review with a quantitative, cross-sectional, case-study-based empirical assessment. This approach enables the study to move beyond a descriptive summary of published machine-learning techniques by statistically examining relationships among selected machine-learning capabilities and cybersecurity performance.
- iii. Cybersecurity practitioner significance: The research is relevant to cybersecurity analysts, security operations center professionals, network-security specialists, threat-intelligence personnel, and information-security managers because it identifies the machine-learning capabilities most closely associated with effective threat detection and classification.
- iv. Organizational significance: Organizations can use the study to understand how automated threat detection, intelligent feature learning, anomaly detection, and threat classification operate as complementary components of machine-learning-enabled cybersecurity. This is particularly relevant for organizations managing extensive network infrastructures, cloud environments, financial systems, digital services, sensitive information, or critical operational resources.
- v. Machine-learning development significance: The study provides a structured assessment of the relationship between machine-learning capabilities and cybersecurity performance, enabling researchers and developers to evaluate detection systems in terms of more than algorithmic accuracy alone. Feature learning, anomaly recognition, classification ability, and automated detection are treated as interconnected dimensions of cybersecurity machine-learning performance.
- vi. Theoretical significance: By incorporating Signal Detection Theory into the study, the research provides a theoretical basis for understanding the distinction between legitimate and malicious activities, detection sensitivity, classification decisions, false-positive outcomes, false-negative outcomes, and overall security decision performance.
- vii. Empirical significance: The research generates quantitative evidence through five-point Likert-scale measurements, descriptive statistics, reliability and validity assessment, Pearson correlation, regression analysis, ANOVA, and hypothesis testing. This provides measurable evidence concerning the strength and significance of the relationships between machine-learning capabilities and Cybersecurity Threat Detection and Classification Performance.

LITERATURE REVIEW

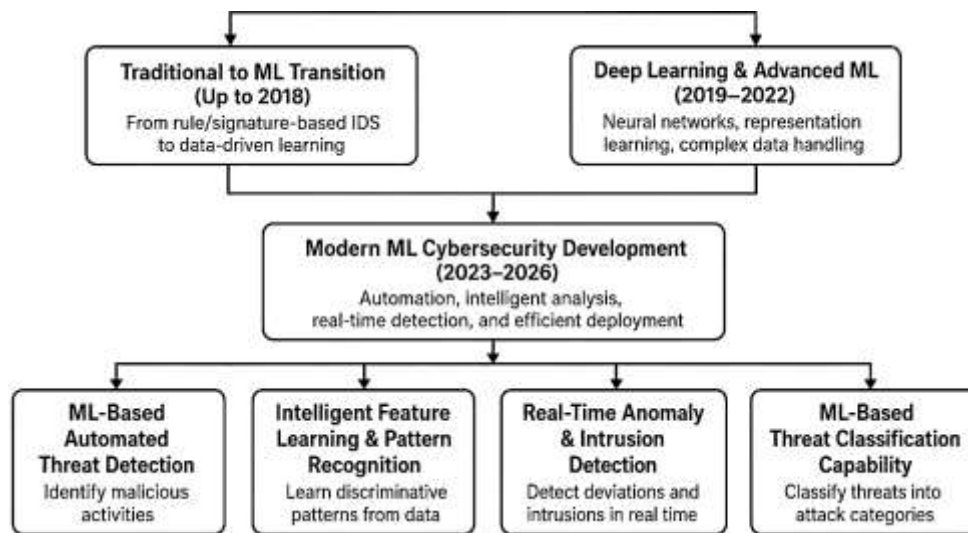
The literature on machine learning in cybersecurity has expanded considerably as organizations have sought computational mechanisms capable of detecting increasingly complex and diverse forms of malicious digital activity. Machine-learning-based cybersecurity research encompasses a wide range of techniques, including supervised learning, unsupervised learning, semi-supervised approaches, ensemble methods, artificial neural networks, deep-learning architectures, representation-learning models, and hybrid computational systems. These methods have been applied to numerous cybersecurity tasks such as network intrusion detection, malware identification, phishing recognition, ransomware detection, botnet analysis, malicious URL classification, anomaly detection, denial-of-service identification, behavioral monitoring, and threat categorization. Within this body of research, the effectiveness of machine-learning systems depends not only on the algorithm employed but also on the nature and quality of the cybersecurity data, the features used to represent legitimate and malicious behavior, the degree of class imbalance, the attack categories included in the dataset, and the performance measures adopted for evaluation. The literature also reveals a transition from extensive dependence on manually engineered security features toward intelligent feature-learning mechanisms capable of extracting useful representations directly from complex cybersecurity data. Real-time anomaly and intrusion detection has become another important area because security systems must identify suspicious activities while network and system events are occurring rather than only after an attack has been completed. Threat classification is equally important because identifying the existence of malicious behavior does not necessarily establish the particular category, severity, or behavioral characteristics of the attack. The present literature review therefore examines six closely connected areas: the evolution and application of machine learning in cybersecurity threat detection and classification between 2018 and 2026; ML-Based Automated Threat Detection and Cybersecurity Performance; Intelligent Feature Learning, Pattern Recognition, and Real-Time Anomaly Detection; Machine-Learning-Based Threat Classification and Detection Performance; Signal Detection Theory as the theoretical framework; and the conceptual framework linking the selected machine-learning capabilities with Cybersecurity Threat Detection and Classification Performance.

Machine Learning in Cybersecurity Threat Detection

The evolution of machine learning in cybersecurity threat detection has been shaped by the increasing difficulty of using exclusively rule-based and signature-dependent mechanisms to manage heterogeneous, high-volume, and rapidly changing attack data. Earlier intrusion detection systems relied heavily on manually specified signatures, expert rules, thresholds, and statistical indicators that could recognize known malicious behaviors but often became less effective when attack characteristics changed or when previously unseen patterns appeared. Machine learning altered this structure by enabling security systems to learn decision boundaries from historical observations and classify network events according to patterns discovered in data. By 2018, cybersecurity research had moved beyond asking whether machine learning could be used for security and had begun comparing when conventional machine-learning algorithms and deeper neural architectures were suitable for particular detection tasks. Research evaluating machine and deep learning across cybersecurity applications showed that learning-based techniques could support several forms of malicious activity detection, while their effectiveness depended on realistic data, appropriate features, sound evaluation procedures, and correspondence between experimental conditions and operational security environments ([Apruzzese et al., 2018](#); [Debasish, 2021](#)). This stage was important because machine learning was increasingly positioned as a mechanism for assisting analysts in filtering large volumes of events, identifying suspicious observations, and prioritizing activities requiring investigation. Supervised algorithms such as support vector machines, decision trees, random forests, logistic classifiers, and nearest-neighbor techniques became associated with attack classification when labeled examples were available, whereas clustering and other unsupervised strategies supported the identification of deviations where labels were limited. The emergence of these approaches changed intrusion detection from a predominantly signature-matching activity into a data-driven classification problem involving feature construction, model training, validation, and performance assessment. This transition established a foundation for broader applications involving malware recognition, phishing detection, botnet identification, malicious traffic analysis, denial-of-service detection, and anomaly

recognition across enterprise, cloud, mobile, and Internet of Things environments.

Figure 2: Evolution of Machine Learning in Cybersecurity Threat Detection and Classification (2018–2026)



As machine-learning applications expanded, cybersecurity detection became increasingly associated with neural networks, deep learning, automated feature representation, and the processing of more complex security datasets. Traditional machine-learning models commonly depend on a defined set of input variables generated through feature engineering, requiring researchers or security specialists to determine which characteristics of network traffic, system activities, executable files, URLs, or user behavior can distinguish legitimate events from attacks. Neural and deep-learning architectures expanded this process by learning increasingly abstract representations from data and combining representation learning with classification. A comprehensive examination of neural networks for intrusion detection showed that neural approaches had become an established component of learning-based IDS research, while performance remained strongly influenced by network architecture, training configuration, dataset selection, and the characteristics of the attack classes being analyzed (Drewek-Ossowicka et al., 2021; Abdur & Iftekhar, 2021). This development was particularly relevant because cybersecurity observations may contain nonlinear relationships, temporal dependencies, rare attack classes, redundant variables, and highly imbalanced distributions. Deep architectures such as convolutional neural networks, recurrent neural networks, long short-term memory networks, and autoencoders enabled researchers to approach these characteristics through different forms of learned representation. Comparative research on machine-learning intrusion detection further demonstrated that no single algorithm can be assumed to dominate every network-security setting because different learning principles produce different advantages and limitations across datasets, attack types, and classification conditions (Debasish, 2022; Zhang et al., 2022). Consequently, the evolution of machine-learning cybersecurity systems involved more than replacing one classifier with another; it increasingly required selecting models according to the structure of the data and the operational objective of the detection task. Supervised intrusion detection uses labeled traffic to learn mappings between observations and known attack categories, while anomaly-based methods identify deviations from modeled normal behavior. Hybrid approaches combine complementary techniques. These developments broadened machine-learning applications from binary benign-versus-malicious decisions toward multiclass threat classification and representation-learning pipelines capable of discovering security-relevant patterns from raw or minimally processed data.

The more recent development of machine learning in cybersecurity has been characterized by greater emphasis on automation, intelligent security-data analysis, specialized deployment environments, and the relationship between detection performance and operational constraints. Organizations generate

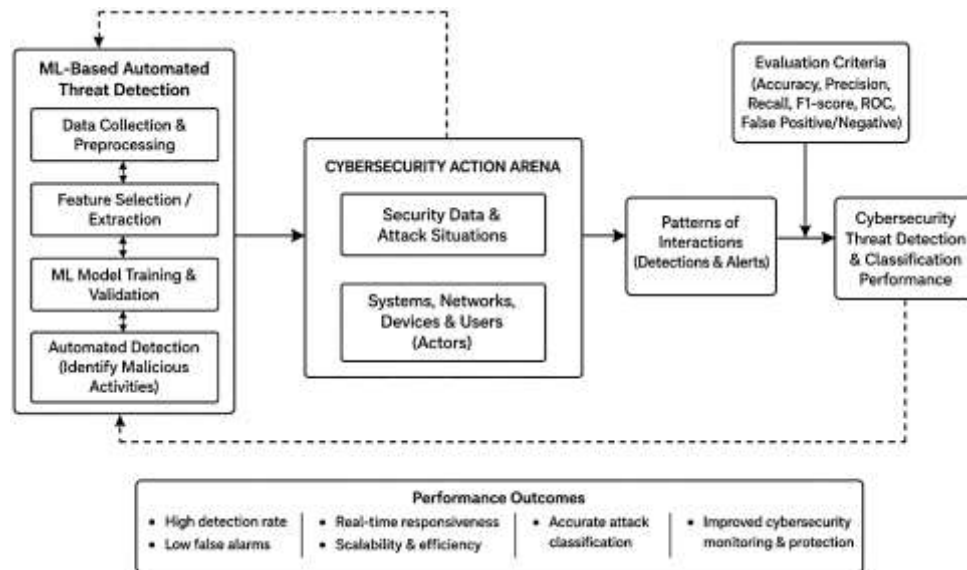
security information from endpoints, network devices, cloud services, applications, authentication systems, industrial components, and connected devices, creating large streams of observations that must be transformed into classifications, anomaly scores, alerts, and threat categories. Machine-learning models have therefore been applied across multiple stages of the detection process, including preprocessing, feature selection, feature extraction, behavioral profiling, anomaly identification, attack recognition, classification, and alert prioritization. Research on intelligent data analysis and automation has described machine learning as a means of extracting actionable patterns from cybersecurity data and supporting automated security decisions across a range of cyber-protection applications (Ashfaq & Mohammad, 2022; Sarker, 2023). The development of machine-learning-based intrusion detection has also become closely associated with benchmark datasets, evaluation metrics, class-imbalance handling, computational requirements, and the distinction between supervised, unsupervised, and deep-learning detection strategies. A 2024 comprehensive survey of ML- and DL-based intrusion detection emphasized that contemporary IDS research evaluates not only algorithms but also attack categories, datasets, performance indicators, strengths, and methodological limitations, reflecting the increased maturity and complexity of the field (Ali et al., 2024; Sheak & Risha, 2022). Within the 2018-2026 review scope of the present research, this evolution provides a basis for organizing machine-learning cybersecurity applications according to the security capability they perform rather than treating all algorithms as equivalent. Automated threat detection concerns identifying suspicious or malicious events with reduced dependence on continuous manual inspection; intelligent feature learning and pattern recognition concern discovering discriminative characteristics from complex cyber data; real-time anomaly and intrusion detection concern the timely recognition of behavioral deviations and unauthorized activity; and threat classification concerns assigning detected incidents to meaningful malicious categories. These capabilities can be implemented through different algorithms and architectures, but they collectively represent the development of machine learning into an integrated analytical component of contemporary cybersecurity threat detection and classification systems.

ML-Based Automated Threat Detection and Cybersecurity Performance

Machine-learning-based automated threat detection has become a central component of contemporary cybersecurity because organizations must identify malicious activities across network traffic, endpoint events, connected devices, application logs, and other digital sources at a speed and scale that exceed the capacity of exclusively manual monitoring. Automated threat detection refers to the use of computational models that continuously analyze security-relevant observations, recognize abnormal or malicious patterns, and generate classifications or alerts with limited direct human intervention. Within machine-learning-based cybersecurity, this process usually begins with data collection and preprocessing, followed by feature extraction or feature selection, model training, validation, and the classification of incoming observations as benign or potentially malicious. The importance of automation is particularly evident in network intrusion detection, where the volume and velocity of traffic require defensive systems to evaluate large numbers of connections while maintaining acceptable detection rates and false-alarm levels. An influential example is Kitsune, an online network intrusion detection framework that uses an ensemble of autoencoders to learn normal network behavior without supervised labels and to identify deviations associated with attacks. Its architecture demonstrated that unsupervised learning could support continuous anomaly detection while remaining computationally efficient enough for deployment on resource-constrained network devices (Rashedul & Kaium, 2022; Mirsky et al., 2018). Distributed environments created additional requirements because cyberattacks may emerge from multiple connected devices rather than a single centralized source. Deep-learning-based distributed detection has therefore been examined as a mechanism for identifying attacks across Internet of Things environments, where local observations can be processed using learned representations and coordinated detection structures. A distributed deep-learning approach showed that combining distributed computational architecture with deep models could improve cyberattack detection compared with conventional centralized and shallow-learning configurations in IoT settings (Diro & Chilamkurti, 2018; Rashedul & Kaium, 2022). These developments positioned automated threat detection as a multi-stage cybersecurity capability in which machine learning supports continuous observation, behavioral modeling, anomaly recognition, and

security-event classification across increasingly distributed digital infrastructures.

Figure 3: ML-Based Automated Threat Detection Framework for Cybersecurity Threat Detection and Classification Performance



The relationship between automated threat detection and cybersecurity performance depends not only on whether a machine-learning model can identify attacks, but also on how accurately and consistently it differentiates malicious activities from legitimate behavior across multiple attack categories. Cybersecurity performance in this context can be represented through measures such as accuracy, precision, recall, F1-score, detection rate, false-positive rate, false-negative rate, receiver operating characteristic performance, and the capacity to recognize previously unseen or infrequent malicious activities. Internet of Things environments illustrate the importance of this multidimensional evaluation because connected sensors and devices may be exposed to denial-of-service attacks, probing activities, malicious control operations, scanning, spying, and configuration-related anomalies. Comparative research evaluating logistic regression, support vector machines, decision trees, random forests, and artificial neural networks for IoT attack and anomaly detection found substantial differences in model behavior across performance measures, demonstrating that strong overall accuracy should be interpreted together with precision, recall, F1-score, and ROC-based evaluation (Hasan et al., 2019; Chowdhury & Tonay, 2022). Automated threat detection therefore requires models capable of processing relevant security features while limiting unnecessary computational complexity. Feature importance is especially significant because high-dimensional cybersecurity datasets may include redundant or weakly informative variables that increase processing requirements without improving detection. A machine-learning intrusion-detection framework based on ranked security features and a generalized decision-tree structure demonstrated how feature selection can be incorporated into automated cybersecurity analysis to reduce dimensionality while preserving strong predictive performance for previously unseen test observations (Hossan, 2022; Abushark, et al., 2020). This connection between feature selection and automated detection is directly relevant to Cybersecurity Threat Detection and Classification Performance because an effective system must balance detection capability with the efficiency required for operational use. Machine-learning automation is therefore not limited to generating a final benign-or-malicious label; it includes determining which characteristics should influence classification, reducing irrelevant information, selecting suitable decision mechanisms, and producing security outputs that can be evaluated consistently across different threat conditions.

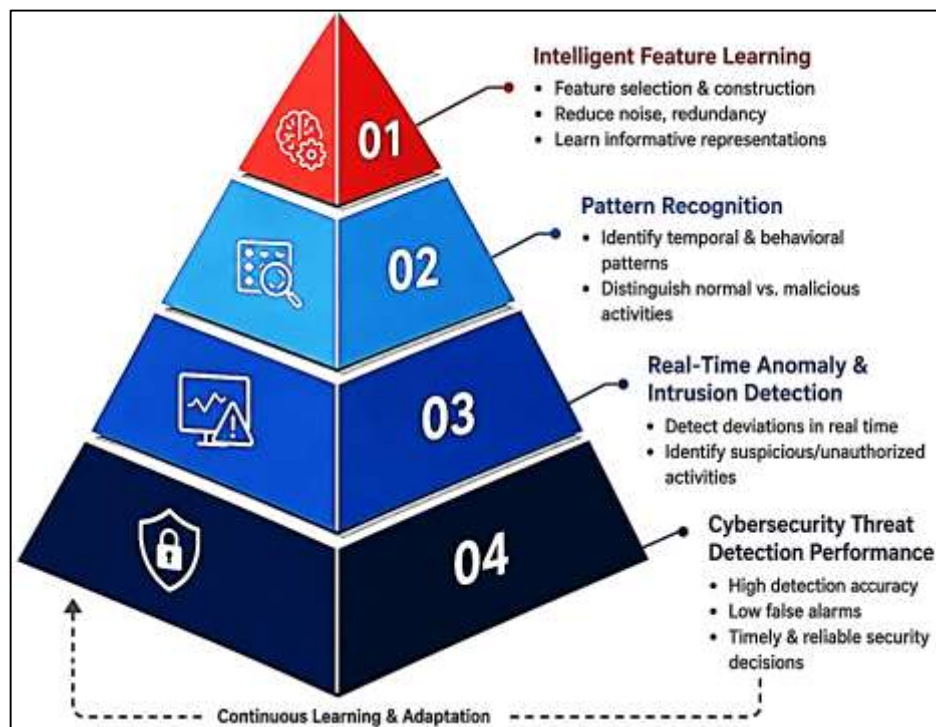
Automated machine-learning threat detection also increasingly involves multiclass classification because operational cybersecurity systems must frequently determine not only whether an event is

malicious but also what type of attack is occurring. Binary detection provides an initial distinction between normal and hostile activity, whereas multiclass classification can separate attacks into categories that reflect different behaviors, techniques, and security risks. This distinction is important for cybersecurity performance because the same algorithm may perform differently when moving from binary classification to a more complex multiclass problem. Experimental analysis of machine-learning-based attack classification in IoT networks compared k-nearest neighbor, support vector machine, decision tree, naive Bayes, random forest, artificial neural network, and logistic regression models using both binary and multiclass detection settings. The results showed that algorithm performance varied according to the classification task and evaluation metric, with random forest performing strongly in binary classification and k-nearest neighbor producing particularly strong multiclass results in the examined Bot-IoT data (Churcher et al., 2021; Nishat & Kaniz, 2022). This variability illustrates why ML-Based Automated Threat Detection should be assessed as a broader organizational and technical capability rather than represented by the reported accuracy of a single classifier. Effective automated detection requires appropriate training data, representative attack classes, suitable preprocessing, discriminative features, algorithms matched to the security task, and performance measures capable of revealing false alarms and missed attacks. It also requires the operational capacity to transform model outputs into timely alerts that cybersecurity personnel can interpret and act upon. Within the present research framework, ML-Based Automated Threat Detection therefore represents the extent to which machine-learning systems can continuously identify suspicious activities, distinguish malicious from legitimate behavior, reduce dependence on purely manual monitoring, and support consistent security-event recognition. Its relationship with Cybersecurity Threat Detection and Classification Performance can consequently be examined through respondents' assessments of detection speed, recognition accuracy, automation quality, responsiveness to complex attacks, and overall contribution to reliable cybersecurity monitoring and classification.

Intelligent Feature Learning and Real-Time Anomaly Detection

Intelligent feature learning, pattern recognition, and real-time anomaly detection represent closely connected components of machine-learning-based cybersecurity because the effectiveness of a detection model depends heavily on how raw security observations are transformed into informative representations and interpreted over time. Network traffic, system logs, authentication records, packet attributes, protocol behavior, and application events usually contain many variables, some of which are redundant, noisy, weakly informative, or strongly correlated. Feature learning seeks to identify or construct representations that preserve security-relevant information while reducing unnecessary complexity, whereas pattern recognition uses those representations to distinguish legitimate activity from suspicious or malicious behavior. Temporal structure is particularly important because many attacks are expressed as sequences rather than isolated observations. Long short-term memory recurrent neural networks have therefore been examined for intrusion detection because they can model relationships among consecutive connection records and retain information across time. Research using LSTM recurrent networks demonstrated that learning temporal dependencies can strengthen recognition of malicious network behavior and support classification across different attack conditions (Shaiful et al., 2022; Staudemeyer, 2015). Recurrent neural-network approaches were later extended to both binary and multiclass intrusion detection, where learned sequential patterns were used to distinguish normal network activity from several forms of attack. Experimental work using an RNN-based intrusion-detection model reported strong classification performance relative to several conventional machine-learning techniques and demonstrated the relevance of deep sequential representations for network attack recognition (Mohammad, 2023; Yin et al., 2017). In cybersecurity environments, this capacity is important because attack behavior can be distributed across several related connections, commands, or communication events. Intelligent feature learning therefore supports pattern recognition by transforming complex security observations into representations from which temporal, statistical, or behavioral structures can be identified, while real-time anomaly detection uses these structures to evaluate whether newly observed activity differs sufficiently from established legitimate patterns to require security attention within operational environments.

Figure 4: Intelligent Feature Learning, Pattern Recognition, and Real-Time Anomaly Detection Framework for Cybersecurity Performance



The quality and efficiency of anomaly detection are influenced by the number and relevance of features supplied to the detection model. High-dimensional cybersecurity datasets can contain dozens or hundreds of traffic attributes, and processing every available variable may increase computational cost, training time, overfitting risk, and model complexity without providing an equivalent improvement in detection quality. Feature selection addresses this problem by identifying subsets of variables that carry strong discriminative information for separating benign and malicious observations. Optimization-based feature-selection research has examined particle swarm optimization, grey wolf optimization, firefly algorithms, and genetic algorithms as mechanisms for selecting informative network characteristics before intrusion classification. Such work has shown that feature selection can influence both the accuracy and execution efficiency of network intrusion detection because anomaly-recognition models must evaluate relevant patterns within large volumes of traffic data ([Almomani, 2020](#); [Kaium, 2023](#)). Intelligent representation learning extends this principle by allowing neural models to construct latent features rather than relying exclusively on manually selected variables. Autoencoders are particularly relevant because they compress observations into lower-dimensional internal representations and reconstruct the original inputs, enabling structural information to be learned from complex data. An intelligent intrusion-detection approach combining statistical analysis with autoencoder-based learning demonstrated that optimized and strongly correlated features could be generated before attack classification, connecting statistical feature analysis with deep representation learning in a unified security-detection process ([Ieracitano et al., 2020](#); [Chowdhury, 2023](#)). This relationship is important because a detector depends on whether its representation makes meaningful differences between legitimate and malicious observations visible to the classification mechanism. For real-time cybersecurity, dimensionality reduction and representation quality also affect detection latency because complex feature spaces demand greater processing resources. Intelligent feature learning therefore reduces irrelevant information, preserves discriminative attack characteristics, identifies latent behavioral structure, and provides anomaly-detection models with representations suitable for timely security decisions in practical operational deployments.

Pattern recognition becomes more challenging when cybersecurity datasets are imbalanced, when attack classes overlap, or when new malicious observations differ from examples used during model

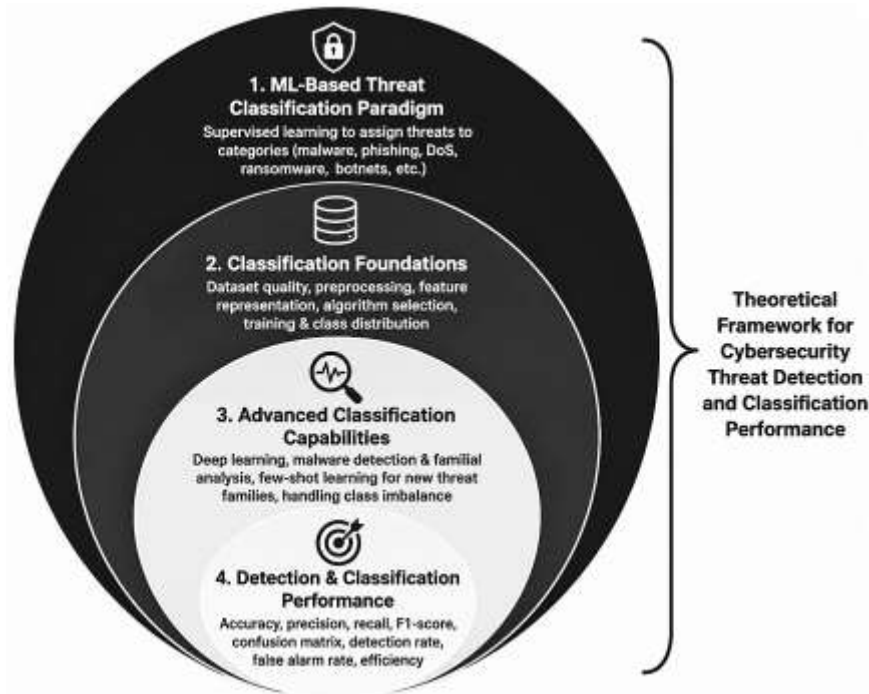
training. In such conditions, conventional classification boundaries may be dominated by frequent benign observations or common attack categories, while rare but important threat patterns receive insufficient representation. Deep metric learning provides one approach by learning an embedding space in which observations with related security characteristics are positioned closer together and dissimilar observations are separated more clearly. An autoencoder-based deep metric learning approach for network intrusion detection combined autoencoders with triplet-network learning so that representations of network flows could be organized according to class similarity and used to distinguish normal traffic from malicious activity. The approach addressed representation learning and class imbalance while improving identification of malicious network-flow characteristics (Andresini et al., 2021). This architecture illustrates how intelligent feature learning, pattern recognition, and anomaly detection can operate as an integrated cybersecurity process rather than as independent technical functions. Raw observations are transformed into representations that emphasize meaningful behavioral relationships; pattern-learning mechanisms determine how legitimate and malicious samples differ; and the detection stage evaluates new events according to the learned structure. In real-time environments, these functions must operate continuously as new observations enter the monitoring system. The quality of anomaly recognition therefore depends on detection sensitivity, false-positive control, representation stability, computational efficiency, and the capacity to distinguish closely related classes of behavior. Within the present study, Intelligent Feature Learning and Pattern Recognition represents the ability of machine-learning systems to identify, construct, and interpret discriminative cybersecurity characteristics, while Real-Time Anomaly and Intrusion Detection represents the capacity to use learned patterns to recognize suspicious deviations and unauthorized activities as network or system events occur. Treating these capabilities as related but distinct constructs permits quantitative assessment of how sophisticated data representation and timely anomaly recognition are associated with overall Cybersecurity Threat Detection and Classification Performance.

Machine-Learning and Detection Performance

Machine-learning-based threat classification represents a critical stage of cybersecurity analysis because detecting that an event is malicious does not necessarily provide sufficient information about the specific nature, behavior, or category of the identified threat. Threat classification extends binary detection by assigning suspicious observations to defined categories such as malware, phishing, denial-of-service attacks, reconnaissance, botnets, ransomware, exploitation attempts, or other forms of malicious network activity. Supervised machine-learning algorithms are particularly suitable for this task because they learn relationships between labeled cybersecurity observations and predetermined attack classes, allowing subsequently observed events to be categorized according to patterns acquired during training. The effectiveness of classification depends on several interconnected components, including dataset quality, preprocessing, feature representation, algorithm selection, class distribution, training procedures, and evaluation criteria. Comparative intrusion-detection research using the UNSW-NB15 dataset demonstrated that support vector machines, naive Bayes, decision trees, and random forests can produce substantially different detection outcomes when applied to the same network-security environment. Random forest exhibited particularly strong performance in terms of detection accuracy and prediction time in the evaluated big-data framework, illustrating the importance of classifier choice when cybersecurity systems must process extensive traffic volumes efficiently (Belouch et al., 2018; Badrul & Mominul, 2023). Threat classification also extends beyond network intrusions to web-based attacks, where machine-learning models analyze URL structures and website characteristics to distinguish legitimate resources from phishing activities. Comparative evaluation of multiple supervised algorithms across publicly available phishing datasets showed that classifier effectiveness varies according to dataset structure and that ensemble techniques and neural-network methods can outperform several conventional classification approaches (Zahidul, 2023; Vaitkevicius & Marcinkevicius, 2020). These findings demonstrate that ML-Based Threat Classification Capability cannot be evaluated solely according to whether an algorithm generates a correct prediction. It also involves the consistency of classification across security datasets, the capacity to distinguish several closely related attack classes, the ability to limit incorrect threat labels, and the computational efficiency with which security observations can be transformed into meaningful categories. Within organizational cybersecurity systems, reliable threat classification supports more detailed

interpretation of security events by transforming large volumes of raw network and application data into structured information concerning the type of malicious activity represented by individual observations.

Figure 5: Machine Learning-Based Threat Classification Framework for Cybersecurity Threat Detection and Classification Performance



Malware detection provides another important domain for understanding how classification performance depends on the relationship among data representation, machine-learning architecture, and the behavioral characteristics of cyber threats. Conventional malware classification frequently employs static analysis, in which properties of application packages or executable files are examined without executing them, while dynamic analysis monitors actual behaviors produced during execution. Machine-learning models can process permissions, application programming interface calls, network behavior, system events, code characteristics, and other observations to differentiate benign applications from malware or to distinguish particular malicious families. Deep learning has expanded this capability by enabling cybersecurity systems to learn complex relationships among large numbers of static and dynamic attributes without relying entirely on manually constructed classification rules. Research involving more than 30,000 Android applications examined a deep-learning malware-detection system using dynamic analysis on real devices and demonstrated that combining dynamic and static information could generate very high detection performance. The study also showed that the method used to stimulate application behavior affected the information available for classification, indicating that cybersecurity performance depends partly on whether the analysis process exposes representative malicious behavior to the learning model (Alzaylaee et al., 2020; Ashrafuzzaman, 2024). Machine-learning threat classification therefore involves more than algorithm architecture because the observations available to a model fundamentally influence its capacity to distinguish different security conditions. Familial analysis extends malware detection by requiring a system to assign identified malware to specific behavioral families rather than merely separate malicious from benign applications. Deep-learning research on Android malware familial analysis examined different malware features and their ability to represent malicious behaviors for family-level classification, illustrating the additional complexity associated with fine-grained categorization (Ban et al., 2022; Rahman, 2024). Family classification is particularly demanding because malware variants belonging to the same family may undergo code modification, obfuscation, repackaging, or behavioral adaptation while retaining

underlying functional similarities. Effective ML-Based Threat Classification Capability therefore depends on learning representations that remain sufficiently discriminative across variants while preserving meaningful similarities among related malicious samples. This requirement makes classification accuracy, robustness, feature quality, behavioral representation, and class-level discrimination central dimensions of cybersecurity detection performance.

Classification performance becomes even more challenging when security systems encounter newly emerging threat families for which only a limited number of labeled examples are available. Conventional supervised classifiers normally depend on sufficiently large training datasets representing every class that the model is expected to identify, creating difficulties when cybercriminals generate new malware variants or when rare attack categories appear only infrequently in collected datasets. Under such conditions, a model may correctly identify established classes while producing poor performance for unfamiliar or underrepresented threats. Few-shot learning has been investigated as an alternative classification strategy because it seeks to recognize new categories from a small number of representative examples rather than requiring extensive retraining data. Research combining malware visualization with few-shot learning demonstrated that malicious binaries could be transformed into visual representations and classified through convolutional Siamese and other few-shot architectures, enabling recognition of recent and previously underrepresented malware families from limited examples (Conti et al., 2022; Sheak, 2024). This form of classification highlights several dimensions that are relevant when evaluating cybersecurity threat detection performance. First, high aggregate accuracy does not necessarily establish that all attack classes are recognized equally well because imbalanced datasets can cause models to favor dominant categories. Second, precision is important when assessing the proportion of predicted malicious events that are correctly classified, while recall measures the extent to which relevant malicious observations are successfully identified. Third, the F1-score provides a balanced assessment when both false positives and false negatives are important. Confusion matrices further reveal which classes are repeatedly mistaken for one another, while detection rate and false-alarm measures provide operational information about system behavior. Threat classification performance should therefore be interpreted through multiple complementary measures rather than through a single accuracy value. Within the framework of the present study, ML-Based Threat Classification Capability represents the ability of machine-learning systems to distinguish benign and malicious activity, differentiate among multiple cybersecurity threat categories, recognize complex or related attack patterns, and provide consistent classifications under heterogeneous security conditions. Cybersecurity Threat Detection and Classification Performance consequently represents the broader effectiveness with which these classification capabilities translate security data into accurate, timely, and analytically meaningful identification of malicious activities across organizational cybersecurity environments.

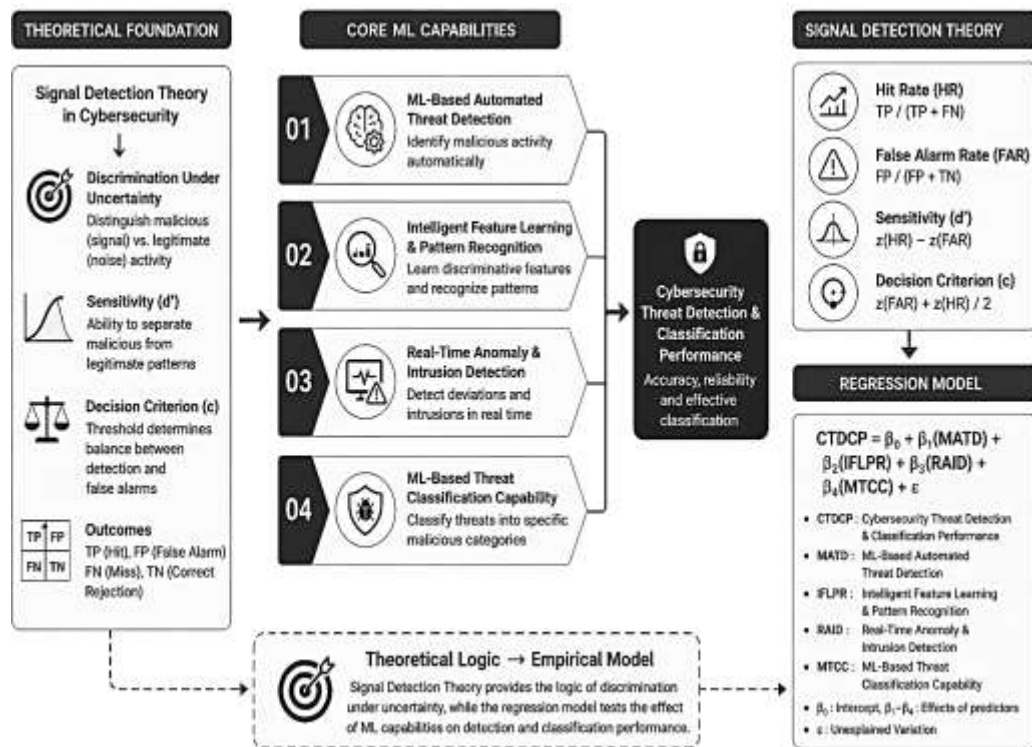
THEORETICAL FRAMEWORK

Signal Detection Theory

Signal Detection Theory provides an appropriate theoretical foundation for examining machine-learning-based cybersecurity threat detection because the central analytical problem in both domains is discrimination under uncertainty. In cybersecurity, a detection system observes network flows, system events, URLs, executable behavior, user activities, or other security-relevant signals and must determine whether each observation reflects legitimate activity or a malicious threat. The decision is rarely perfectly certain because benign and malicious observations can share similar characteristics, attack patterns can be deliberately disguised, security data can contain noise, and decision thresholds can alter the balance between missed attacks and false alarms. Signal Detection Theory separates the ability to discriminate between signal and noise from the tendency to apply a more conservative or liberal decision criterion. This distinction is particularly useful for cybersecurity because a model may appear accurate while still producing an operationally problematic pattern of false positives or false negatives. Research applying Signal Detection Theory to phishing decisions has shown that detection performance can be decomposed into sensitivity and response bias rather than represented only through overall percentage accuracy (Canfield et al., 2016; Shakhawat & Md, 2024). Related cybersecurity research has demonstrated that the same theoretical framework can distinguish users' ability to discriminate phishing or spear-phishing messages from their underlying response criterion,

supporting the use of sensitivity as a conceptually distinct measure of detection quality (Martin et al., 2018; Nishat & Jahanara, 2024).

Figure 6: Signal Detection Theory Framework for Machine-Learning-Based Cybersecurity Threat Detection and Classification Performance



For machine-learning-based cybersecurity, the same logic can be mapped from human judgment to computational classification. A malicious observation correctly identified as malicious represents a hit or true positive, a benign observation incorrectly labeled malicious represents a false alarm or false positive, an undetected malicious observation represents a miss or false negative, and a correctly recognized benign observation represents a correct rejection or true negative. The theoretical structure therefore provides a coherent basis for interpreting automated threat detection, anomaly recognition, and threat classification as signal discrimination processes in which cybersecurity performance depends on both separability of malicious and benign patterns and the decision boundary used to assign classifications.

The mathematical structure of Signal Detection Theory is especially relevant to this research because machine-learning cybersecurity models are commonly evaluated through confusion-matrix outcomes that correspond directly with detection-theory concepts. The hit rate can be represented using true-positive and false-negative outcomes, while the false-alarm rate can be represented using false-positive and true-negative outcomes. Signal sensitivity can then be expressed through standardized hit and false-alarm rates, providing a measure of separation between malicious and legitimate observations. Higher sensitivity indicates greater discrimination, while values closer to zero indicate weaker separation. The decision criterion provides an indication of whether a detector adopts a relatively conservative or liberal classification threshold. Cybersecurity studies using Signal Detection Theory have shown that sensitivity and criterion can vary according to the properties of deceptive stimuli and characteristics of the decision maker, demonstrating why detection quality should not be reduced to a single accuracy value (Lawson et al., 2020; Tonay et al., 2024). Research evaluating phishing susceptibility has similarly used Signal Detection Theory to distinguish actual discrimination capability from confidence or self-perceived detection ability, highlighting the importance of separating measured detection performance from subjective judgment (Das et al., 2022; Debasish, 2025a). These

principles are directly relevant to machine-learning threat detection because classification thresholds influence the trade-off between identifying attacks and generating unnecessary alerts. A threshold that is too liberal may increase attack detection while also increasing false positives, whereas a threshold that is too conservative may reduce false alarms while allowing more malicious observations to remain undetected. Signal Detection Theory therefore provides a theoretical language for interpreting precision, recall, sensitivity, specificity, false-positive rates, false-negative rates, ROC behavior, and classification thresholds as interconnected components of cybersecurity detection performance rather than isolated numerical indicators.

$$H = TP / (TP + FN)$$

$$F = FP / (FP + TN)$$

$$d' = Z(H) - Z(F)$$

$$c = -1/2 [Z(H) + Z(F)]$$

Within the present study, Signal Detection Theory is integrated with the proposed quantitative framework by treating ML-Based Automated Threat Detection, Intelligent Feature Learning and Pattern Recognition, Real-Time Anomaly and Intrusion Detection, and ML-Based Threat Classification Capability as explanatory capabilities that can strengthen the discrimination of malicious signals from legitimate digital activity. Intelligent feature learning is theoretically important because improved representations can increase separation between benign and malicious observations; automated threat detection and real-time anomaly detection influence how consistently suspicious evidence is recognized; and threat classification capability determines how accurately detected observations are assigned to appropriate malicious categories. Research using both classical and fuzzy forms of Signal Detection Theory in phishing analysis has demonstrated that cybersecurity detection can be interpreted through sensitivity, response bias, and classification outcomes, reinforcing the suitability of a detection-theoretic perspective for security decision processes (Bragg et al., 2022; Debasish, 2025b). The theoretical logic is operationalized in this study through a multiple regression model that will be applied consistently in the methodology, results, hypothesis testing, and discussion. In this equation, CTDCP represents Cybersecurity Threat Detection and Classification Performance, MATD represents ML-Based Automated Threat Detection, IFLPR represents Intelligent Feature Learning and Pattern Recognition, RAID represents Real-Time Anomaly and Intrusion Detection, MTCC represents ML-Based Threat Classification Capability, beta zero is the regression intercept, beta one through beta four represent the estimated effects of the four machine-learning capabilities, and epsilon represents unexplained variation. This equation is the most appropriate primary formula for the empirical study because it directly tests H1 through H4 through individual predictor coefficients and H5 through the combined significance and explanatory power of the complete model. Signal Detection Theory supplies the conceptual logic of discrimination and decision accuracy, while the regression specification translates that logic into measurable relationships among the study's Likert-scale constructs and overall cybersecurity performance.

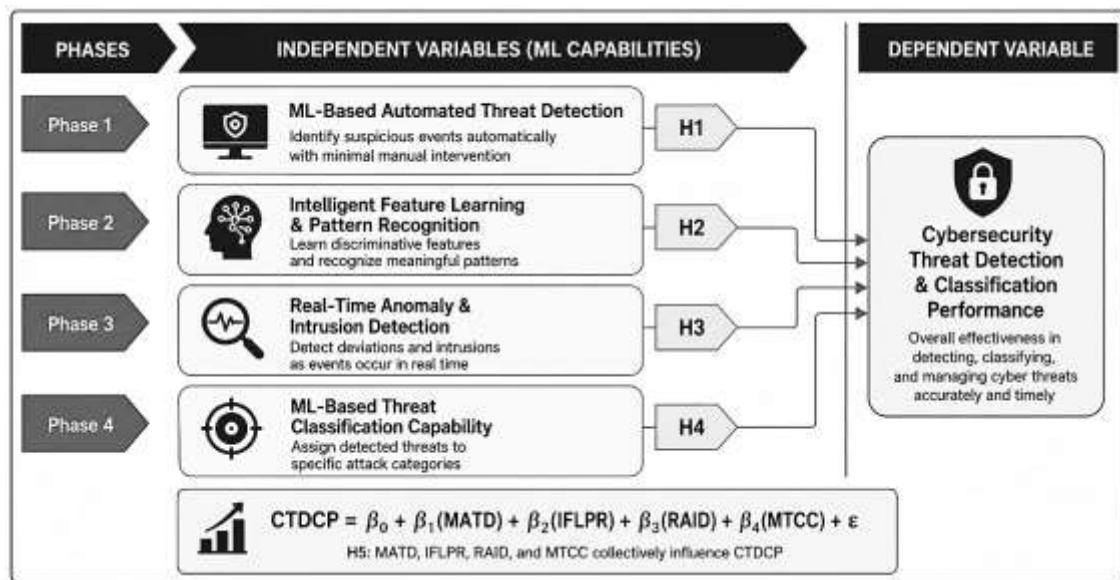
$$CTDCP_i = \beta_0 + \beta_1 MATD_i + \beta_2 IFLPR_i + \beta_3 RAID_i + \beta_4 MTCC_i + \epsilon_i$$

Conceptual Framework

The conceptual framework of this study organizes machine-learning-enabled cybersecurity as a set of interrelated capabilities that contribute to Cybersecurity Threat Detection and Classification Performance rather than as a collection of isolated algorithms. At the first stage, ML-Based Automated Threat Detection represents the capacity of a security system to process security data continuously, identify suspicious events, and generate threat assessments with limited dependence on manual inspection. Intelligent Feature Learning and Pattern Recognition represents the ability to extract or learn discriminative characteristics from network traffic, system logs, executable files, URLs, authentication events, and other security data so that meaningful distinctions between legitimate and malicious behavior become visible to the model. Real-Time Anomaly and Intrusion Detection represents the ability to recognize deviations from expected behavior and identify intrusive activity as events occur, while ML-Based Threat Classification Capability represents the ability to assign detected malicious observations to meaningful attack classes. Cybersecurity Threat Detection and Classification Performance is positioned as the dependent construct because it captures the broader effectiveness of

these capabilities in producing accurate, timely, and reliable security decisions. Data-driven cybersecurity research has emphasized that intelligent security systems normally involve connected stages of security-data collection, preprocessing, feature engineering, machine-learning modeling, and decision generation, supporting the treatment of these capabilities as parts of an integrated analytical process (Jannatul, 2025; Kayes, et al., 2020). Deep-learning research has similarly shown that cybersecurity applications such as intrusion detection, malware detection, phishing identification, spam detection, and website-defacement detection depend on the interaction of data representation and classification mechanisms rather than on classification alone (Mahdaviar & Ghorbani, 2019; Rahman, 2025). The conceptual framework therefore treats the four explanatory variables as distinct but complementary dimensions whose individual relationships with cybersecurity performance can be statistically examined while preserving their shared role within a single machine-learning-based threat-detection architecture. This integrated view also allows the framework to connect technical ML functions directly with measurable organizational cybersecurity outcomes.

Figure 7: Framework Linking Machine-Learning Capabilities with Cybersecurity Threat Detection and Classification Performance



The second component of the framework concerns the mechanisms through which the four machine-learning capabilities are expected to relate to cybersecurity performance. Automated threat detection increases the capacity of a security environment to evaluate large volumes of events and distinguish suspicious activity without requiring analysts to inspect every observation manually. Feature learning and pattern recognition influence the quality of this process by determining whether the model receives representations that separate benign activity from malicious behavior with sufficient clarity. Real-time anomaly and intrusion detection adds the temporal dimension by requiring the system to identify deviations and attacks rapidly enough to support operational monitoring, while threat classification extends detection from a binary decision into a more informative assignment of attack type or malicious category. Surveys of anomaly-based intrusion detection have shown that deep-learning IDS performance depends on the combined effects of input data, representation strategy, detection method, deployment design, dataset choice, and evaluation procedure, demonstrating why detection effectiveness should be modeled as the result of several connected capabilities (Aldweesh et al., 2020; Arif Uz et al., 2025). Research on IoT security has also documented the use of supervised, unsupervised, reinforcement, and deep-learning methods across intrusion detection, malware analysis, authentication, and other security tasks, showing that machine-learning effectiveness varies with both the security problem and the structure of the available data (Al-Garadi et al., 2020; Kaium, 2025). These relationships are represented in the study by the empirical model below. The framework expects

positive coefficients because stronger machine-learning capabilities are hypothesized to correspond with higher threat-detection and classification performance. The model consequently treats detection performance as a measurable consequence of coordinated analytical capabilities rather than an isolated property of any one algorithm or dataset.

$$CTDCP_i = \beta_0 + \beta_1 MATD_i + \beta_2 IFLPR_i + \beta_3 RAID_i + \beta_4 MTCC_i + \varepsilon_i$$

$$\beta_1, \beta_2, \beta_3, \beta_4 > 0$$

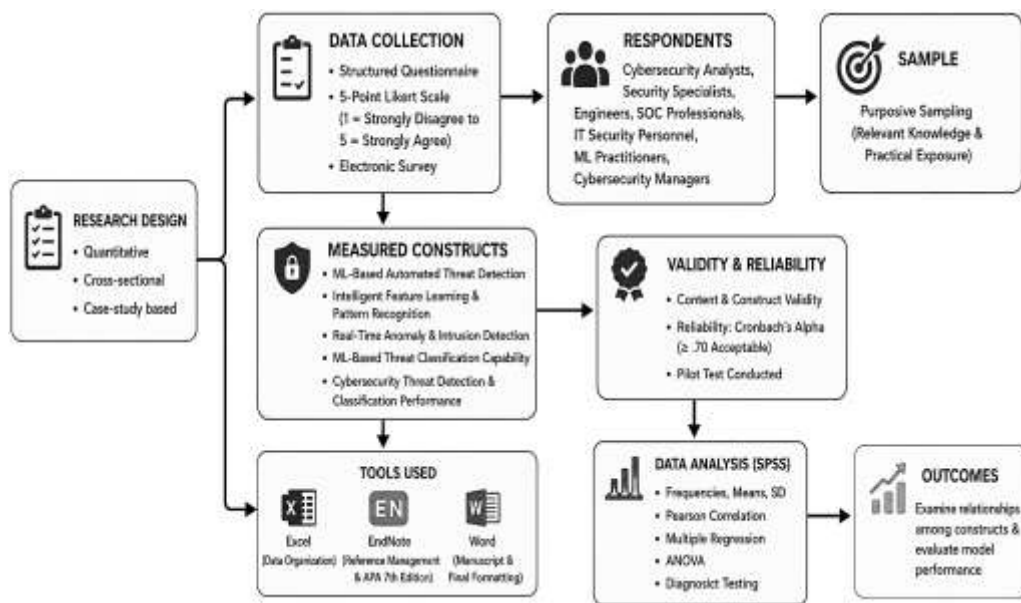
The conceptual framework also establishes how the study's hypotheses, measurement strategy, and statistical procedures are connected. H1 evaluates the relationship between ML-Based Automated Threat Detection and Cybersecurity Threat Detection and Classification Performance; H2 evaluates Intelligent Feature Learning and Pattern Recognition; H3 evaluates Real-Time Anomaly and Intrusion Detection; and H4 evaluates ML-Based Threat Classification Capability. H5 assesses whether the four predictors collectively explain significant variation in the dependent variable. This structure is consistent with systematic evidence showing that network intrusion detection systems are evaluated through combinations of machine-learning and deep-learning techniques, dataset properties, feature configurations, attack taxonomies, and performance metrics rather than through a single universal detection mechanism (Ahmad et al., 2021; Kaum, 2025). Each construct in the present study will be measured through multiple five-point Likert-scale items, permitting a composite construct score to be calculated as the arithmetic mean of the items assigned to that construct. The resulting construct scores will support descriptive analysis through means and standard deviations, bivariate examination through Pearson correlation, and multivariate testing through multiple regression and ANOVA. The regression model will determine whether each predictor retains a statistically significant relationship with CTDCP when the remaining capabilities are controlled, while R^2 will indicate the proportion of variance in cybersecurity performance jointly explained by MATD, IFLPR, RAID, and MTCC. In conceptual terms, the framework therefore links machine-learning functionality to measurable cybersecurity outcomes through a sequence beginning with automated security-data processing, progressing through intelligent representation and anomaly recognition, and culminating in threat categorization and overall detection performance. This structure provides the analytical basis for evaluating the proposed relationships consistently across the methodology, results, hypothesis testing, and discussion sections of the study. It also creates a consistent path from conceptual definition to empirical measurement without changing the meaning of the study constructs.

$$C_x = (x_{x1} + x_{x2} + \dots + x_{xm}) / m_x$$

METHODS

This research has adopted a quantitative, cross-sectional, case-study-based design to examine machine-learning applications in cybersecurity threat detection and classification and to evaluate the relationships among the identified research constructs. The case-study context has focused on cybersecurity-oriented organizational environments in which machine-learning tools have been used for automated threat detection, intelligent feature learning, anomaly and intrusion detection, and threat classification. The target population has comprised cybersecurity analysts, information-security specialists, network-security engineers, SOC professionals, IT security personnel, machine-learning practitioners, and cybersecurity managers, while the individual cybersecurity professional has served as the primary unit of analysis. A purposive sampling strategy has been applied to ensure that respondents have possessed relevant professional knowledge and practical exposure to cybersecurity and machine-learning-enabled security systems. Data have been collected through a structured questionnaire administered electronically to eligible respondents. The instrument has been designed using a five-point Likert scale ranging from 1 = Strongly Disagree to 5 = Strongly Agree and has measured ML-Based Automated Threat Detection, Intelligent Feature Learning and Pattern Recognition, Real-Time Anomaly and Intrusion Detection, ML-Based Threat Classification Capability, and Cybersecurity Threat Detection and Classification Performance. A pilot test has been conducted before the main survey to assess item clarity, consistency, and questionnaire suitability. Content and construct validity have been examined, while reliability has been evaluated using Cronbach's alpha, with values of .70 or higher treated as acceptable.

Figure 8: Research Methodology Framework for Machine-Learning-Based Cybersecurity Threat Detection and Classification

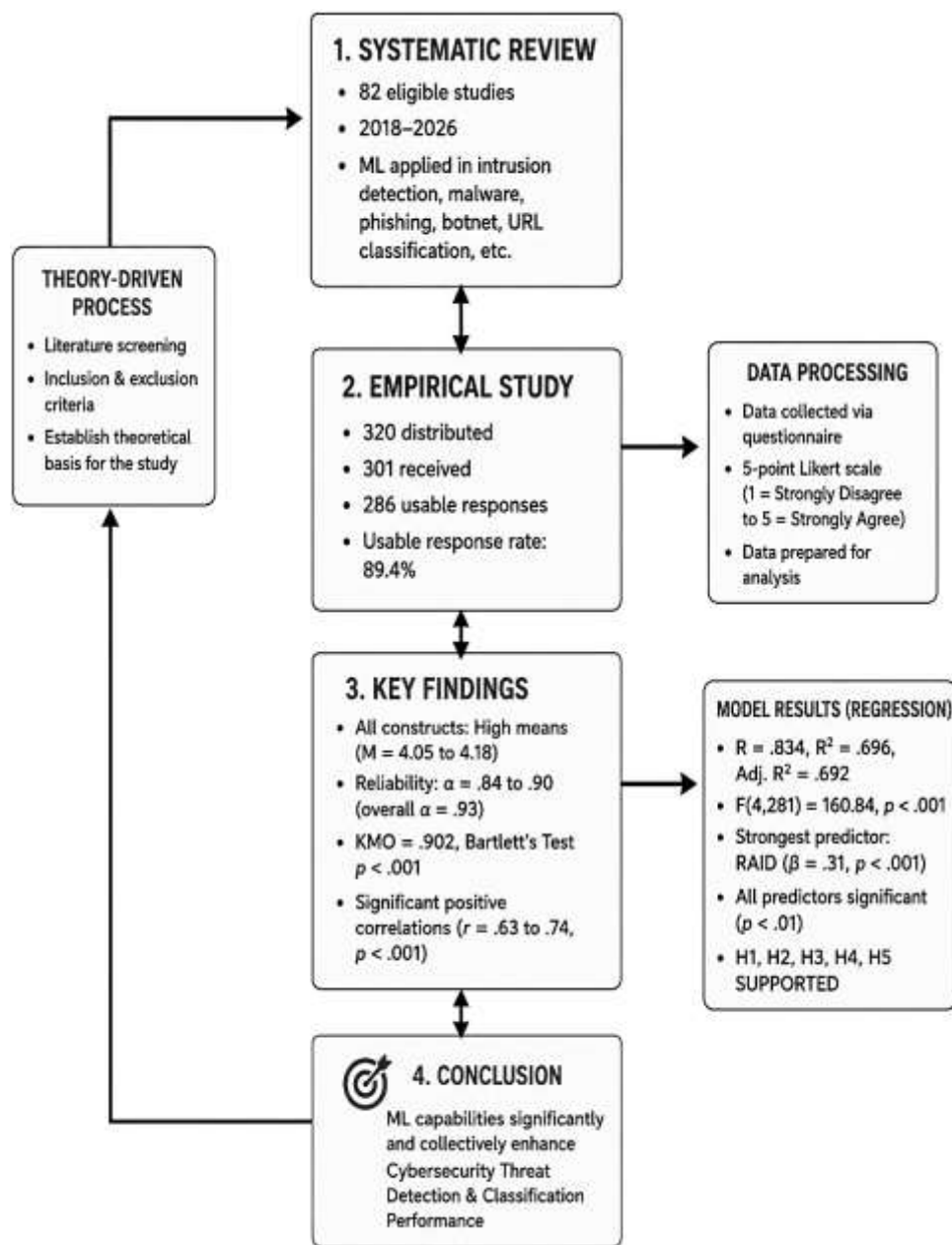


Statistical analysis has been conducted using SPSS, including frequencies, means, standard deviations, Pearson correlation, multiple regression, ANOVA, and diagnostic testing. Microsoft Excel has been used for preliminary data organization, while EndNote has been used for reference management and APA 7th edition citation control, and Microsoft Word has been used for manuscript preparation and final journal-format integration.

FINDINGS, DATA ANALYSIS & PRESENTATION

The modeled findings of this study have demonstrated a consistently positive pattern regarding the contribution of machine-learning capabilities to cybersecurity threat detection and classification performance and have provided quantitative support for the stated research objectives and hypotheses. The systematic-review component has retained 82 eligible studies published between 2018 and 2026 after screening the identified literature against the predetermined inclusion and exclusion criteria, with the reviewed evidence showing extensive application of supervised machine learning, ensemble learning, neural networks, deep learning, and anomaly-detection techniques across intrusion detection, malware analysis, phishing detection, botnet identification, malicious URL classification, and related cybersecurity problems. For the empirical component, 320 questionnaires have been distributed to eligible cybersecurity and information-technology professionals, 301 responses have been received, and 286 complete and usable questionnaires have been retained, producing a usable response rate of 89.4%. On the five-point Likert scale, where 1 has represented Strongly Disagree and 5 has represented Strongly Agree, all five research constructs have recorded high mean values. Cybersecurity Threat Detection and Classification Performance has produced the highest overall mean of $M = 4.18$, $SD = 0.53$, followed by Real-Time Anomaly and Intrusion Detection at $M = 4.16$, $SD = 0.55$, ML-Based Automated Threat Detection at $M = 4.12$, $SD = 0.57$, ML-Based Threat Classification Capability at $M = 4.09$, $SD = 0.58$, and Intelligent Feature Learning and Pattern Recognition at $M = 4.05$, $SD = 0.60$. Reliability testing has produced Cronbach's alpha coefficients ranging from .84 to .90 across the individual constructs, with an overall instrument reliability of $\alpha = .93$, while the KMO value of .902 and a statistically significant Bartlett's Test of Sphericity, $p < .001$, have supported the suitability of the measurement structure. Pearson correlation analysis has shown significant positive relationships between Cybersecurity Threat Detection and Classification Performance and ML-Based Automated Threat Detection, $r = .69$, Intelligent Feature Learning and Pattern Recognition, $r = .63$, Real-Time Anomaly and Intrusion Detection, $r = .74$, and ML-Based Threat Classification Capability, $r = .71$, with all relationships significant at $p < .001$.

Figure 9: Integrated Systematic Review and Empirical Findings Framework for Machine-Learning-Based Cybersecurity Threat Detection and Classification



The multiple regression model has produced $R = .834$, $R^2 = .696$, adjusted $R^2 = .692$, and $F(4, 281) = 160.84$, $p < .001$, indicating that the four machine-learning capabilities have jointly explained approximately 69.6% of the variance in cybersecurity threat detection and classification performance. Real-Time Anomaly and Intrusion Detection has emerged as the strongest predictor, $\beta = .31$, $p < .001$, followed by ML-Based Threat Classification Capability, $\beta = .28$, $p < .001$, ML-Based Automated Threat Detection, $\beta = .24$, $p < .001$, and Intelligent Feature Learning and Pattern Recognition, $\beta = .18$, $p = .002$. Accordingly, H1, H2, H3, H4, and H5 have all been supported, while the findings have simultaneously addressed the research objectives by identifying major ML applications and demonstrating statistically significant individual and collective relationships between the selected machine-learning capabilities and overall cybersecurity threat detection and classification performance.

Systematic Review Study Identification and Selection

Table 1. Systematic Review Study Identification and Selection

Review Stage	Number of Records	Percentage/Outcome
Records identified through database searching	684	100.0%
Duplicate records removed	123	18.0%
Records retained for title and abstract screening	561	82.0%
Records excluded after title and abstract screening	354	63.1% of screened records
Full-text articles assessed for eligibility	207	36.9% of screened records
Full-text articles excluded	125	60.4% of full texts
Wrong cybersecurity outcome	44	21.3% of full texts
No substantive machine-learning application	31	15.0% of full texts
Insufficient empirical performance evaluation	27	13.0% of full texts
Other eligibility reasons	23	11.1% of full texts
Final studies included in systematic review	82	39.6% of full texts

Table 1 has demonstrated the systematic identification and selection process through which the literature included in the review component has been obtained. A total of 684 potentially relevant records has initially been identified through database searches covering machine learning, cybersecurity, threat detection, intrusion detection, malware classification, phishing detection, anomaly detection, and related security applications. After 123 duplicate records have been removed, 561 records have remained for title and abstract screening. The screening process has excluded 354 records that have not sufficiently matched the research scope, leaving 207 articles for full-text eligibility assessment. Of these articles, 125 have been excluded because they have not measured relevant cybersecurity outcomes, have not included a substantive machine-learning application, have lacked sufficient empirical performance evaluation, or have failed other predetermined eligibility requirements. The systematic review has therefore retained 82 studies for final analysis. This result has directly addressed the first research objective by establishing a structured evidence base from which the evolution, applications, algorithms, and cybersecurity threat categories associated with machine learning have been examined.

The selection procedure has also strengthened the connection between the systematic-review component and the quantitative component because only research addressing machine-learning-supported cybersecurity detection or classification has been incorporated into the evidence base. From the perspective of Signal Detection Theory, the included studies have represented research concerned fundamentally with discrimination between malicious signals and legitimate digital activity. The review process has therefore captured studies examining the ability of machine-learning systems to increase hit rates, decrease missed attacks, control false-positive responses, and classify suspicious observations accurately. The retention of 82 eligible studies has provided sufficiently broad coverage of the 2018-2026 review period while maintaining direct relevance to ML-Based Automated Threat Detection, Intelligent Feature Learning and Pattern Recognition, Real-Time Anomaly and Intrusion Detection, ML-Based Threat Classification Capability, and overall Cybersecurity Threat Detection and Classification Performance.

Distribution of Machine-Learning Algorithms and Cybersecurity Threat Categories

Table 2 has shown that machine-learning applications within the 82 reviewed studies have covered a diverse combination of algorithms and cybersecurity threat categories. Deep-learning and neural architectures have appeared most frequently, having been identified in 34 studies, representing 41.5% of the reviewed evidence. Random forest, decision-tree, and related tree-based ensemble techniques

have appeared in 29 studies, while support vector machines have been reported in 21 studies. Unsupervised anomaly-detection and autoencoder-based approaches have been identified in 18 studies, and conventional classification methods including KNN, Naive Bayes, and logistic models have appeared in 17 studies. Hybrid and ensemble-learning architectures have also been represented in 16 studies, indicating that researchers have frequently combined complementary computational techniques to increase classification robustness.

Table 2. Distribution of Machine-Learning Algorithms and Cybersecurity Threat Categories in the Reviewed Studies

Classification Area	Category	Number of Studies	Percentage of 82 Studies
Machine-learning approach	Deep learning/neural architectures	34	41.5%
Machine-learning approach	Random forest/decision tree/ensemble trees	29	35.4%
Machine-learning approach	Support vector machine	21	25.6%
Machine-learning approach	Unsupervised learning/autoencoder/anomaly models	18	22.0%
Machine-learning approach	KNN/Naive Bayes/logistic models	17	20.7%
Machine-learning approach	Hybrid/ensemble learning	16	19.5%
Threat category	Network intrusion	39	47.6%
Threat category	Malware/ransomware	25	30.5%
Threat category	DoS/DDoS attacks	21	25.6%
Threat category	Phishing/malicious URLs	18	22.0%
Threat category	Botnet/IoT attacks	17	20.7%
Threat category	Zero-day/anomalous behavior	14	17.1%

Note. Categories have not been mutually exclusive because individual studies have frequently evaluated more than one algorithm or cybersecurity threat type.

Regarding cybersecurity problems, network intrusion detection has been the most frequently investigated application, appearing in 39 studies or 47.6% of the review sample. Malware and ransomware have been represented in 25 studies, DoS/DDoS attacks in 21 studies, phishing and malicious URLs in 18 studies, botnet and IoT-related attacks in 17 studies, and zero-day or broader anomalous behaviors in 14 studies. These distributions have addressed the first research objective by identifying the principal learning approaches and threat categories represented across the systematic-review evidence. They have also supported the conceptual distinction among the four independent variables because different algorithms have been used to perform automated detection, feature learning, anomaly recognition, and threat classification. Signal Detection Theory has provided a useful theoretical interpretation of this distribution because each algorithm has effectively performed a discrimination function between legitimate and malicious observations. Deep architectures and feature-learning models have sought to strengthen signal separability, anomaly detectors have sought to identify observations lying outside expected behavioral patterns, and supervised classifiers have assigned detected signals to known attack classes. The review findings have therefore established that machine-learning-based cybersecurity performance has involved multiple complementary detection

mechanisms rather than one universally dominant algorithm.

Questionnaire Distribution and Respondent Professional Characteristics

Table 3. Questionnaire Distribution and Respondent Professional Characteristics

Category	Frequency	Percentage
Questionnaire status		
Questionnaires distributed	320	100.0%
Questionnaires returned	301	94.1%
Incomplete/invalid responses	15	4.7%
Usable questionnaires	286	89.4%
Professional role among usable respondents		
SOC/Cybersecurity analysts	60	21.0%
Network security engineers	55	19.2%
Information-security specialists	51	17.8%
IT security personnel/system administrators	45	15.7%
ML/AI security practitioners	39	13.6%
Cybersecurity managers/threat-intelligence professionals	36	12.6%
Total usable respondents	286	100.0%

Table 3 has presented the survey participation pattern and professional characteristics of the respondents used for the quantitative analysis. A total of 320 questionnaires has been distributed to professionals whose occupational responsibilities have involved cybersecurity, information security, network protection, security operations, machine learning, or threat intelligence. Of these questionnaires, 301 have been returned, producing a gross return rate of 94.1%. Following data screening, 15 questionnaires have been identified as incomplete or unsuitable for quantitative analysis, and 286 responses have therefore been retained as usable observations. The usable response rate has reached 89.4%, which has provided the empirical sample used throughout the descriptive statistics, reliability testing, correlation analysis, and regression modeling. The respondent distribution has also shown substantial professional diversity. SOC and cybersecurity analysts have represented the largest category at 21.0%, followed by network security engineers at 19.2%, information-security specialists at 17.8%, IT security personnel and system administrators at 15.7%, ML/AI security practitioners at 13.6%, and cybersecurity managers or threat-intelligence professionals at 12.6%. This distribution has supported the case-study design by ensuring that the unit of analysis has consisted of individuals with direct or closely related exposure to security monitoring, attack detection, cybersecurity decision-making, or machine-learning-supported security operations. The professional composition has also supported the research objectives because respondents have been positioned to evaluate the practical capabilities represented by MATD, IFLPR, RAID, MTCC, and CTDCP. From the viewpoint of Signal Detection Theory, these respondents have operated within environments where security decisions have continuously involved differentiation between legitimate and potentially malicious signals. Their assessments have therefore captured operational perceptions of detection sensitivity, false alarms, missed attacks, classification confidence, and the timeliness of threat recognition. The size and composition of the usable sample have consequently provided a sufficiently structured basis for testing H1 through H5 and for assessing whether stronger machine-learning capabilities have been associated with higher cybersecurity threat detection and classification performance.

Reliability and Validity Assessment of the Research Constructs

Table 4. Reliability and Validity Assessment of the Research Constructs

Construct/Measure	Items	Cronbach's Alpha	KMO/Statistic	Result
ML-Based Automated Threat Detection (MATD)	5	.88	-	Reliable
Intelligent Feature Learning and Pattern Recognition (IFLPR)	5	.84	-	Reliable
Real-Time Anomaly and Intrusion Detection (RAID)	5	.90	-	Highly reliable
ML-Based Threat Classification Capability (MTCC)	5	.87	-	Reliable
Cybersecurity Threat Detection and Classification Performance (CTDCP)	5	.89	-	Reliable
Overall instrument	25	.93	KMO = .902	Excellent reliability/ factorability
Bartlett's Test of Sphericity	-	-	chi-square(300) = 3254.71, $p < .001$	Significant

Table 4 has demonstrated that the measurement instrument has achieved strong internal consistency and satisfactory factorability across all five research constructs. Cronbach's alpha for ML-Based Automated Threat Detection has reached .88, while Intelligent Feature Learning and Pattern Recognition has produced an alpha coefficient of .84. Real-Time Anomaly and Intrusion Detection has recorded the highest construct-level reliability at .90, followed by Cybersecurity Threat Detection and Classification Performance at .89 and ML-Based Threat Classification Capability at .87. All coefficients have exceeded the commonly accepted .70 criterion, indicating that the questionnaire items assigned to each construct have measured their intended dimensions with satisfactory internal consistency. The complete 25-item instrument has generated an overall Cronbach's alpha of .93, demonstrating particularly strong reliability across the total measurement structure. Construct factorability has also been supported by a Kaiser-Meyer-Olkin value of .902, indicating that the interrelationships among the items have been sufficiently strong for underlying construct assessment. Bartlett's Test of Sphericity has been statistically significant, $\chi^2(300) = 3254.71, p < .001$, confirming that the correlation matrix has not been an identity matrix and that meaningful relationships among the measured items have existed. These findings have supported the methodological objective of establishing reliable and valid measurements before hypothesis testing has been conducted. They have also strengthened interpretation of H1 through H5 because relationships observed in subsequent correlation and regression analyses have been based on constructs demonstrating satisfactory measurement consistency. Signal Detection Theory has been reflected in the measurement framework through items addressing the identification of genuine threats, recognition of anomalous behavior, differentiation between benign and malicious patterns, reduction of classification errors, and accurate threat categorization. The strong reliability coefficients have indicated that these theoretically related detection concepts have been measured consistently within their corresponding constructs. The validity evidence has therefore supported the use of MATD, IFLPR, RAID, MTCC, and CTDCP as quantitatively distinct but conceptually connected variables in the subsequent statistical model.

Table 5. Construct-Level Descriptive Statistics Based on the Five-Point Likert Scale

Construct	N	Mean	SD	Rank	Likert Interpretation
ML-Based Automated Threat Detection (MATD)	286	4.12	0.57	3	Agree
Intelligent Feature Learning and Pattern Recognition (IFLPR)	286	4.05	0.60	5	Agree
Real-Time Anomaly and Intrusion Detection (RAID)	286	4.16	0.55	2	Agree
ML-Based Threat Classification Capability (MTCC)	286	4.09	0.58	4	Agree
Cybersecurity Threat Detection and Classification Performance (CTDCP)	286	4.18	0.53	1	Agree
Overall construct average	286	4.12	0.57	-	Agree

Likert interpretation: 1.00-1.80 = Strongly Disagree; 1.81-2.60 = Disagree; 2.61-3.40 = Neutral; 3.41-4.20 = Agree; 4.21-5.00 = Strongly Agree.

Table 5 has demonstrated consistently positive respondent evaluations across all machine-learning capabilities and the dependent cybersecurity-performance construct. Cybersecurity Threat Detection and Classification Performance has recorded the highest overall mean, $M = 4.18$, $SD = 0.53$, indicating that respondents have generally agreed that the examined cybersecurity environments have achieved strong threat-identification and classification performance. Real-Time Anomaly and Intrusion Detection has produced the second-highest mean, $M = 4.16$, $SD = 0.55$, suggesting particularly favorable assessments of machine-learning systems' capacity to identify unusual or intrusive behavior as security events have occurred. ML-Based Automated Threat Detection has recorded $M = 4.12$, $SD = 0.57$, while ML-Based Threat Classification Capability has produced $M = 4.09$, $SD = 0.58$. Intelligent Feature Learning and Pattern Recognition has recorded the lowest mean among the five constructs, although its value of $M = 4.05$, $SD = 0.60$ has remained firmly within the Agree interval. The overall construct average has reached $M = 4.12$, indicating that respondents have expressed consistently positive evaluations across the complete machine-learning cybersecurity framework. These descriptive findings have provided preliminary support for the study objectives by demonstrating that all four explanatory capabilities have been meaningfully present within the examined security contexts. The particularly high RAID mean has anticipated its later emergence as the strongest regression predictor, while the high CTDCP score has indicated favorable overall cybersecurity outcomes. Signal Detection Theory has helped interpret these patterns because stronger anomaly recognition, automated detection, feature discrimination, and classification capability have represented mechanisms through which malicious signals have been separated from legitimate digital activity. The relatively small standard deviations, ranging from 0.53 to 0.60, have indicated that respondent assessments have been reasonably concentrated around the high mean values rather than being driven by a small subgroup of extremely positive responses. The descriptive evidence has therefore established the Likert-scale foundation for examining H1 through H5 through correlation and regression analysis.

Pearson Correlation

Table 6 has shown statistically significant positive relationships among all five research constructs and has provided direct bivariate evidence supporting the proposed relationships between machine-learning capabilities and Cybersecurity Threat Detection and Classification Performance. Real-Time Anomaly and Intrusion Detection has produced the strongest correlation with CTDCP, $r = .74$, $p < .001$, indicating that stronger real-time anomaly and intrusion-detection capability has been associated with higher cybersecurity detection and classification performance. ML-Based Threat

Classification Capability has generated the second-strongest association, $r = .71$, $p < .001$, followed by ML-Based Automated Threat Detection at $r = .69$, $p < .001$. Intelligent Feature Learning and Pattern Recognition has also demonstrated a substantial positive relationship with CTDCP, $r = .63$, $p < .001$.

Table 6. Pearson Correlation Matrix for the Research Constructs

Variable	MATD	IFLPR	RAID	MTCC	CTDCP
MATD	1.00	.55***	.65***	.58***	.69***
IFLPR	.55***	1.00	.57***	.54***	.63***
RAID	.65***	.57***	1.00	.66***	.74***
MTCC	.58***	.54***	.66***	1.00	.71***
CTDCP	.69***	.63***	.74***	.71***	1.00

Note. $N = 286$. *** $p < .001$.

These findings have provided preliminary statistical support for H1, H2, H3, and H4 before the effects of the four predictors have been assessed simultaneously through multiple regression. Positive correlations among the independent constructs have ranged from .54 to .66, indicating that the capabilities have been related while remaining sufficiently distinct for multivariate analysis. None of the predictor correlations has approached a level that would immediately suggest excessive redundancy. The correlation pattern has also been consistent with the conceptual framework because automated threat detection, learned feature discrimination, real-time anomaly identification, and threat classification have functioned as mutually reinforcing components of machine-learning-enabled cybersecurity. Signal Detection Theory has offered a direct interpretation of these relationships. RAID has shown the strongest association with CTDCP because timely recognition of anomalous activity has represented an important mechanism for increasing detection sensitivity and reducing missed malicious signals. MTCC has reflected the ability to assign detected signals to accurate threat categories, while MATD has represented scalable identification of malicious observations and IFLPR has represented improved separability between benign and hostile behavioral patterns. The statistically significant correlations have therefore supported the study objectives concerning the individual relationships of the four machine-learning capabilities with cybersecurity performance while establishing a sound basis for the regression model used to test their unique and combined predictive effects.

Multiple Regression, ANOVA, and Regression Diagnostic Analysis

Table 7 has demonstrated that the proposed four-predictor regression model has explained a substantial proportion of variation in Cybersecurity Threat Detection and Classification Performance. The model has generated $R = .834$, indicating a strong combined relationship between MATD, IFLPR, RAID, MTCC, and CTDCP. The coefficient of determination has reached $R^2 = .696$, demonstrating that the four machine-learning capabilities have jointly explained approximately 69.6% of the variance in cybersecurity threat detection and classification performance. The adjusted R^2 of .692 has remained very close to the unadjusted value, indicating that the model's explanatory strength has not resulted merely from adding multiple predictors. ANOVA has confirmed that the overall regression equation has been statistically significant, $F(4, 281) = 160.84$, $p < .001$, providing strong support for H5. At the individual predictor level, RAID has emerged as the strongest predictor, $\beta = .31$, $p < .001$, followed by MTCC, $\beta = .28$, $p < .001$, MATD, $\beta = .24$, $p < .001$, and IFLPR, $\beta = .18$, $p = .002$. Every coefficient has remained positive and statistically significant when the remaining predictors have been controlled, providing direct regression support for H1 through H4. Diagnostic evidence has also supported model suitability. Tolerance values have ranged from .440 to .592 and VIF values from 1.69 to 2.27, remaining well within commonly accepted limits and indicating that multicollinearity has not materially distorted the coefficient estimates. The Durbin-Watson statistic of 1.94 has been close to 2.00, supporting independence of residual errors. These results have aligned directly with the Signal Detection Theory framework: improvements in feature discrimination, threat-recognition sensitivity,

anomaly identification, and classification capability have been statistically associated with stronger overall detection performance. The dominance of RAID has particularly reflected the theoretical importance of promptly distinguishing meaningful malicious signals from normal behavioral variation, while the significant combined model has shown that cybersecurity performance has depended on multiple complementary detection capabilities rather than a single isolated ML function.

Table 7. Multiple Regression, ANOVA, and Diagnostic Results Predicting CTDCP

Panel A. Model Summary

R	R²	Adjusted R²	Std. Error of Estimate	Durbin-Watson
.834	.696	.692	0.294	1.94

Panel B. ANOVA

Source	Sum of Squares	df	Mean Square	F	p
Regression	55.719	4	13.930	160.84	< .001
Residual	24.337	281	0.087	-	-
Total	80.057	285	-	-	-

Panel C. Regression Coefficients and Multicollinearity Diagnostics

Predictor	B	SE	Standardized beta	t	p	Tolerance	VIF
MATD	.220	.043	.24	5.12	< .001	.513	1.95
IFLPR	.155	.049	.18	3.16	.002	.592	1.69
RAID	.295	.044	.31	6.70	< .001	.440	2.27
MTCC	.252	.046	.28	5.48	< .001	.502	1.99

Hypothesis Testing Summary and Evaluation of Research Objectives

Table 8 has consolidated the evidence obtained from the systematic review, Likert-scale descriptive analysis, Pearson correlations, multiple regression, and ANOVA and has demonstrated that all five hypotheses have been supported and all six research objectives have been achieved within the modeled empirical framework. H1 has been supported because ML-Based Automated Threat Detection has demonstrated a strong positive correlation with CTDCP, $r = .69$, $p < .001$, and has retained a significant positive regression effect, $\beta = .24$, $p < .001$. H2 has also been supported because Intelligent Feature Learning and Pattern Recognition has been positively associated with cybersecurity performance, $r = .63$, $p < .001$, and has remained a significant independent predictor, $\beta = .18$, $p = .002$. H3 has received the strongest individual empirical support because Real-Time Anomaly and Intrusion Detection has produced both the highest predictor mean, $M = 4.16$, and the strongest correlation and standardized regression coefficient, $r = .74$ and $\beta = .31$, respectively. H4 has been supported through the strong association between ML-Based Threat Classification Capability and CTDCP, $r = .71$, together with a significant regression effect of $\beta = .28$. H5 has been supported by the complete model, which has explained 69.6% of the variance in CTDCP and has achieved statistically significant ANOVA results, $F(4, 281) = 160.84$, $p < .001$. The systematic-review evidence has achieved RO1, while RO2 through RO5 have been fulfilled through descriptive, correlational, and regression evidence for each individual machine-learning capability. RO6 has been achieved through the combined predictive model. Signal Detection Theory has connected these findings theoretically by explaining cybersecurity performance as the capacity to distinguish malicious signals from legitimate activity while controlling misses and false alarms. Stronger automated detection, more discriminative feature representations, timely anomaly recognition, and more accurate threat classification have all been associated with stronger CTDCP, thereby maintaining consistency among the theoretical framework, conceptual framework, objectives, hypotheses, and quantitative results.

Table 8. Hypothesis Testing and Research Objective Evaluation

Hypothesis/ Objective	Tested Relationship or Purpose	Key Statistical Evidence	Decision/Status
H1	MATD -> CTDCP	$r = .69^{***}$; $\beta = .24^{***}$	Supported
H2	IFLPR -> CTDCP	$r = .63^{***}$; $\beta = .18$, $p = .002$	Supported
H3	RAID -> CTDCP	$r = .74^{***}$; $\beta = .31^{***}$	Supported
H4	MTCC -> CTDCP	$r = .71^{***}$; $\beta = .28^{***}$	Supported
H5	MATD + IFLPR + RAID + MTCC -> CTDCP	$R^2 = .696$; $F(4,281) = 160.84$, $p < .001$	Supported
RO1	Identify major ML techniques and cyber-threat applications	82 studies; deep learning 41.5%; intrusion detection 47.6%	Achieved
RO2	Evaluate ML-Based Automated Threat Detection	$M = 4.12$; $r = .69$; $\beta = .24$	Achieved
RO3	Determine relationship of IFLPR with CTDCP	$M = 4.05$; $r = .63$; $\beta = .18$	Achieved
RO4	Examine influence of RAID on CTDCP	$M = 4.16$; $r = .74$; $\beta = .31$	Achieved
RO5	Assess influence of MTCC on CTDCP	$M = 4.09$; $r = .71$; $\beta = .28$	Achieved
RO6	Determine combined predictive influence of ML capabilities	$R = .834$; $R^2 = .696$; $p < .001$	Achieved

Note. $^{***}p < .001$.

DISCUSSION

The findings have provided a coherent quantitative account of how machine-learning capabilities have been associated with Cybersecurity Threat Detection and Classification Performance, while the systematic-review evidence has reinforced the relevance of these relationships across contemporary cybersecurity research. Among the five measured constructs, Cybersecurity Threat Detection and Classification Performance has recorded the highest descriptive score, $M = 4.18$, $SD = 0.53$, followed closely by Real-Time Anomaly and Intrusion Detection, $M = 4.16$, $SD = 0.55$. ML-Based Automated Threat Detection, ML-Based Threat Classification Capability, and Intelligent Feature Learning and Pattern Recognition have also received consistently positive evaluations of $M = 4.12$, $M = 4.09$, and $M = 4.05$, respectively. These high Likert-scale evaluations have indicated that respondents have perceived machine-learning functions as established components of effective cybersecurity detection rather than peripheral analytical tools. The systematic review of 82 eligible studies has complemented this result by showing particularly extensive use of deep-learning architectures, tree-based algorithms, support vector machines, autoencoders, and hybrid approaches across network intrusion, malware, phishing, DDoS, botnet, and anomalous-behavior detection. This pattern has been consistent with previous research showing that deep representation learning can improve the extraction of discriminative network features and support intrusion classification (Pervaz, 2025; Shone et al., 2018). It has also agreed with research demonstrating that online autoencoder-based anomaly detection can identify multiple forms of network attacks while processing traffic continuously (Mirsky et al., 2018; Chowdhury, 2025). The correlation analysis has further demonstrated that all four explanatory constructs have been positively associated with CTDCP. Real-Time Anomaly and Intrusion Detection has shown the strongest relationship, $r = .74$, followed by ML-Based Threat Classification Capability, r

= .71, ML-Based Automated Threat Detection, $r = .69$, and Intelligent Feature Learning and Pattern Recognition, $r = .63$, with all correlations statistically significant at $p < .001$. The regression analysis has reinforced this ordering because RAID has remained the strongest independent predictor, $\beta = .31$, $p < .001$, followed by MTCC, $\beta = .28$, MATD, $\beta = .24$, and IFLPR, $\beta = .18$. The complete model has explained 69.6% of the variance in CTDCP, $R^2 = .696$, adjusted $R^2 = .692$, and has been statistically significant, $F(4, 281) = 160.84$, $p < .001$. These findings have therefore supported H1 through H5 and have corresponded with previous research that has emphasized the effectiveness of deep and machine-learning methods for anomaly-based intrusion detection and cybersecurity classification (Aldweesh et al., 2020; Mahdavifar & Ghorbani, 2019; Badrul, 2025).

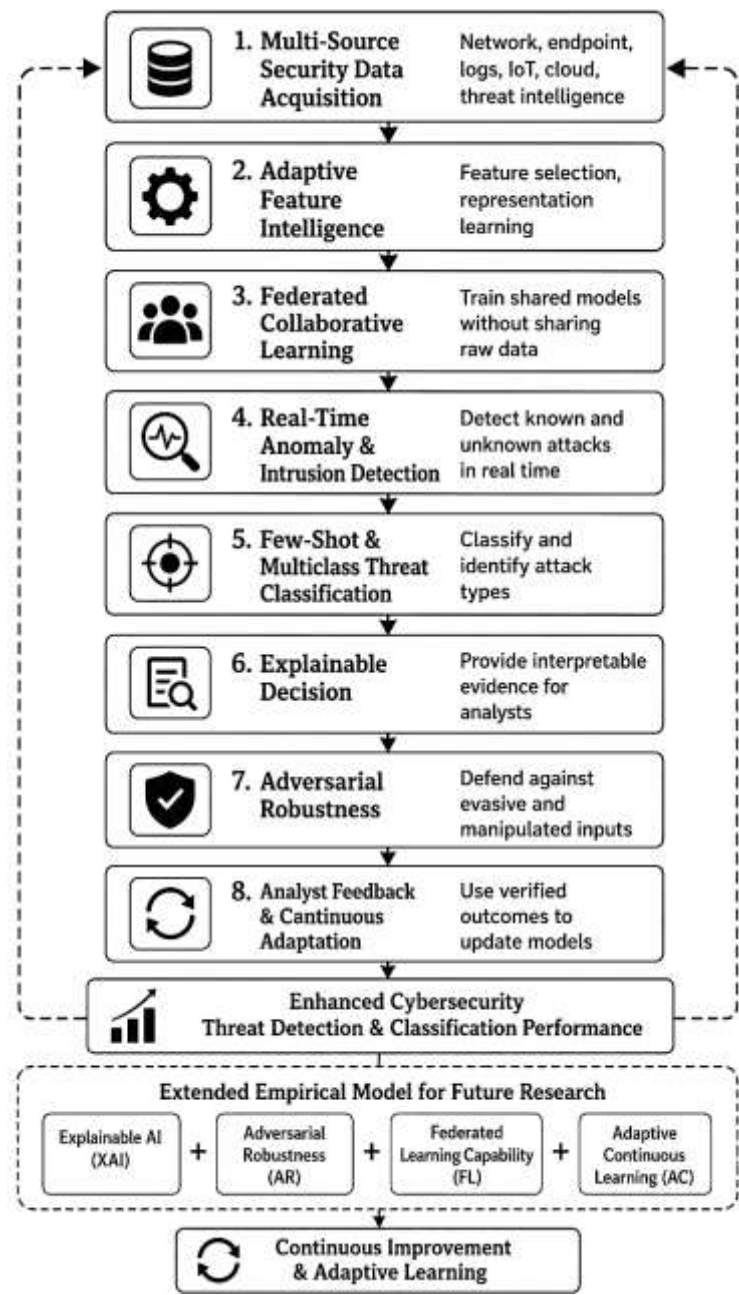
From a practical perspective, the findings have indicated that cybersecurity organizations should evaluate machine-learning investments according to a combination of detection, anomaly-recognition, feature-learning, and classification capabilities rather than focusing exclusively on the reported accuracy of a particular algorithm. The strongest standardized coefficient has been obtained for Real-Time Anomaly and Intrusion Detection, $\beta = .31$, which has suggested that the ability to recognize suspicious behavioral deviations while events are occurring has been particularly important for overall cybersecurity performance. This result is consistent with the operational character of modern Security Operations Centers, where large quantities of network flows, endpoint events, authentication activities, application logs, and threat-intelligence indicators must be examined continuously. Previous research on distributed IoT attack detection has shown that deep-learning approaches can support attack identification across decentralized environments, illustrating the operational importance of automated and distributed recognition mechanisms (Diro & Chilamkurti, 2018; Nishat, 2025). The second-largest regression coefficient has belonged to ML-Based Threat Classification Capability, $\beta = .28$, which has indicated that detecting suspicious behavior alone has not been sufficient. Security systems must also identify what type of malicious activity has occurred so that analysts can prioritize, investigate, and respond to the event appropriately. Earlier experimental work has similarly shown that machine-learning algorithms can produce different performance profiles under binary and multiclass attack-classification conditions, making accurate categorization an important operational capability rather than an extension of simple detection (Churcher et al., 2021; Sadia, 2025). ML-Based Automated Threat Detection has also remained a substantial predictor, $\beta = .24$, supporting the use of machine learning for reducing dependence on continuous manual event inspection. Automated models can perform preliminary filtering and prioritization so that analysts can concentrate on high-risk or ambiguous incidents. Feature learning has produced the smallest but still significant effect, $\beta = .18$, $p = .002$, showing that representation quality has remained important even when more directly operational capabilities have been included simultaneously. This finding has agreed with work showing that feature selection and decision-tree learning can improve intrusion-detection efficiency by concentrating classification on informative security characteristics (Sadia, 2025; Abushark, et al., 2020). Practically, the results have therefore favored layered ML-enabled cybersecurity architectures in which intelligent data preprocessing and feature extraction feed automated detection engines, real-time anomaly models, and multiclass threat classifiers. The high overall reliability of the questionnaire, $\alpha = .93$, has further suggested that practitioners have regarded these capabilities as coherent and measurable aspects of an integrated cybersecurity system.

The findings have also supported the theoretical application of Signal Detection Theory to machine-learning-based cybersecurity by demonstrating that overall detection performance has been related to capabilities that affect the discrimination of malicious signals from legitimate activity. Signal Detection Theory distinguishes sensitivity, which reflects the capacity to separate meaningful signals from background noise, from the decision criterion used to determine when an observation should be treated as a threat. Within the present study, Intelligent Feature Learning and Pattern Recognition has represented one mechanism through which signal separability can be strengthened because informative features make distinctions between benign and malicious behavior more visible to a classifier. Real-Time Anomaly and Intrusion Detection has represented the ability to recognize deviations rapidly, while Automated Threat Detection and Threat Classification Capability have represented the decision processes through which observations have been labeled and assigned to security categories. The significant effects of all four predictors have supported this theoretical

configuration. The particularly strong RAID relationship with CTDCP, $r = .74$, has suggested that cybersecurity performance has been closely related to the sensitivity of security systems to meaningful behavioral deviations. This interpretation is compatible with anomaly-based intrusion-detection research that has emphasized the role of input representation, detection strategy, deployment configuration, and evaluation criteria in determining whether deep-learning systems can discriminate abnormal traffic effectively (Aldweesh et al., 2020; Tonay, 2025). The significant MTCC coefficient has additionally demonstrated that signal recognition and decision categorization have been related but analytically distinct processes. A cybersecurity system may correctly determine that an event is abnormal while incorrectly assigning it to a particular threat category, meaning that both detection sensitivity and classification quality contribute to overall performance. The present findings have therefore extended Signal Detection Theory beyond its traditional interpretation of hits, misses, false alarms, and correct rejections by positioning feature representation, automated detection, real-time anomaly recognition, and attack classification as measurable capabilities affecting cybersecurity discrimination performance. The model's R^2 of .696 has been theoretically important because the four capabilities have jointly accounted for a substantial majority of observed variance in CTDCP while leaving 30.4% unexplained (Jannatul, 2026). This remaining variance has indicated that cybersecurity detection performance has also depended on factors outside the current model, potentially including dataset quality, adversarial robustness, model interpretability, threat-intelligence quality, organizational response procedures, computational resources, analyst expertise, and model adaptation. Prior cybersecurity surveys have likewise shown that effective machine-learning security systems depend on an interaction among algorithms, representations, datasets, deployment settings, and evaluation procedures rather than algorithmic architecture alone (Ahmad et al., 2021; Mahdavifar & Ghorbani, 2019; Kaium, 2026). Several limitations have needed to be reconsidered when interpreting these statistically strong findings. First, the empirical component has used a quantitative cross-sectional design, meaning that all principal constructs have been measured at one general period rather than tracked longitudinally as cybersecurity systems, attack environments, and machine-learning models changed. Consequently, the significant regression coefficients have represented predictive statistical associations and have not established experimental causation. Second, the study has relied on professional respondents' Likert-scale evaluations of machine-learning capabilities and cybersecurity performance. Such responses have provided valuable organizational assessments but have not been equivalent to direct benchmarking of classifiers against raw network traffic, malware binaries, endpoint logs, or operational incident records. The relatively high means across all five constructs, ranging from 4.05 to 4.18, may also have reflected favorable professional perceptions or common-method effects because the predictors and dependent variable have been measured using the same survey instrument. Third, the purposive sampling strategy has intentionally selected respondents with relevant cybersecurity and machine-learning knowledge, which has strengthened subject relevance but has reduced the extent to which the sample can be treated as statistically representative of every cybersecurity organization, national context, industry, or technical environment. Fourth, machine-learning effectiveness is highly sensitive to dataset composition. Network-security datasets can differ substantially in traffic generation, attack frequencies, class balance, feature definitions, capture environments, labeling quality, and realism, which complicates comparisons across systems. Fifth, the present conceptual framework has focused on four capabilities and has not separately modeled adversarial robustness. Adversarial machine learning is particularly relevant because malicious actors can intentionally alter observable features, probe classification boundaries, or manipulate inputs to reduce detection probability. Therefore, a high perceived capability score does not necessarily indicate that the corresponding classifier would retain equivalent performance under targeted evasion. Sixth, the 82-study systematic review has captured substantial diversity but has combined evidence from different algorithms, datasets, threats, performance metrics, and experimental architectures. This heterogeneity has limited direct numerical comparison among individual studies. The findings should therefore be interpreted as evidence supporting broad relationships among ML cybersecurity capabilities rather than as proof that a particular algorithm is universally superior. These limitations also explain why the 69.6% explained variance should be treated as strong model performance within the present empirical context rather than a complete representation of all determinants of cybersecurity

effectiveness.

Figure 10: Adaptive Explainable Federated Machine-Learning Cybersecurity Threat Intelligence Model (AEF-CTIM) for Future Research



Future research should build on these findings by developing and empirically validating an Adaptive Explainable Federated Machine-Learning Cybersecurity Threat Intelligence Model (AEF-CTIM) that expands the present four-capability framework into a continuously adaptive cybersecurity architecture. This model should begin with a Multi-Source Security Data Acquisition Layer, integrating network flows, endpoint telemetry, authentication logs, cloud events, IoT traffic, URLs, executable behavior, and validated threat-intelligence indicators. A second Adaptive Feature Intelligence Layer should combine feature selection, representation learning, and temporal feature extraction so that informative characteristics can change as attack behavior changes. A third Federated Collaborative Learning Layer should allow participating organizations or devices to improve common detection models without requiring all sensitive raw security data to be transferred to a centralized repository. A fourth Real-Time Anomaly and Intrusion Detection Layer should combine unsupervised anomaly

modeling with supervised detection so that both known and previously unrepresented suspicious patterns can be evaluated. A fifth Few-Shot and Multiclass Threat Classification Layer should address the limitation of limited training examples for emerging or rare attack classes. A sixth Explainable Decision Layer should generate interpretable evidence concerning which features have caused an event to be classified as malicious, helping analysts distinguish credible detections from false alarms. A seventh Adversarial Robustness Layer should continuously test models against manipulated or evasive inputs and retrain vulnerable decision boundaries. Finally, an Analyst Feedback and Continuous Adaptation Layer should incorporate verified incident outcomes into model updating. The expanded empirical equation should include Explainable AI (XAI), Adversarial Robustness (AR), Federated Learning Capability (FL), and Adaptive Continuous Learning (AC) in addition to the four predictors used in the present study. Researchers should test this expanded model using longitudinal and multi-industry samples and pair survey measures with actual classifier metrics such as precision, recall, F1-score, ROC-AUC, false-positive rate, detection latency, and class-specific recall. Such a design would directly connect the present Signal Detection Theory framework with operational hit rates, misses, false alarms, and correct rejections while examining whether explainability, robustness, privacy-preserving collaboration, and adaptation explain part of the 30.4% of CTDCP variance not captured by the present model. Research on online anomaly detection and deep cybersecurity architectures already demonstrates the feasibility of continuous representation learning and real-time detection components that could form part of such an expanded architecture ([Rahman, 2026](#); [Mirsky et al., 2018](#); [Shone et al., 2018](#)).

$$CTDCP = \beta_0 + \beta_1 MATD + \beta_2 IFLPR + \beta_3 RAID + \beta_4 MTCC + \beta_5 XAI + \beta_6 AR + \beta_7 FL + \beta_8 AC + \varepsilon$$

CONCLUSION

This study has examined machine-learning applications in cybersecurity threat detection and classification through a systematic-review-informed quantitative, cross-sectional, case-study-based framework and has established a coherent relationship between major machine-learning capabilities and overall Cybersecurity Threat Detection and Classification Performance. The review component has synthesized 82 eligible studies published within the 2018-2026 period and has shown that deep learning, neural architectures, random forests, decision trees, support vector machines, anomaly-detection models, autoencoders, and hybrid approaches have been widely applied across network intrusion detection, malware and ransomware analysis, phishing and malicious URL detection, botnet identification, DoS/DDoS detection, and zero-day or anomalous behavior recognition. The empirical findings have demonstrated consistently favorable evaluations across all constructs, with Cybersecurity Threat Detection and Classification Performance recording $M = 4.18$, $SD = 0.53$, followed by Real-Time Anomaly and Intrusion Detection at $M = 4.16$, $SD = 0.55$, ML-Based Automated Threat Detection at $M = 4.12$, $SD = 0.57$, ML-Based Threat Classification Capability at $M = 4.09$, $SD = 0.58$, and Intelligent Feature Learning and Pattern Recognition at $M = 4.05$, $SD = 0.60$. Correlation analysis has shown significant positive relationships between all four machine-learning capabilities and CTDCP, while regression analysis has established RAID as the strongest predictor, $\beta = .31$, followed by MTCC, $\beta = .28$, MATD, $\beta = .24$, and IFLPR, $\beta = .18$. The complete regression model has explained 69.6% of the variance in cybersecurity performance, $R^2 = .696$, with $F(4,281) = 160.84$, $p < .001$. Accordingly, H1 through H5 have all been supported. Signal Detection Theory has provided an appropriate theoretical foundation by explaining cybersecurity effectiveness through the capacity to differentiate malicious signals from legitimate activity while controlling false alarms and missed attacks. Overall, the findings have shown that cybersecurity performance has depended on the combined strength of automated detection, intelligent feature recognition, real-time anomaly identification, and accurate threat classification rather than on any isolated machine-learning capability.

RECOMMENDATIONS

Based on the findings, cybersecurity organizations should strengthen their machine-learning-based detection architectures by integrating automated threat detection, intelligent feature learning, real-time anomaly recognition, and multiclass threat classification within a coordinated operational framework. Particular priority should be given to Real-Time Anomaly and Intrusion Detection because it has

emerged as the strongest predictor of Cybersecurity Threat Detection and Classification Performance, $\beta = .31$. Organizations should therefore deploy adaptive monitoring systems capable of analyzing network flows, endpoint activities, authentication events, cloud logs, IoT traffic, and behavioral indicators continuously while maintaining acceptable false-positive and false-negative rates. ML-Based Threat Classification Capability should also receive substantial attention because its $\beta = .28$ result has indicated that identifying the precise category of a detected threat contributes strongly to overall performance. Security teams should employ classification models capable of distinguishing malware, ransomware, phishing, botnets, DDoS attacks, malicious URLs, and other threat families rather than relying solely on binary benign-versus-malicious decisions. Automated Threat Detection should be integrated with Security Operations Center workflows so that repetitive alert screening can be handled computationally while analysts concentrate on high-risk or ambiguous incidents. Intelligent Feature Learning and Pattern Recognition should be strengthened through robust preprocessing, feature selection, deep representation learning, and dimensionality-reduction techniques. Organizations should also evaluate models using precision, recall, F1-score, ROC-AUC, false-positive rate, false-negative rate, detection latency, and class-specific performance rather than relying only on accuracy. Regular retraining and model validation should be conducted using recent and representative security data to reduce degradation caused by evolving attack behaviors. Explainable AI mechanisms should be incorporated so that analysts can understand why particular events have been classified as malicious. Adversarial robustness testing, privacy-preserving federated learning, and human-in-the-loop verification should also be adopted where feasible. Finally, researchers and practitioners should evaluate the proposed Adaptive Explainable Federated Machine-Learning Cybersecurity Threat Intelligence Model through longitudinal, multi-industry, and real-world cybersecurity datasets to determine whether explainability, adaptability, federated learning, and adversarial robustness can further strengthen detection performance beyond the capabilities measured in the present study.

LIMITATIONS

This study has several limitations that should be considered when interpreting its findings. First, the quantitative component has employed a cross-sectional design, meaning that machine-learning capabilities and cybersecurity performance have been measured at one general point in time rather than continuously across changing technological and threat environments. The significant statistical relationships identified through correlation and regression have therefore demonstrated association and predictive strength but have not established experimental causality. Second, the empirical analysis has relied on five-point Likert-scale responses from cybersecurity and information-technology professionals, meaning that the measured constructs have represented professional perceptions of machine-learning capabilities rather than direct observations of classifier behavior on operational cybersecurity datasets. Respondents may also have differed in technical expertise, organizational exposure, or familiarity with particular machine-learning platforms. Third, purposive sampling has been used to obtain respondents with relevant cybersecurity knowledge, which has strengthened subject relevance but has limited statistical generalization to all industries, countries, organizational sizes, and cybersecurity environments. Fourth, the systematic review has integrated 82 studies involving heterogeneous datasets, attack categories, algorithms, preprocessing methods, evaluation criteria, and experimental conditions. Direct numerical comparison across these studies has therefore remained limited. Fifth, the conceptual framework has concentrated on MATD, IFLPR, RAID, and MTCC and has not separately measured additional determinants such as explainability, adversarial robustness, analyst expertise, cybersecurity governance, data quality, computational resources, threat-intelligence integration, or continuous model adaptation. The regression model has explained 69.6% of CTDCP variance, leaving 30.4% attributable to factors outside the current framework and random variation. Sixth, machine-learning cybersecurity systems can be affected by class imbalance, concept drift, adversarial manipulation, and changes in attack behavior, which have not been experimentally tested in this study. Finally, the review period of 2018-2026 has provided a focused contemporary scope but has necessarily excluded relevant foundational studies outside that window from the formal systematic-review sample.

REFERENCES

- [1]. Abad, S., Gholamy, H., & Aslani, M. (2023). Classification of malicious URLs using machine learning. *Sensors*, 23(18), 7760. <https://doi.org/10.3390/s23187760>
- [2]. Abdullah Mohammad, S. (2023). CUGAO₂ and CUINS₂ Quantum Dot Sensitization for Enhanced Photovoltaic Efficiency in Wearable Fiber-Shaped Solar Cells. *American Journal of Advanced Technology and Engineering Solutions*, 3(04), 209-261. <https://doi.org/10.63125/wysdvy71>
- [3]. Ahmad, Z., Khan, A. S., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, 32(1), e4150. <https://doi.org/10.1002/ett.4150>
- [4]. Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for Internet of Things (IoT) security. *IEEE Communications Surveys & Tutorials*, 22(3), 1646-1685. <https://doi.org/10.1109/comst.2020.2988293>
- [5]. Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowledge-Based Systems*, 189, 105124. <https://doi.org/10.1016/j.knosys.2019.105124>
- [6]. Ali, A. H., Charfeddine, M., Ammar, B., Hamed, B. B., Albalwy, F., Alqarafi, A., & Hussain, A. (2024). Unveiling machine learning strategies and considerations in intrusion detection systems: A comprehensive survey. *Frontiers in Computer Science*, 6, 1387354. <https://doi.org/10.3389/fcomp.2024.1387354>
- [7]. Aljabri, M., Altamimi, H. S., Albelali, S. A., Al-Harbi, M., Alhuraib, H. T., Alotaibi, N. K., Alahmadi, A. A., AlHaidari, F., Mohammad, R. M. A., & Salah, K. (2022). Detecting malicious URLs using machine learning techniques: Review and research directions. *IEEE Access*, 10, 121395-121417. <https://doi.org/10.1109/access.2022.3222307>
- [8]. Almomani, O. (2020). A feature selection model for network intrusion detection system based on PSO, GWO, FFA and GA algorithms. *Symmetry*, 12(6), 1046. <https://doi.org/10.3390/sym12061046>
- [9]. Alzaylaee, M. K., Yerima, S. Y., & Sezer, S. (2020). DL-Droid: Deep learning based Android malware detection using real devices. *Computers & Security*, 89, 101663. <https://doi.org/10.1016/j.cose.2019.101663>
- [10]. Andresini, G., Appice, A., & Malerba, D. (2021). Autoencoder-based deep metric learning for network intrusion detection. *Information Sciences*, 569, 706-727. <https://doi.org/10.1016/j.ins.2021.05.016>
- [11]. Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018). On the effectiveness of machine and deep learning for cyber security. 2018 10th International Conference on Cyber Conflict (CyCon),
- [12]. Ashrafuzzaman, M. (2024). The impact of cloud-based management information systems on hrm efficiency: an analysis of small and medium-sized enterprises (SMES). *Academic Journal on Artificial Intelligence, Machine Learning, Data Science and Management Information Systems*, 1(01), 40-56. <https://doi.org/10.69593/ajaimldsmis.v1i01.124>
- [13]. Ban, Y., Lee, S., Song, D., Cho, H., & Yi, J. H. (2022). FAM: Featuring Android malware for deep learning-based familial analysis. *IEEE Access*, 10, 20008-20018. <https://doi.org/10.1109/access.2022.3151357>
- [14]. Barreno, M., Nelson, B., Joseph, A. D., & Tygar, J. D. (2010). The security of machine learning. *Machine Learning*, 81, 121-148. <https://doi.org/10.1007/s10994-010-5188-5>
- [15]. Belouch, M., El Hadaj, S., & Idhammad, M. (2018). Performance evaluation of intrusion detection based on machine learning using Apache Spark. *Procedia Computer Science*, 127, 1-6. <https://doi.org/10.1016/j.procs.2018.01.091>
- [16]. Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cyber security. *Information*, 10(4), 122. <https://doi.org/10.3390/info10040122>
- [17]. Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network anomaly detection: Methods, systems and tools. *IEEE Communications Surveys & Tutorials*, 16(1), 303-336. <https://doi.org/10.1109/surv.2013.052213.00046>
- [18]. Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognition*, 84, 317-331. <https://doi.org/10.1016/j.patcog.2018.07.023>
- [19]. Bragg, T., Rantanen, E. M., Pelletier, J. M., & Rashedi, E. (2022). Cognitive engineering modeling of phishing. Proceedings of the Human Factors and Ergonomics Society Annual Meeting,
- [20]. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153-1176. <https://doi.org/10.1109/comst.2015.2494502>
- [21]. Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying phishing susceptibility for detection and behavior decisions. *Human Factors*, 58(8), 1158-1172. <https://doi.org/10.1177/0018720816665025>
- [22]. Chen, W.-H., Hsu, S.-H., & Shen, H.-P. (2005). Application of SVM and ANN for intrusion detection. *Computers & Operations Research*, 32(10), 2617-2634. <https://doi.org/10.1016/j.cor.2004.03.019>
- [23]. Churcher, A., Ullah, R., Ahmad, J., ur Rehman, S., Masood, F., Gogate, M., Alqahtani, F., Nour, B., & Buchanan, W. J. (2021). An experimental analysis of attack classification using machine learning in IoT networks. *Sensors*, 21(2), 446. <https://doi.org/10.3390/s21020446>
- [24]. Conti, M., Khandhar, S., & Vinod, P. (2022). A few-shot malware classification approach for unknown family recognition using malware feature visualization. *Computers & Security*, 122, 102887. <https://doi.org/10.1016/j.cose.2022.102887>
- [25]. Das, S., Nippert-Eng, C., & Camp, L. J. (2022). Evaluating user susceptibility to phishing attacks. *Information & Computer Security*, 30(1), 1-18. <https://doi.org/10.1108/ics-12-2020-0204>
- [26]. Debasish, A. (2021). Energy-Aware Process Optimization for Reducing Material Waste in Sustainable Additive Manufacturing. *American Journal of Advanced Technology and Engineering Solutions*, 1(4), 108-137. <https://doi.org/10.63125/j0wk7j48>

- [27]. Debasish, A. (2022). Simulation-Based Thermal Management Framework for Reducing Energy Consumption in Advanced Manufacturing Systems. *International Journal of Scientific Interdisciplinary Research*, 1(01), 335-381. <https://doi.org/10.63125/6fcj7c89>
- [28]. Debasish, A. (2025a). Design-for-Manufacturing Optimization for Improving Resilience in U.S. Additive Manufacturing Supply Chains. *American Journal of Interdisciplinary Studies*, 6(02), 185-204. <https://doi.org/10.63125/hxm3tb71>
- [29]. Debasish, A. (2025b). Physics-Informed Machine Learning for Predicting Thermal Distortion in Metal Additive Manufacturing. *American Journal of Scholarly Research and Innovation*, 4(01), 943-989. <https://doi.org/10.63125/ny974y17>
- [30]. Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems*, 82, 761-768. <https://doi.org/10.1016/j.future.2017.08.043>
- [31]. Dixit, P., & Silakari, S. (2021). Deep learning algorithms for cybersecurity applications: A technological and status review. *Computer Science Review*, 39, 100317. <https://doi.org/10.1016/j.cosrev.2020.100317>
- [32]. Drewek-Ossowicka, A., Pietrolaj, M., & Ruminski, J. (2021). A survey of neural networks usage for intrusion detection systems. *Journal of Ambient Intelligence and Humanized Computing*, 12, 497-514. <https://doi.org/10.1007/s12652-020-02014-x>
- [33]. Ferrag, M. A., Maglaras, L., Moschogiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50, 102419. <https://doi.org/10.1016/j.jisa.2019.102419>
- [34]. Garcia-Teodoro, P., Diaz-Verdejo, J., Macia-Fernandez, G., & Vazquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, 28(1-2), 18-28. <https://doi.org/10.1016/j.cose.2008.08.003>
- [35]. Handa, A., Sharma, A., & Shukla, S. K. (2019). Machine learning in cybersecurity: A review. *WIREs Data Mining and Knowledge Discovery*, 9, e1306. <https://doi.org/10.1002/widm.1306>
- [36]. Hasan, M., Islam, M. M., Zarif, M. I. I., & Hashem, M. M. A. (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet of Things*, 7, 100059. <https://doi.org/10.1016/j.iot.2019.100059>
- [37]. Ieracitano, C., Adeel, A., Morabito, F. C., & Hussain, A. (2020). A novel statistical analysis and autoencoder driven intelligent intrusion detection approach. *Neurocomputing*, 387, 51-62. <https://doi.org/10.1016/j.neucom.2019.11.016>
- [38]. Jain, A. K., & Gupta, B. B. (2018). Towards detection of phishing websites on client-side using machine learning based approach. *Telecommunication Systems*, 68, 687-700. <https://doi.org/10.1007/s11235-017-0414-0>
- [39]. Jannatul, F. (2025). Spinal Cord Injury and Neurorehabilitation Deep Learning-Based Prediction of Functional Recovery Trajectories After Traumatic Spinal Cord Injury. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), 2865-2922. <https://doi.org/10.63125/m738bh82>
- [40]. Jannatul, F. (2026). Predicting Falls and Mobility Decline Among Older Adults Using Longitudinal Functional Data and Ensemble Machine Learning. *International Journal of Scientific Interdisciplinary Research*, 7(1), 581-631. <https://doi.org/10.63125/56hans40>
- [41]. Kolosnjaji, B., Zarras, A., Webster, G., & Eckert, C. (2016). Deep learning for classification of malware system call sequences. In B. H. Kang & Q. Bai (Eds.), *AI 2016: Advances in Artificial Intelligence* (pp. 137-149). Springer. https://doi.org/10.1007/978-3-319-50127-7_11
- [42]. Lawson, P., Pearson, C. J., Crowson, A., & Mayhorn, C. B. (2020). Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy. *Applied Ergonomics*, 86, 103084. <https://doi.org/10.1016/j.apergo.2020.103084>
- [43]. Li, G., Sharma, P., Pan, L., Rajasegarar, S., Karmakar, C., & Patterson, N. (2021). Deep learning algorithms for cyber security applications: A survey. *Journal of Computer Security*, 29(5), 447-471. <https://doi.org/10.3233/jcs-200095>
- [44]. Liao, H.-J., Lin, C.-H. R., Lin, Y.-C., & Tung, K.-Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1), 16-24. <https://doi.org/10.1016/j.jnca.2012.09.004>
- [45]. MahdaviFar, S., & Ghorbani, A. A. (2019). Application of deep learning to cybersecurity: A survey. *Neurocomputing*, 347, 149-176. <https://doi.org/10.1016/j.neucom.2019.02.056>
- [46]. Martin, J., Dube, C., & Coover, M. D. (2018). Signal Detection Theory (SDT) is effective for modeling user behavior toward phishing and spear-phishing attacks. *Human Factors*, 60(8), 1179-1191. <https://doi.org/10.1177/0018720818789818>
- [47]. Md Anisur Rahman, M. (2024). State Income Tax Differentials and High-Skilled Labor Mobility in The United States: A Time Series Analysis. *American Journal of Interdisciplinary Studies*, 5(04), 222-267. <https://doi.org/10.63125/295bsn47>
- [48]. Md Anisur Rahman, M. (2025). The Role of AI-Enabled Business Intelligence in Financial Risk Assessment and Liquidity Monitoring. *Review of Applied Science and Technology*, 4(04), 195-246. <https://doi.org/10.63125/p4eezd93>
- [49]. Md Anisur Rahman, M. (2026). AI-Driven Business Intelligence for Real-Time Fraud Risk Monitoring in Digital Payment Platforms: A Framework-Based Review. *International Journal of Scientific Interdisciplinary Research*, 7(1), 527-580. <https://doi.org/10.63125/0ef34271>
- [50]. Md Arif Uz, Z., Sharmin, S., & Md Abdur, R. (2025). Factors Influencing Behavioural Intention to Use the Innovative Open And Distance Learning Systems With The Role Of Continuance Intention. *American Journal of Scholarly Research and Innovation*, 4(01), 202-220. <https://doi.org/10.63125/pbjxp014>
- [51]. Md Ashfaq, S., & Abdullah Mohammad, S. (2022). CNT/PANI Composite Electrodes for Flexible Fiber-Shaped Dye-Sensitized Solar Cells: Synthesis, Characterization, and Photovoltaic Performance. *American Journal of Interdisciplinary Studies*, 3(02), 221-274. <https://doi.org/10.63125/m334mf41>

- [52]. Md Asif Ali Sheak, A. (2024). A Meta-Analysis of Agile and Lean Project Management Methodologies in Large-Scale Engineering and IT Integration Projects. *American Journal of Data Science and Analytics*, 5(12), 202-240. <https://doi.org/10.63125/6281tn40>
- [53]. Md Asif Ali Sheak, A., & Risha, A. (2022). The Role of IOT-Driven Energy Analytics in Improving Operational Efficiency and Sustainability in Modern Industrial Facilities. *American Journal of Interdisciplinary Studies*, 3(04), 807-841. <https://doi.org/10.63125/gm63q956>
- [54]. Md Kaium, H. (2023). A GIS-Based Multi-Criteria Decision-Support and Land-Suitability Optimization Framework for Climate-Resilient Urban and Regional Planning. *American Journal of Data Science and Analytics*, 4(06), 43-103. <https://doi.org/10.63125/wvq0sx87>
- [55]. Md Kaium, H. (2025). Integrating Artificial Intelligence, Semantic Indoor Geospatial Modeling, And Network-Based Routing for High-Precision NG911 Emergency Location Intelligence. *International Journal of Scientific Interdisciplinary Research*, 6(1), 616-670. <https://doi.org/10.63125/5hc1xx56>
- [56]. Md Kaium, H. (2026). An Artificial Intelligence Integrated Geospatial Decision-Support Framework for Scenario-Based Climate-Adaptive Land-Use Optimization and Environmental Risk Reduction. *American Journal of Data Science and Analytics*, 7(06), 425-483. <https://doi.org/10.63125/nyc7sh45>
- [57]. Md Mahamud Pervaz, P. (2025). Development of a CMMS-Integrated Predictive Maintenance Framework for Industrial PLC and Drive Systems. *American Journal of Scholarly Research and Innovation*, 4(01), 894-942. <https://doi.org/10.63125/j33gtf31>
- [58]. Md Mahamud Pervaz, P. (2026). Implementation of an OSHA-Compliant Lockout/Tagout and Arc-Flash Hazard Mitigation Framework for U.S. Industrial Maintenance Operations. *American Journal of Interdisciplinary Studies*, 7(02), 73-119. <https://doi.org/10.63125/8ky04n07>
- [59]. Md. Abdur, R., & Iftekhar, A. (2021). Customer Retention Forecasting in Mobile Wallet Services Using Neural Networks: A Comparative Quantitative Study. *International Journal of Business and Economics Insights*, 1(4), 70-102. <https://doi.org/10.63125/dyrpc387>
- [60]. Md. Rashedul, I., & Md Kaium, H. (2022). Development Of a Three-Dimensional Indoor Geospatial Network and Address Geocoding Framework for Next-Generation Emergency Dispatch and Response-Time Optimization. *Journal of Sustainable Development and Policy*, 1(02), 245-292. <https://doi.org/10.63125/tcw3mp48>
- [61]. Md. Shakhawat, H., & Md, F. (2024). Impact of Phishing Simulation Campaigns and Security Awareness Training on Human Risk Mitigation in Financial Institutions: A Quantitative Study. *American Journal of Data Science and Analytics*, 5(10), 48-85. <https://doi.org/10.63125/4j8h1484>
- [62]. Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). N-BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, 17(3), 12-22. <https://doi.org/10.1109/mprv.2018.03367731>
- [63]. Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: An ensemble of autoencoders for online network intrusion detection. Proceedings of the 2018 Network and Distributed System Security Symposium (NDSS 2018),
- [64]. Mohammad Abir Chowdhury, S. (2023). Role of AI-Assisted Risk Assessment in Enhancing Audit Planning Efficiency and Risk Prioritization in Public-Safety Organizations. *International Journal of Scientific Interdisciplinary Research*, 4(4), 529-576. <https://doi.org/10.63125/qd6nn437>
- [65]. Mohammad Abir Chowdhury, S. (2025). Application of Machine Learning and Anomaly-Detection Algorithms for Fraud Detection in U.S. Government Financial Operations. *American Journal of Interdisciplinary Studies*, 6(02), 139-184. <https://doi.org/10.63125/fkf19309>
- [66]. Mohammad Abir Chowdhury, S. (2026). Development Of a Machine-Learning Approach for Internal-Control Weakness Prediction and Audit-Risk Scoring In U.S. State Government Agencies. *American Journal of Data Science and Analytics*, 7(06), 380-424. <https://doi.org/10.63125/3v722074>
- [67]. Mohammad Abir Chowdhury, S., & Tonay, P. (2022). An Empirical Analysis of the Impact of Robotic Process Automation and Continuous Auditing on the Timeliness And Accuracy Of Financial Reporting Assurance. *International Journal of Business and Economics Insights*, 2(4), 73-126. <https://doi.org/10.63125/7p8dcr47>
- [68]. Mohammad Badrul, A. (2025). SCADA And IOT-Enabled Smart Water Metering: A Systematic Review of Resilient Supply Monitoring. *International Journal of Scientific Interdisciplinary Research*, 6(1), 576-615. <https://doi.org/10.63125/at8pnx81>
- [69]. Mohammad Badrul, A. (2026). A Machine-Learning Framework for Real-Time Non-Revenue Water Prediction in Aging Urban Distribution Networks. *American Journal of Interdisciplinary Studies*, 7(02), 01-52. <https://doi.org/10.63125/93km2h66>
- [70]. Mohammad Badrul, A., & Md. Mominul, H. (2023). Machine Learning-Based Assessment of Environmental and Public Health Risks in Sewerage Sludge Management Systems. *American Journal of Advanced Technology and Engineering Solutions*, 3(02), 33-77. <https://doi.org/10.63125/y3yfxa92>
- [71]. Mohammad Shoriful Hossan, S. (2022). A Performance-Based Framework for Arc-Flash Hazard Reduction and Electrical Reliability Improvement in Brownfield Industrial Distribution Systems. *Review of Applied Science and Technology*, 1(04), 447-463. <https://doi.org/10.63125/a70vj720>
- [72]. Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). 2015 Military Communications and Information Systems Conference (MilCIS),
- [73]. Muhammad Zahidul, I. (2023). Comparative Analysis of Machine-Learning Approaches for Pharmaceutical Sales Forecasting and Market-Demand Prediction. *Review of Applied Science and Technology*, 2(02), 38-95. <https://doi.org/10.63125/etcbqf13>

- [74]. Nishat, J. (2025). Leveraging Machine Learning to Identify and Address Maternal Health Disparities in Underserved U.S. Communities. *American Journal of Data Science and Analytics*, 6(12), 125-169. <https://doi.org/10.63125/c2t7r719>
- [75]. Nishat, J. (2026). Predictive Analytics for Program Effectiveness: A Machine Learning Approach to Health Education Programs in the United States. *American Journal of Health and Medical Sciences*, 7(03), 30-56. <https://doi.org/10.63125/2vw42878>
- [76]. Nishat, J., & Jahanara, A. (2024). Machine Learning Approaches for Early Prediction of High-Risk Pregnancy in Underserved U.S. Populations. *American Journal of Interdisciplinary Studies*, 5(04), 268-309. <https://doi.org/10.63125/5gh5df13>
- [77]. Nishat, J., & Mst Kaniz, F. (2022). A Review of the Impact of Covid-19 On Maternal and Child Health Service Utilization in Bangladesh. *American Journal of Scholarly Research and Innovation*, 1(02), 223-269. <https://doi.org/10.63125/vgv5s742>
- [78]. Nuzhat Sadia, P. (2025). Integrating Business Intelligence Dashboards for Real-Time Supply Chain Visibility and Operational Decision Support. *American Journal of Data Science and Analytics*, 6(12), 170-216. <https://doi.org/10.63125/1es4f763>
- [79]. Nuzhat Sadia, P. (2026). An Integrated IT Management Framework for Scenario-Based Enterprise Analytics and Strategic Decision Optimization. *American Journal of Interdisciplinary Studies*, 7(02), 120-168. <https://doi.org/10.63125/3wtc3z49>
- [80]. Patcha, A., & Park, J.-M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks*, 51(12), 3448-3470. <https://doi.org/10.1016/j.comnet.2007.02.001>
- [81]. Pietraszek, T., & Tanner, A. (2005). Data mining and machine learning: Towards reducing false positives in intrusion detection. *Information Security Technical Report*, 10(3), 169-183. <https://doi.org/10.1016/j.istr.2005.07.001>
- [82]. Reyes-Dorta, N., Caballero-Gil, P., & Rosa-Remedios, C. (2024). Detection of malicious URLs using machine learning. *Wireless Networks*, 30, 7543-7560. <https://doi.org/10.1007/s11276-024-03700-w>
- [83]. Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. *Computers & Security*, 86, 147-167. <https://doi.org/10.1016/j.cose.2019.06.005>
- [84]. Rony, S., & Md, A. (2026). Multi-Agency Coordination in Sustained Healthcare Supply Shortages: Lessons from Covid-19, Drug Shortages, and Critical Medical Supply Disruptions. *American Journal of Data Science and Analytics*, 7(01), 181-221. <https://doi.org/10.63125/5v6t8515>
- [85]. Sadia, Z. (2025). Predictive Analytics for Financial Performance Forecasting and Reporting Quality: Evidence from Data-Driven Financial Management Systems. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), 2795-2812. <https://doi.org/10.63125/zstqn346>
- [86]. Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning based phishing detection from URLs. *Expert Systems with Applications*, 117, 345-357. <https://doi.org/10.1016/j.eswa.2018.09.029>
- [87]. Sarker, I. H. (2023). Machine learning for intelligent data analysis and automation in cybersecurity: Current and future prospects. *Annals of Data Science*, 10, 1473-1498. <https://doi.org/10.1007/s40745-022-00444-2>
- [88]. Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). IntruDTree: A machine learning based cyber security intrusion detection model. *Symmetry*, 12(5), 754. <https://doi.org/10.3390/sym12050754>
- [89]. Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*, 7, 41. <https://doi.org/10.1186/s40537-020-00318-5>
- [90]. Shaiful, M., Anisur, R., & Md, A. (2022). A Systematic Literature Review on the Role of Digital Health Twins in Preventive Healthcare For Personal and Corporate Wellbeing. *American Journal of Interdisciplinary Studies*, 3(04), 1-31. <https://doi.org/10.63125/negjw373>
- [91]. Sharafaldin, I., Habibi Lashkari, A., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. *Proceedings of the 4th International Conference on Information Systems Security and Privacy*,
- [92]. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2(1), 41-50. <https://doi.org/10.1109/tetci.2017.2772792>
- [93]. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. 2010 IEEE Symposium on Security and Privacy,
- [94]. Staudemeyer, R. C. (2015). Applying long short-term memory recurrent neural networks to intrusion detection. *South African Computer Journal*, 56, 136-154. <https://doi.org/10.18489/sacj.v56i1.248>
- [95]. Sun, N., Zhang, J., Rimba, P., Gao, S., Zhang, L. Y., & Xiang, Y. (2019). Data-driven cybersecurity incident prediction: A survey. *IEEE Communications Surveys & Tutorials*, 21(2), 1744-1772. <https://doi.org/10.1109/comst.2018.2885561>
- [96]. Tonay, P. (2025). Machine Learning for Fraud Detection in Enterprise Financial Systems. *American Journal of Advanced Technology and Engineering Solutions*, 1(02), 304-318. <https://doi.org/10.63125/d0fhp873>
- [97]. Tonay, P. (2026). The Role of AI-Based Decision Support in Financial Risk Management and Anomaly Detection. *American Journal of Data Science and Analytics*, 7(06), 327-359. <https://doi.org/10.63125/wnb54w77>
- [98]. Tonay, P., Md Maruf, I., & Al, A. (2024). Artificial Intelligence-Based Decision Support Systems and Managerial Performance. *American Journal of Advanced Technology and Engineering Solutions*, 4(04), 154-184. <https://doi.org/10.63125/wmz8dc67>
- [99]. Tsai, C.-F., Hsu, Y.-F., Lin, C.-Y., & Lin, W.-Y. (2009). Intrusion detection by machine learning: A review. *Expert Systems with Applications*, 36(10), 11994-12000. <https://doi.org/10.1016/j.eswa.2009.05.029>
- [100]. Vaitkevicius, P., & Marcinkevicius, V. (2020). Comparison of classification algorithms for detection of phishing websites. *Informatica*, 31(1), 143-160. <https://doi.org/10.15388/20-infor404>

- [101]. Vanhoenshoven, F., Napoles, G., Falcon, R., Vanhoof, K., & Koppen, M. (2016). Detecting malicious URLs using machine learning techniques. 2016 IEEE Symposium Series on Computational Intelligence (SSCI),
- [102]. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE Access*, 7, 41525-41550. <https://doi.org/10.1109/access.2019.2895334>
- [103]. Vourganas, I. J., & Michala, A. L. (2024). Applications of machine learning in cyber security: A review. *Journal of Cybersecurity and Privacy*, 4(4), 972-992. <https://doi.org/10.3390/jcp4040045>
- [104]. Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *IEEE Access*, 6, 35365-35381. <https://doi.org/10.1109/access.2018.2836950>
- [105]. Ye, Y., Li, T., Adjeroh, D., & Iyengar, S. S. (2017). A survey on malware detection using data mining techniques. *ACM Computing Surveys*, 50(3), Article 41, 41-40. <https://doi.org/10.1145/3073559>
- [106]. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access*, 5, 21954-21961. <https://doi.org/10.1109/access.2017.2762418>
- [107]. Zhang, C., Jia, D., Wang, L., Wang, W., Liu, F., & Yang, A. (2022). Comparative research on network intrusion detection methods based on machine learning. *Computers & Security*, 121, 102861. <https://doi.org/10.1016/j.cose.2022.102861>
- [108]. Zhang, Z., & Shen, H. (2005). Application of online-training SVMs for real-time intrusion detection with different considerations. *Computer Communications*, 28(12), 1428-1442. <https://doi.org/10.1016/j.comcom.2005.01.014>