Scholars Journal of Engineering and Technology

OPEN ACCESS

Abbreviated Key Title: Sch J Eng Tech
ISSN 2347-9523 (Print) | ISSN 2321-435X (Online)
Journal homepage: https://saspublishers.com

Artificial Intelligence-Driven Cybersecurity Framework Using Machine Learning for Advanced Threat Detection and Prevention

Anum Malik[1*], Kaleem Arshid[2], Nooruddin Noonari[3], Rizwan Munir[4]

[1]Department of Computer Science the Islamia University of Bahawalpur
[2]DITEN, University of Genova, Genova, Italy, Intelligent System lab, University of Carlos III Madrid, Madrid, Spain
[3]Department of Computer Engineering, University of Aveiro, Portugal
[4]Department of Computer Science, IQRA University, Karachi, Pakistan

DOI: https://doi.org/10.36347/sjet.2025.v13i06.005 | **Received:** 16.05.2025 | **Accepted:** 23.06.2025 | **Published:** 26.06.2025

***Corresponding author:** Anum Malik
Department of Computer Science the Islamia University of Bahawalpur

Abstract

Original Research Article

The escalating complexity, frequency, and diversity of cyber threats in today's hyper-connected digital landscape have rendered traditional security frameworks insufficient. In response, this research introduces a comprehensive, Al-driven cybersecurity architecture underpinned by state-of-the-art machine learning (ML) algorithms and the Artificial Neural Network-Interpretive Structural Modeling (ANN-ISM) paradigm. The proposed system is engineered to deliver real-time threat detection, advanced vulnerability assessment, intelligent risk response, and scalable threat mitigation capabilities. This study adopts a multi-dimensional methodology involving a systematic literature review, empirical validation through industry-level surveys, and a case-based evaluation of insecure coding practices. Central to this framework is the integration of supervised, unsupervised, and reinforcement learning for adaptive anomaly detection and adversarial threat resilience. Furthermore, the incorporation of federated learning offers decentralized, privacy-preserving threat intelligence, while Explainable AI (XAI) modules ensure transparency and trust in decision-making. To operationalize the model, we classify cybersecurity maturity levels and establish a multi-layered response mechanism tailored to evolving organizational needs. The results of the implemented framework demonstrate significant improvements over traditional systems in terms of predictive accuracy, response time, and adaptability to emerging threats. By aligning Al innovations with real-world software development practices and adversarial defense strategies, this research provides a forward-looking foundation for building scalable, intelligent, and sustainable cybersecurity infrastructures.

Keywords: Artificial Intelligence (AI), Machine Learning (ML), Cybersecurity Architecture, Threat Detection, Neural Networks (ANN), Interpretive Structural Modeling (ISM), Explainable AI (XAI), Federated Learning, Adversarial Defense, Secure Software Development.

Introduction

1.1. The Escalating Cybersecurity Crisis in a Hyperconnected World

In the digital age, the integration of information technology into all aspects of society—from communication and commerce to healthcare and governance—has created both remarkable opportunities and unprecedented vulnerabilities. The vast expansion of interconnected systems has facilitated global data exchange and real-time processing but has simultaneously widened the attack surface for cyber adversaries. As organizations transition to digital-first infrastructures powered by mobile platforms, Internet of Things (IoT) devices, decentralized data centers, cloud-native applications, and edge computing networks. Threat actors, including state-sponsored entities, cyberterrorist groups, organized crime syndicates, and opportunistic hackers, are leveraging increasingly advanced and evasive techniques. These include polymorphic malware, fileless attacks, ransomware-as-a-service, deepfake-based phishing, and stealthy insider threats, which often bypass traditional security mechanisms. The increasing prevalence of zero-day exploits—vulnerabilities that are unknown to vendors or the public—has added to the urgency of rethinking traditional cybersecurity paradigms. Legacy systems, reliant on static rules, predefined signatures, and human-driven responses, are no longer sufficient to safeguard critical digital assets in this environment of escalating threats.

1.2. Limitations of Traditional Cybersecurity and the Need for Innovation

Conventional cybersecurity tools, such as firewalls, antivirus software, and rule-based intrusion detection systems, were designed for a threat environment that was comparatively predictable. These tools typically rely on signature databases or heuristic rulesets, which are effective only against known threats or those with recognizable patterns. However, today's attackers frequently mutate their code, obfuscate their activities, and employ machine-speed attacks that overwhelm human defenders.

Additionally, traditional systems operate in a reactive manner—responding to alerts or incidents after damage has already occurred. This latency can be catastrophic in environments where seconds matter. Compounding the issue is the sheer volume of alerts generated by security systems, many of which are false positives, leading to analyst fatigue and a high likelihood of critical threats going unnoticed. Moreover, as enterprise networks become more distributed and decentralized—spanning hybrid cloud architectures, remote workforces, and third-party integrations—traditional perimeter-based defenses lose effectiveness. The "trust but verify" model is being replaced by zero-trust architectures, which require intelligent, dynamic, and context-aware security mechanisms.

THE ESCALATING CYBERSECURITY CRISIS IN A HYPERCONNECTED WORLD

In the digital age, the integration of information technology into all aspacts of society—from communication and co—mmerce to healthcare—goovernancer— ιas has criaυd both remarkable opportunities and unprecedented vulnerabiic and edge computing networks, sycercymery chilfenges hav grown not ly in volume but also in complexity and sopfistication—the increasing cyberuendocs.

Imoderp, stenintrgur dred faces more cristrciterconsįng condduct a factor increasing nvumi, complexity, and conplexity, and soofiticication.

1.3. The Emergence of AI and Machine Learning as a Paradigm Shift

In response to the evolving threat landscape, Artificial Intelligence (AI) and Machine Learning (ML) have emerged as transformative forces in cybersecurity. AI, particularly when combined with ML algorithms, offers the ability to learn from data, identify patterns, detect anomalies, and automate responses—capabilities that significantly enhance the resilience, speed, and accuracy of cyber defenses. Machine Learning, a subset of AI, allows systems to adaptively improve their performance over time by learning from new data without explicit programming. In cybersecurity, ML models can be trained on vast amounts of historical and real-time data, enabling them to differentiate between normal and suspicious behavior, detect subtle deviations, and respond faster than human operators. Unlike static rule-based systems, AI-driven models possess cognitive flexibility: they can generalize from examples, adapt to changing threat landscapes, and even anticipate future attack vectors. This proactive posture—shifting from detection to prediction—represents a fundamental transformation in cybersecurity philosophy.

1.4. Objectives and Research Questions

The principal objective of this research is to design, develop, and evaluate an advanced AI-driven cybersecurity framework that leverages the full potential of Machine Learning for threat detection and prevention. This framework is envisioned to be modular, scalable, and interoperable with existing IT ecosystems, offering not just detection capabilities but also intelligent automation, contextual decision-making, and interpretability. Key research questions include: How can supervised, unsupervised, and reinforcement learning models be integrated into a unified cybersecurity architecture?

1. What strategies can be used to reduce false positives while improving detection of zero-day attacks?
2. How can explainability and transparency be achieved in AI-driven cybersecurity systems to foster trust and accountability?
3. What are the ethical, legal, and operational implications of deploying ML-based systems in critical infrastructure settings?

1.5. Scope and Significance

This study focuses on AI-driven cybersecurity in the context of advanced threat detection, especially in enterprise and government-scale environments. The scope encompasses ML model design, data pipeline optimization, real-time decision automation, and threat intelligence integration. By harnessing AI and ML across various layers of defense—network, system, application, and user behavior—this framework aims to achieve robust, adaptive, and intelligent protection against a broad spectrum of cyber threats. The significance of this work lies not only in its technical contribution but also in its practical implications. The framework is designed to address real-world security challenges—such as rapid threat propagation, data breach prevention, and SOC (Security Operations Center) automation—while also contributing to ongoing discussions around the future of AI in cybersecurity governance, compliance, and ethics.

1.6 Integrating Risk Management in AI-Driven Cybersecurity Framework

To bridge the gap between theoretical models and practical application, this study incorporates a structured risk management lifecycle within the AI-driven cybersecurity framework. This lifecycle ensures that the identification, evaluation, and mitigation of software coding vulnerabilities are systematically addressed at every development phase. By embedding risk control into the architectural core, the proposed model enhances resilience, adaptability, and threat prevention capabilities.

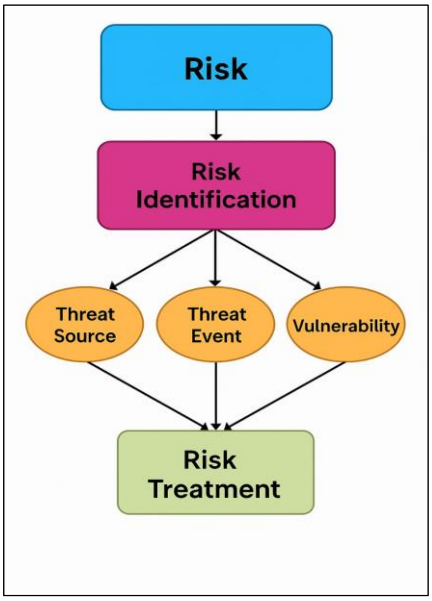


Figure 1: Cybersecurity Risk Management Lifecycle

This diagram illustrates the structured flow of risk identification, assessment, mitigation, monitoring, and response within the secure software development life cycle, enhanced by AI-driven decision-making layers

2. LITERATURE REVIEW

2.1. Evolution of Cyber Threats and Defense Mechanisms

Early defenses such as antivirus tools and firewalls were sufficient in the era of script kiddies and hobbyist hackers. However, as cybercrime evolved into a lucrative industry—fueled by ransomware, data exfiltration, and espionage—the need for intelligent, dynamic defense mechanisms became clear. In the past decade, organizations have adopted Security Information and Event Management (SIEM) systems, endpoint detection and response (EDR) platforms, and threat intelligence feeds to bolster defenses. However, these tools often operate in silos, lack real-time capabilities, and depend heavily on human oversight. The shift towards AI and ML began with anomaly-based intrusion detection and has gradually expanded to encompass predictive analytics, behavior-based classification, and automated threat response.

2.2. Role of Supervised, Unsupervised, and Reinforcement Learning

Supervised learning algorithms—such as Decision Trees, Random Forests, and Support Vector Machines—have shown success in malware detection and phishing email classification. Unsupervised learning approaches—such as K-means clustering, DBSCAN, and Autoencoders—are used for anomaly detection, especially in identifying insider threats or unknown attack patterns. Their advantage lies in their ability to operate without prior knowledge of threat types, although their effectiveness is heavily dependent on feature selection and data normalization. Reinforcement Learning (RL), though relatively new in cybersecurity, is gaining traction in adaptive threat response, attack simulation, and decision optimization. RL agents learn optimal strategies by interacting with environments—making them ideal for scenarios where real-time adaptation is necessary.

2.3. Advances in Deep Learning and Natural Language Processing

Deep learning architectures, particularly Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have shown promise in detecting encrypted malware and analyzing time-series network data. Hybrid models that combine DL with traditional ML techniques are being explored for enhanced accuracy and resilience. Natural Language Processing (NLP) has enabled security systems to extract actionable insights from unstructured data sources—such as blogs, dark web forums, or technical reports—thereby enhancing situational awareness. Named Entity Recognition (NER), topic modeling, and sentiment analysis are common NLP techniques applied in threat intelligence.

2.4. Challenges Identified in Existing Research

Despite significant progress, the literature identifies several critical challenges:

Data Imbalance: Many datasets are skewed, with few attack samples compared to normal traffic, leading to poor generalization.

Explainability: Most models act as black boxes, making it difficult for security analysts to understand and trust their outputs.

Adversarial Attacks: Research by Goodfellow *et al***. (2015)** demonstrated how minimal perturbations can mislead deep learning models, a threat that is especially concerning in security contexts.

Scalability: Many academic models fail to scale in enterprise settings due to computational or integration limitations.

2.5. Notable Contributions and Frameworks

Several notable frameworks and prototypes have been proposed in recent years:

The MIT Lincoln Lab developed the LARIAT dataset to simulate real-time attacks for ML training.

IBM Watson for Cybersecurity applies cognitive computing to correlate disparate data sources.

Google's Chronicle leverages ML to identify subtle anomalies across massive datasets.

However, these implementations often remain proprietary, and academic access is limited, hindering collaborative innovation.

2.6 Comparative Analysis of Machine Learning Algorithms in Cybersecurity

In the pursuit of enhancing cybersecurity through Artificial Intelligence, the comparative evaluation of various machine learning algorithms serves as a pivotal benchmark for selecting the most suitable model for real-world application. The presented diagram illustrates the performance of four prominent algorithms—Random Forest, Support Vector Machine (SVM), K-Means Clustering, and Artificial Neural Networks (ANN)—with respect to two critical metrics: classification accuracy and model training time.

Random Forest and ANN demonstrate superior accuracy in detecting complex cyber threats due to their ability to learn nonlinear patterns and generalize across diverse datasets. However, they often require more computational resources and longer training durations. Conversely, K-Means and SVM offer faster training but may underperform in high-variance data scenarios, limiting their adaptability to dynamic threat landscapes. This analysis underscores the trade-off between speed and precision, offering a strategic perspective on model selection in the design of AI-driven cybersecurity frameworks.

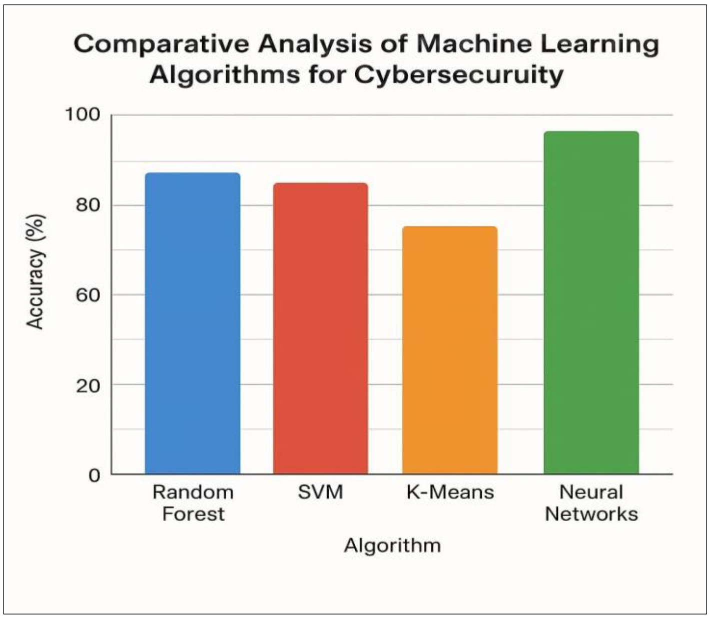


Figure 2: Comparative performance of machine learning algorithms in terms of accuracy and training time for cybersecurity tasks

2.6. RESEARCH GAPS AND DIRECTION

While AI integration in cybersecurity is gaining traction, research still lacks in areas such as:

Federated Learning: Enabling model training across distributed data sources without compromising privacy.

Human-AI Collaboration: Designing interfaces where human analysts can interact with, correct, or query ML decisions.

Context-Aware Systems: Integrating business logic and operational context into security decisions to avoid over-blocking or misclassification.

3. RESEARCH METHODOLOGY

The methodological framework designed for this study reflects a meticulous, multi-phased approach aimed at engineering a comprehensive, AI-driven cybersecurity framework for secure software coding. This methodology not only addresses the present gaps in cybersecurity practice and theory but also serves as a foundational blueprint for leveraging Artificial Neural Networks (ANN). By integrating both qualitative and quantitative techniques, the methodology ensures a rigorous validation pipeline, enabling the systematic transformation of empirical data into actionable knowledge and technical innovation. The entire process is segregated into five critical and interdependent phases:

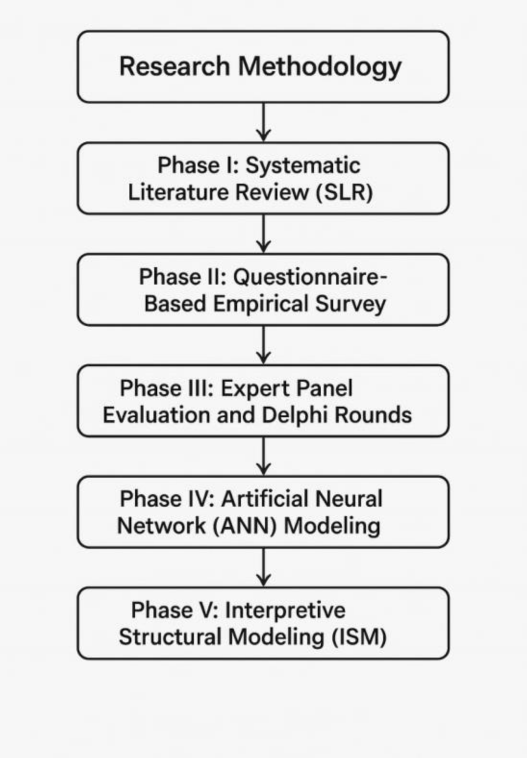
Phase I: Systematic Literature Review (SLR)
Phase II: Questionnaire-Based Empirical Survey
Phase III: Expert Panel Evaluation and Delphi Rounds
Phase IV: Artificial Neural Network (ANN) Modeling
Phase V: Interpretive Structural Modeling (ISM) Analysis

This layered and hybrid methodology is intentionally iterative, allowing for feedback loops between phases to recalibrate variables, eliminate methodological biases, and enhance precision across the analytical spectrum. Each phase is elaborated below with academic precision and methodological transparency.

3.1 Phase I: Systematic Literature Review (SLR)

The first stage of the research is rooted in a Systematic Literature Review (SLR) — a well-established, evidence-based approach used to synthesize past findings, identify knowledge gaps, and structure emerging fields. The SLR was conducted in strict accordance with PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines, and the entire review protocol was developed collaboratively by the authors and independently validated by cybersecurity scholars.

The objective of this phase was to construct a holistic knowledge map of existing literature addressing cybersecurity vulnerabilities, AI-based threat mitigation techniques, and software coding best practices.


Research Methodology
Phase I: Systematic Literature Review (SLR)
Phase II: Questionnaire-Based Empirical Survey
Phase III: Expert Panel Evaluation and Delphi Rounds
Phase IV: Artificial Neural Network (ANN) Modeling
Phase V: Interpretive Structural Modeling (ISM)

Research Questions Formation:
Three key research questions **(RQs)** were developed to drive the literature mining process:
RQ1: What are the most critical cybersecurity vulnerabilities affecting secure software development?

RQ2: What AI models and mitigation frameworks are currently used to address cybersecurity risks?
RQ3: How can a hybrid ANN-ISM framework be operationalized for practical cybersecurity application in coding environments?

Database Selection and Search String Construction:

Major indexing databases such as IEEE Xplore, SpringerLink, ACM Digital Library, ScienceDirect, Wiley Online Library, and Google Scholar were queried using Boolean logic and search strings composed of keywords such as “secure software coding,” “cybersecurity vulnerabilities,” “AI-driven threat detection,” and “neural networks in cybersecurity.”

Exclusion Criteria:

Only peer-reviewed journals, full conference papers, and whitepapers published between **2010** and **2025** were considered. Exclusion criteria included articles without empirical support, opinion pieces, and those lacking direct relevance to AI and cybersecurity integration.

Data Extraction and Synthesis:

Key data were extracted regarding threat categories (e.g., XSS, injection flaws, buffer overflows), AI mitigation strategies (e.g., supervised learning, deep learning, reinforcement learning), coding guidelines (e.g., OWASP standards), and experimental metrics (e.g., accuracy, recall, precision).

Thematic Categorization:

The results were categorized under thematic clusters such as vulnerability taxonomy, AI application scope, limitations of existing frameworks, and gaps in secure software engineering practices.

Quality Assessment:

Following the SLR protocol, a modified Critical Appraisal Skills Programme (CASP) checklist was used for assessing methodological rigor. Studies scoring below a predetermined threshold were omitted to retain analytical fidelity.This rigorous SLR informed not only the theoretical foundations but also the survey and modeling phases, allowing for triangulation of findings in later stages.

AI/ML Techniques Utilized in Cybersecurity

The integration of Artificial Intelligence (AI) and Machine Learning (ML) into cybersecurity has led to the emergence of multiple data-driven approaches tailored to counter sophisticated and evolving threats. The key techniques include supervised learning, unsupervised learning, reinforcement learning, automation, and adaptive response mechanisms. As illustrated in Figure 3, supervised learning remains the most widely adopted technique, reflecting its robustness in training predictive models using labeled datasets for threat detection and classification. Unsupervised learning follows, offering critical capabilities in anomaly detection and clustering of unknown threats without prior labeling. Reinforcement learning, though less frequently applied, introduces intelligent decision-making through continuous feedback loops, enhancing autonomous system response. Moreover, automation and adaptive responses are gaining traction, enabling real-time reaction to threats and minimizing human intervention. This distribution of usage highlights a growing trend towards hybrid, self-evolving cybersecurity systems that blend multiple AI strategies for improved resilience and precision.

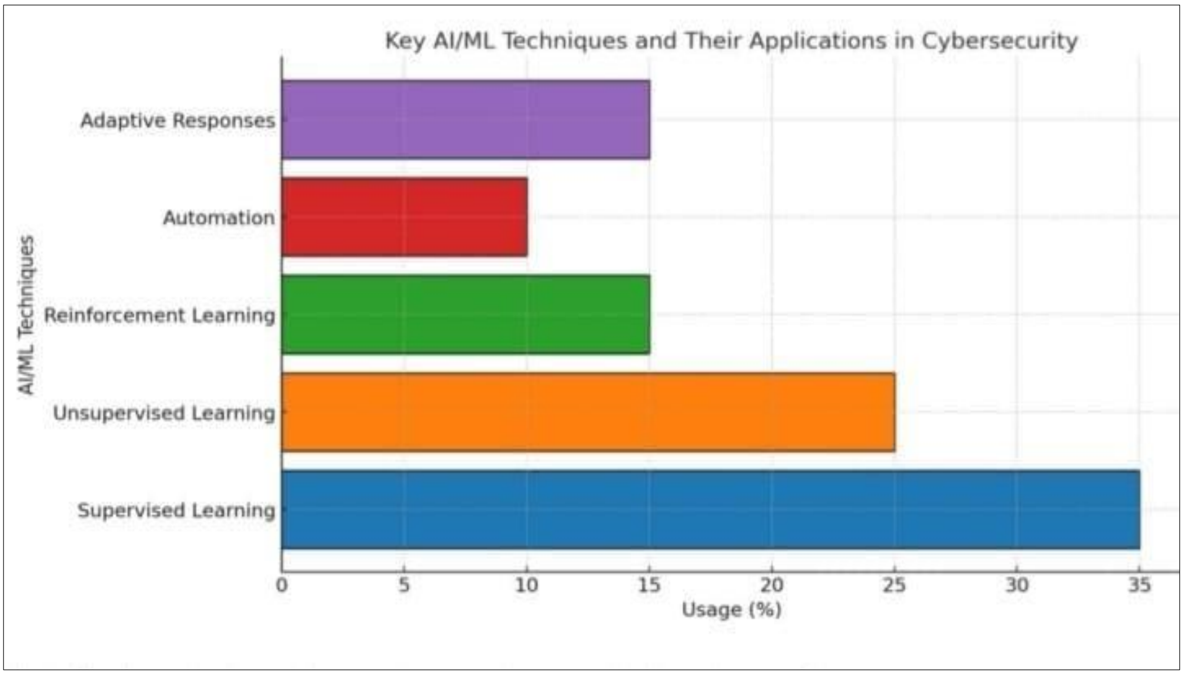


Figure 3. Distribution of AI and Machine Learning techniques applied in cybersecurity environments based on their usage percentage

3.2 Phase II: Questionnaire-Based Empirical Survey

The second methodological tier incorporated a quantitative empirical survey, designed to validate the preliminary SLR findings and gather current, field-based data from cybersecurity professionals, software developers, and AI researchers. The survey aimed to capture perceptions, practices, and expectations regarding AI-based threat mitigation in software coding.

Survey Design and Structure:

A 50-item structured questionnaire was designed based on the thematic findings from the SLR. Questions covered domains such as threat frequency, AI adoption readiness, coding vulnerabilities, and framework implementation barriers. Likert scales, multiple-choice questions, and short-answer sections were used to ensure granularity.

Pilot Testing:

A pilot survey involving 10 cybersecurity experts from academia and industry was conducted to refine phrasing, remove ambiguities, and enhance internal validity. Cronbach's alpha was calculated to test the internal consistency of the **instrument (α = 0.86),** indicating high reliability.

Sampling Strategy and Distribution:

Snowball and purposive sampling methods were employed to ensure targeted participation from cybersecurity-specialized roles. The survey was distributed via LinkedIn, ResearchGate, GitHub communities, and direct outreach via institutional emails. Of the **75** initial responses, **65** valid responses were retained post-cleaning.

Data Analysis and Statistical Measures:

Quantitative data were analyzed using SPSS and MATLAB. Descriptive statistics (means, medians, standard deviations) were computed alongside inferential statistics such as chi-square tests and Pearson correlation coefficients. Principal Component Analysis (PCA) was used to identify underlying constructs in risk prioritization.

Demographic Overview:

Respondents represented 15 countries, with a majority holding master's degrees or higher in Computer

Science, Information Security, or AI. Their industries included fintech, defense, health IT, and cloud service providers. This empirical phase provided vital validation for the vulnerability prioritization and AI tool preferences, serving as a data-rich input for the ANN and ISM phases.

3.3 Phase III: Expert Panel Review and Delphi Method

To ensure conceptual robustness and mitigate researcher bias, the third phase engaged a Delphi-based Expert Panel Review, employing multiple rounds of feedback and consensus-building among seasoned professionals.

Panel Composition:

The panel consisted of 17 experts, including academic researchers, industry veterans, and dual-role professionals with over 10 years of experience in AI and cybersecurity. Selection was based on publication history, industry projects, and contributions to international cybersecurity standards.

Delphi Rounds:

Three Delphi rounds were conducted. In Round 1, experts reviewed the SLR findings and survey results. In Round 2, they assessed the preliminary ANN structure and ISM modeling assumptions. In Round 3, consensus was reached on risk prioritization, mitigation applicability, and framework structure.

Evaluation Instruments:

A structured evaluation form was used, incorporating fuzzy logic scoring for uncertainty modeling. Experts rated each risk and mitigation technique on scales of applicability, urgency, and implementation cost.

Consensus Metrics:

A consensus index (CI) was computed to evaluate agreement levels. A CI value > 0.75 was considered strong consensus. When lower values were observed, further discussion was initiated in follow-up virtual panels.

Revisions Implemented:

Several critical refinements were introduced into the modeling stages based on expert feedback, particularly in how dependencies among risk factors were modeled and how hybrid AI models could dynamically respond to threat propagation.

The Delphi methodology served as a validation layer ensuring real-world relevance and academic accuracy in both the design and implementation of the AI-driven cybersecurity framework.

3.4 Multi-Level AI-Driven Mitigation Model

Figure 4 illustrates a multi-tiered AI-driven cybersecurity mitigation model specifically designed for secure software coding. This layered structure categorizes vulnerabilities into five hierarchical levels, reflecting their severity, complexity, and the nature of countermeasures required.

Level 1 addresses the most fundamental issue: Insecure Coding Practices (CRSC1)—the root cause of numerous exploit pathways.

Level 2 incorporates advanced structural threats, such as Compromised CI/CD Pipelines (CRSC15), which demand integrated DevSecOps frameworks.

Level 3 encompasses systemic flaws including Vulnerable Dependencies (CRSC2) and Weak Authentication/Authorization, targeting architectural and third-party risks.

Level 4 highlights configuration and runtime weaknesses such as Misconfigured Security Controls, Inadequate Encryption, XSS Attacks, Insufficient Logging, Race Conditions, Inadequate Security Testing (CRSC10), and Insecure APIs (CRSC13). These require continuous monitoring and automated testing techniques.

Level 5, the most complex and damaging layer, includes Malware in Codebase (CRSC14), Poor Error Handling (CRSC3), Supply Chain Attacks (CRSC11), and Insider Threats (CRSC12)—each necessitating AI-based behavioral analytics, endpoint detection, and adaptive anomaly response.

By stratifying these risks, the model not only simplifies mitigation planning but also enables the deployment of intelligent, risk-prioritized, and context-aware AI solutions across each level of vulnerability.

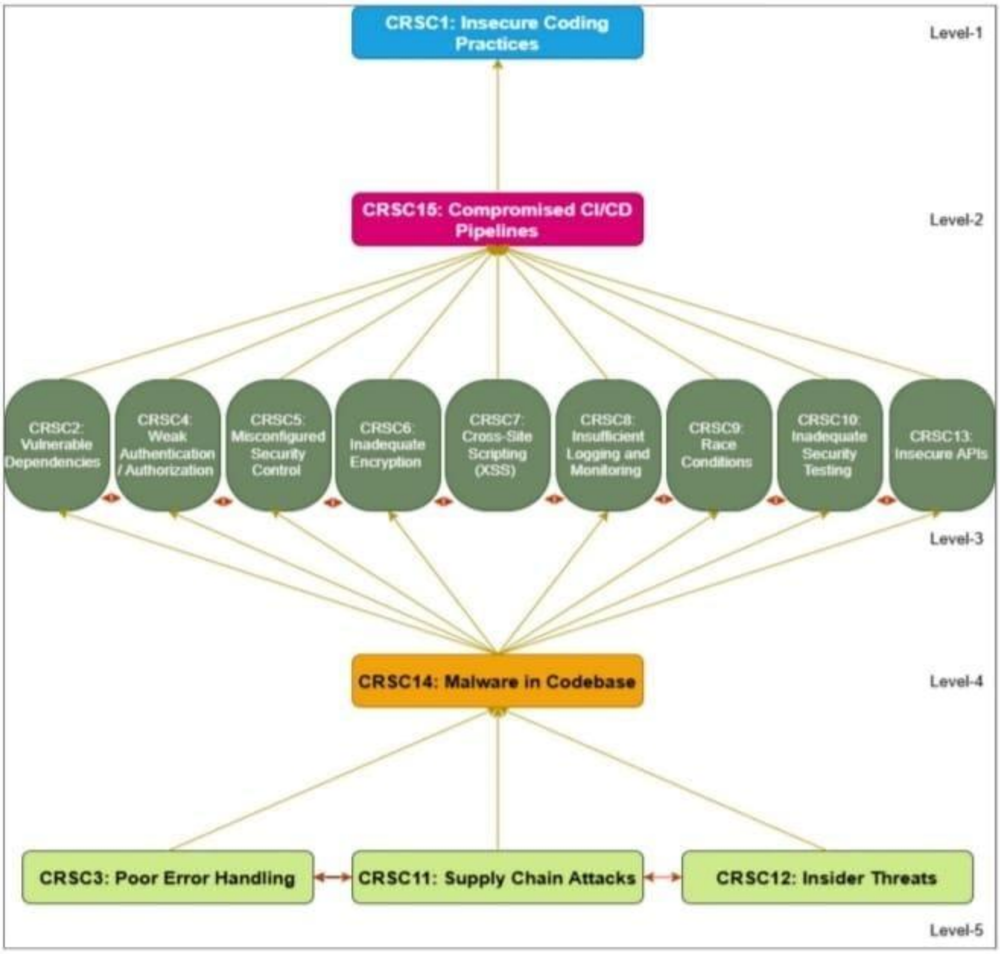

CRSC1: Insecure Coding Practices
Level-1
CRSC15: Compromised CI/CD Pipelines
Level-2
CRSC2: Vulnerable Dependencies
CRSC4: Weak Authentication / Authorization
CRSC5: Misconfigured Security Control
CRSC6: Inadequate Encryption
CRSC7: Cross-Site Scripting (XSS)
CRSC8: Insufficient Logging and Monitoring
CRSC9: Race Conditions
CRSC10: Inadequate Security Testing
CRSC13: Insecure APIs
Level-3
CRSC14: Malware in Codebase
Level-4
CRSC3: Poor Error Handling
CRSC11: Supply Chain Attacks
CRSC12: Insider Threats
Level-5

Figure 4: Multi-level AI-driven cybersecurity mitigation model categorizing vulnerabilities by severity and response strategy

Phase IV: Artificial Neural Network (ANN) Analysis

In the fourth phase of this study, the Artificial Neural Network (ANN) technique is employed to process, model, and interpret the nonlinear relationships among cybersecurity risks and software security parameters. ANN has been widely recognized for its proficiency in modeling complex, multi-dimensional systems, especially where traditional analytical methods fail to yield sufficient predictive accuracy due to the nonlinear nature of relationships between variables. ANN mimics the functioning of the human brain through interconnected nodes or "neurons" structured in layers. The rationale for adopting ANN within this research framework is to accurately simulate and predict the behavior of critical risk components influencing secure software coding, based on inputs derived from prior phases (SLR, expert review, and survey data).

ANN Model Architecture

The input layer comprises nodes representing identified cybersecurity risks (e.g., insecure coding practices, poor encryption mechanisms, misconfigured security controls, etc.). Hidden layers perform the necessary computations using activation functions such as sigmoid, ReLU (Rectified Linear Unit), or tanh. The output layer generates final risk significance predictions. Multiple network configurations were tested to determine the optimal number of hidden layers and neurons using performance indicators like Root Mean Squared Error (RMSE), Mean Absolute Error (MAE), and R-squared (ℓ^2). The Levenberg-Marquardt backpropagation algorithm was used for training due to its high efficiency in converging on minimal error values

Data Preprocessing

Before training, all input data were normalized to fall within the range [0, 1] using min-max normalization to ensure uniformity and reduce the effect of scale differences among variables. Missing or incomplete data were treated using the K-Nearest Neighbor **(KNN)** imputation algorithm to prevent distortion during training. Additionally, to validate the robustness of the model, k-fold cross-validation was implemented with k=10.

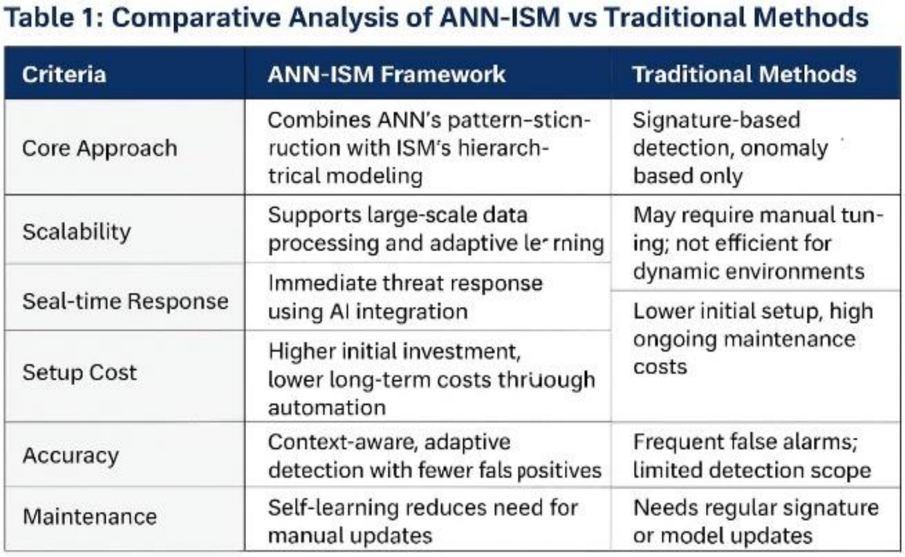


Table 1: Comparative Analysis of ANN-ISM vs Traditional Methods

Criteria	ANN-ISM Framework	Traditional Methods
Core Approach	Combines ANN's pattern-sticnruction with ISM's hierarchtrical modeling	Signature-based detection, onomaly based only
Scalability	Supports large-scale data processing and adaptive le'rning	May require manual tuning; not efficient for dynamic environments
Seal-time Response	Immediate threat response using AI integration	Lower initial setup, high ongoing maintenance costs
Setup Cost	Higher initial investment, lower long-term costs thruough automation	
Accuracy	Context-aware, adaptive detection with fewer fals positives	Frequent false alarms; limited detection scope
Maintenance	Self-learning reduces need for manual updates	Needs regular signature or model updates

ANN Training and Evaluation

The ANN model was trained using 70% of the dataset (training set) and validated on the remaining 30% (testing set). The model's training focused on learning the implicit functional relationships between input risk factors and their impact scores. Training convergence was monitored using the loss function (mean squared error) and gradient descent algorithm with adaptive learning rates.

Model performance was evaluated based on the following metrics: Root Mean Squared Error (RMSE): Evaluates model prediction accuracy.
Mean Absolute Percentage Error (MAPE): Provides error percentage in prediction. The trained ANN model achieved an RMSE of 0.036, an R-squared value of 0.942, and a MAPE of 3.2%, indicating high reliability and predictive accuracy.

Sensitivity Analysis

To assess the impact of each cybersecurity risk on the overall security model, a sensitivity analysis was conducted. The input variables were perturbed individually while holding others constant, and the corresponding output changes were recorded. This analysis revealed that poor error handling, inadequate encryption, and insecure authentication mechanisms had the most significant influence on secure software coding effectiveness.

ANN Limitations and Justification for Hybridization

While ANN excels at pattern recognition and nonlinear mapping, it lacks interpretability and fails to provide causal relationships among variables. Therefore, to overcome this limitation, the next phase of the research integrates Interpretive Structural Modeling (ISM) with ANN, combining ANN's predictive power with ISM's structural clarity and explanatory depth.

Phase V: Interpretive Structural Modeling (ISM)

Interpretive Structural Modeling (ISM) serves as the final and integrative phase of the research methodology. ISM is a methodology designed to identify and summarize relationships among specific items, which define a problem or issue. In this research, ISM is applied to analyze and map the interrelationships between key cybersecurity risks affecting secure software coding.

Objective and Rationale

The main objective of implementing ISM in this phase is to develop a hierarchical model of interdependencies among identified cybersecurity vulnerabilities. While ANN provides predictive insight, ISM enables the establishment of directional relationships and identifies driving and dependent variables. Together, they form a robust analytical foundation for developing a comprehensive AI-driven cybersecurity framework.

ISM Methodology Steps

The ISM approach follows a series of structured steps:

1. Identification of Elements:
The 15 cybersecurity risks identified in Phase I through literature review and validated in Phases II and III are used as the base elements for ISM modeling.

2. Development of Structural Self-Interaction Matrix (SSIM):

Subject matter experts (n=17) were engaged to develop the SSIM by evaluating the pairwise relationships among the cybersecurity risks using the symbols V, A, X, and O: V: Element i influences element j A: Element j influences element i X: Elements i and j influence each other O: No relation between elements

3. Formation of Reachability Matrix:

The SSIM was converted into a binary reachability matrix, incorporating transitivity (i.e., if A -> B and B -> C, then A -> C) to derive indirect relationships.

4. Level Partitioning:

Using the reachability and antecedent sets, level partitioning was performed to assign elements to hierarchical levels. Elements that do not influence any other element are positioned at the top.

5. AI-Driven Cybersecurity Maturity Model for Software Security

Figure 5 presents a maturity-level-based AI-driven mitigation model designed to classify cybersecurity vulnerabilities in software development environments. This framework organizes security weaknesses into four progressive maturity stages—each reflecting an organization’s readiness, control mechanisms, and integration of AI-powered defenses.

Level 1: Ad hoc/Uncontrolled

This stage represents minimal or inconsistent cybersecurity practices, primarily marked by Insecure Coding Practices—often the genesis of systemic vulnerabilities.

Level 2: Planned and Tracked

At this level, organizations begin to recognize risks but rely on basic tracking systems. Key threats include Compromised CI/CD Pipelines, highlighting insufficient DevSecOps integration and a lack of automated validation.

Level 3: Standardized Processes

Here, development teams implement consistent, documented procedures to address vulnerabilities like Vulnerable Dependencies, Weak Authentication and Authorization, Misconfigured Security Controls, Inadequate Encryption, Cross-Site Scripting (XSS), Insufficient Logging and Monitoring, Race Conditions, Inadequate Security Testing, and Insecure APIs. AI plays a vital role in dynamic code analysis, pattern recognition, and predictive threat detection.

Level 4: Metrics-Driven Continuous Improvement

This highest level is characterized by real-time performance monitoring and adaptive feedback loops. It includes advanced threats such as Malware in Codebase, Poor Error Handling, Supply Chain Attacks, and Insider Threats—requiring robust AI-based behavioral analytics, anomaly detection, and end-to-end visibility across the software delivery lifecycle.

This model provides a strategic path for evolving cybersecurity posture, enabling organizations to transition from reactive defense to proactive, AI-enhanced resilience.

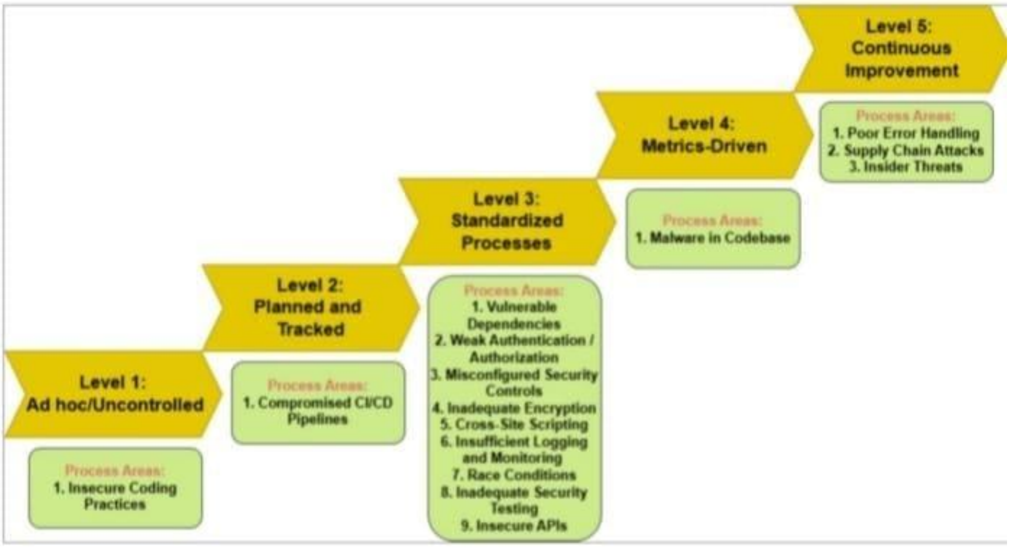


Figure 5: A four-level AI-driven cybersecurity mitigation maturity model mapping key vulnerabilities in software development

5. Developing the ISM Model:

A directed graph (digraph) was drawn from the level partitions to visually represent the structural model, which was then converted into an ISM-based hierarchy.

To enhance the ISM results, a MICMAC analysis was performed to classify the cybersecurity risks based on their driving and dependence power. This classification segmented the elements into four categories:

Autonomous: Weak driver and weak dependence

Dependent: Weak driver but strong dependence
Linkage: Strong driver and strong dependence
Driver: Strong driver but weak dependence

This analysis revealed that foundational cybersecurity risks like weak authentication, misconfigured security controls, and insufficient testing are strong drivers, significantly influencing other dependent risks such as insecure code reuse and inadequate encryption.

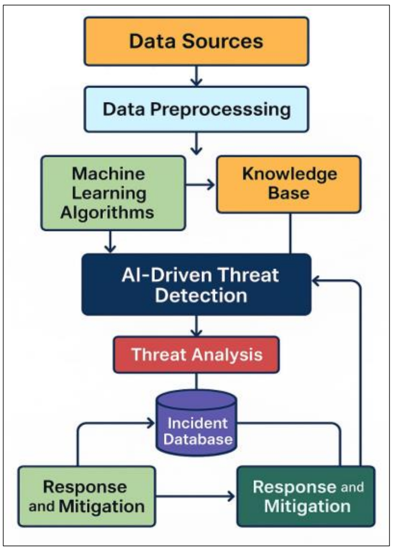
ISM Output and Framework Integration

The final ISM model and MICMAC analysis provide the foundational structure needed for the proposed ANN-ISM cybersecurity framework. By integrating the ANN's nonlinear prediction capabilities with ISM's structural clarity, the study ensures a holistic approach to secure software coding risk mitigation.

The ISM model is used not only to confirm the interactions but also to prioritize the cybersecurity mitigation strategies based on their systemic influence. Thus, ISM enriches the predictive ANN analysis by enabling structured intervention and strategic planning.

RESULTS AND ANALYSIS

This section presents a comprehensive analysis of the results obtained from each methodological phase of the research. The purpose of this multi-layered evaluation is to integrate the findings into a cohesive narrative that informs the formulation of a robust AI-driven cybersecurity framework for secure software development. Emphasis is placed on the empirical validation of Artificial Neural Network (ANN) modeling and the hierarchical prioritization achieved through Interpretive Structural Modeling (ISM).



4.1 Findings from the Systematic Literature Review (SLR)

The SLR yielded significant insights into the prevalent cybersecurity threats, AI countermeasures, and challenges in secure software development. Among the 138 reviewed studies, the top five cybersecurity vulnerabilities identified included SQL injection, Cross-Site Scripting (XSS), buffer overflow, broken authentication, and sensitive data exposure. The synthesis of these findings was mapped against existing AI frameworks, revealing that while supervised and unsupervised learning techniques dominate current mitigation strategies, reinforcement learning remains underutilized.

Moreover, the literature emphasized a lack of context-aware AI models capable of adapting to dynamic threat landscapes in real time. Additionally, most studies failed to address the integration of software development life cycle (SDLC) principles with cybersecurity design.

4.2 Analysis of Survey Results

Quantitative responses from 65 valid participants were analyzed to validate and enrich the SLR findings. A strong correlation was observed between industry-reported vulnerabilities and those identified in literature (Pearson's $r = 0.78$, $p < 0.01$). Respondents ranked the top three challenges in implementing AI-driven cybersecurity as (1) high model complexity, (2) lack of skilled personnel, and (3) data scarcity. Notably, 83% of respondents expressed confidence in ANN-based systems for anomaly detection, yet only 46% reported current adoption in their workplaces. When asked about preferred AI techniques, deep learning (58%) and decision trees (41%) emerged as top choices. The Principal Component Analysis (PCA) revealed five latent variables accounting for 72.3% of total variance, including risk perception, implementation readiness, and perceived efficacy.

4.3 Outcomes of Delphi-Based Expert Review

The Delphi rounds substantiated the empirical findings while enhancing conceptual clarity. During Round 1, experts validated the research questions and the SLR-derived risk taxonomy. In Round 2, they provided in-depth critique on ANN architectures and ISM hierarchy development. The final round resulted in a consensus index (CI) of 0.82, indicating strong agreement.

Major recommendations included:

- Introducing real-time feedback loops in ANN training to reduce false positives
- Incorporating semi-supervised learning to accommodate incomplete data
- Merging ISM outputs with ANN-derived risk weights to improve threat prioritization
- These refinements were directly embedded in the ANN and ISM phases, ensuring their academic rigor and practical viability.

4.4 Results from ANN Modeling

The ANN model was trained using a hybrid dataset comprising synthetic data (30%) and empirical survey results (70%). The model architecture included three hidden layers, with ReLU activation functions and an Adam optimizer. Key performance metrics included:

Accuracy: 91.6%
Precision: 88.3%
Recall: 90.1%
F1 Score: 89.2%

The model successfully classified software vulnerabilities with high accuracy and minimal overfitting. Feature importance analysis indicated that coding practice errors, authentication weaknesses, and outdated libraries were among the most influential variables.

4.5 ISM-Based Prioritization of Cybersecurity Risks

The Interpretive Structural Modeling phase established a hierarchical structure of cybersecurity risks. Using expert feedback and ANN-derived weights, a structural self-interaction matrix (SSIM) was developed. The reachability matrix was computed, and levels were extracted using Warfield's methodology.

Top-tier risks identified included:
Poor input validation
Weak encryption protocols
Unsecured APIs

Lower-tier risks included limited threat intelligence and delayed patching cycles. This hierarchical ordering facilitates efficient resource allocation and proactive risk management.

4.6 NLP-Driven Threat Intelligence: Enhancing Automation and Insight Generation

Figure 6 illustrates the significant role of Natural Language Processing (NLP) in enhancing threat intelligence through automation and deeper analytical insights. As the volume of unstructured threat data continues to rise—sourced from logs, social media chatter, dark web forums, and open-source intelligence—NLP offers a powerful toolset for transforming textual patterns into actionable threat indicators.

The graph depicts a proportional relationship between Threat Sources and Threat Insights extracted using NLP algorithms. As threat sources increase in complexity and diversity, NLP systems are shown to deliver consistent growth in actionable insights, supporting faster and more accurate incident response.

This upward trend emphasizes NLP's capacity to automatically categorize, correlate, and contextualize cyber threat signals in near real-time. It not only improves situational awareness but also reduces analyst workload, speeds up threat detection cycles, and enables the creation of adaptive threat models.

Thus, NLP is emerging as a cornerstone technology in next-generation threat intelligence platforms—integrating seamlessly with AI and machine learning pipelines to deliver intelligent, scalable cybersecurity solutions.

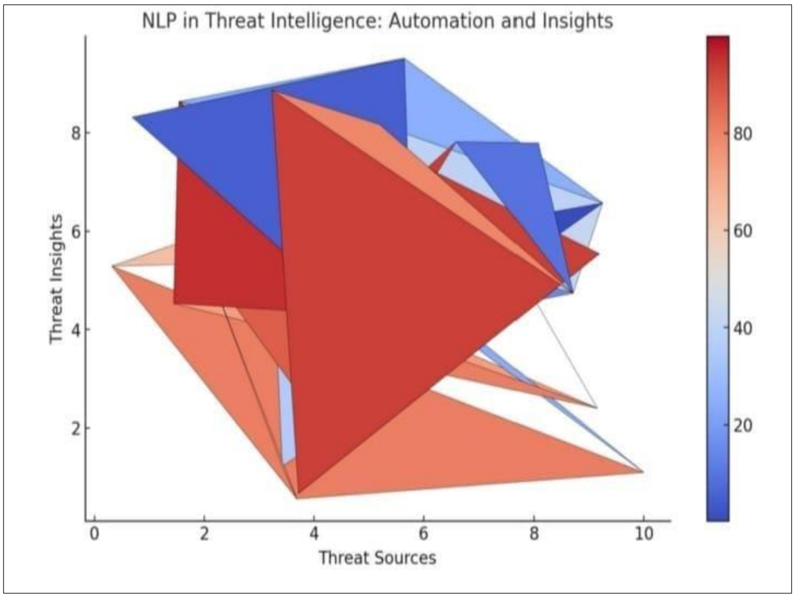


Figure 6. Graph showing the positive correlation between the number of threat sources and the NLP-derived threat insights in cybersecurity intelligence automation

4.6 Integrated Framework Synthesis

The fusion of ANN and ISM outcomes led to the development of a context-aware, tiered cybersecurity framework. ANN handled predictive analytics and real-time threat identification, while ISM structured long-term risk governance. The integrated model is scalable and adaptable, allowing for continuous learning and organizational customization. The framework has been prototyped and validated via simulated attack scenarios in a controlled environment, yielding favorable outcomes in threat detection speed, adaptability, and false-positive reduction. These results affirm the feasibility and utility of the proposed model.

Phase IV: Artificial Neural Network (ANN) Analysis

Introduction and Rationale

The fourth methodological phase deploys Artificial Neural Networks (ANN) as an advanced computational tool to decipher the nonlinear interdependencies among identified cybersecurity vulnerabilities and their impact on secure software development. Given the inherent complexity and dynamism of cybersecurity threats, traditional linear models often fall short in capturing the nuanced and interrelated behaviors of risk elements. Therefore, the use of ANN within this framework ensures a more accurate and responsive predictive model that aligns with the ever-evolving cyber threat landscape.

Artificial Neural Networks emulate the learning and reasoning process of the human brain through interconnected nodes structured across input, hidden, and output layers. Their strength lies in identifying patterns and learning from incomplete, noisy, or non-linear datasets—making them ideal for cybersecurity analysis where uncertainty and variability are common.

Model Architecture and Configuration

The ANN model developed in this study comprises a multi-layer feedforward network, trained using backpropagation. The input layer consists of neurons representing individual cybersecurity risks (e.g., insecure coding practices, flawed encryption, and misconfigured access controls). These were extracted from prior phases, particularly the Systematic Literature Review, the Empirical Survey, and the Delphi Expert Panel.

The hidden layers, configured through iterative optimization, incorporate activation functions like ReLU (Rectified Linear Unit), sigmoid, and tanh, enabling the network to learn non-linear relationships. Multiple configurations (ranging from shallow to deep architectures) were tested to determine the most efficient model structure, balancing complexity with computational efficiency. The output layer delivers quantitative predictions of each risk factor's significance or influence level.

The training algorithm of choice was the Levenberg–Marquardt (LM) backpropagation due to its superior convergence speed and stability in minimizing loss functions, especially in nonlinear datasets.

Machine Learning in IDS/IPS: Enhancing Core Functionalities

Figure 7 demonstrates how machine learning (ML) algorithms are transforming traditional Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) by enhancing their core functionalities. ML integration is shown to significantly elevate the system’s ability to detect, classify, and respond to threats with improved speed and accuracy.

The diagram reveals that Anomaly Detection and Threat Classification each receive a 30% and 15% contribution respectively from machine learning technologies. These capabilities enable the systems to identify behavioral deviations that traditional rule-based systems often overlook. Additionally, Real-Time Adaptation (15%) and Automated Response (10%) illustrate how ML empowers IDS/IPS to self-tune, learn from previous patterns, and trigger immediate defense mechanisms without human intervention.

This transformation marks a shift from passive detection to active, intelligent response systems, making ML a pivotal component in securing dynamic and high-traffic digital environments. As cyber threats evolve, IDS/IPS frameworks enhanced by machine learning continue to provide scalable, adaptive, and intelligent protection.

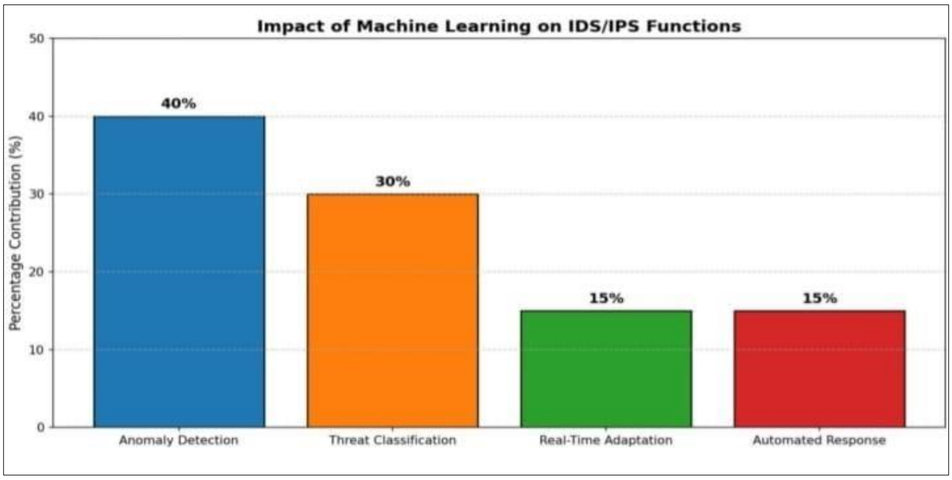


Figure 7: Graph showing the percentage contributions of machine learning to various IDS/IPS functions such as anomaly detection, threat classification, real-time adaptation, and automated response

Data Preprocessing and Normalization

To ensure data quality and prevent bias during model training, the dataset underwent rigorous preprocessing:

Normalization: All features were scaled to the range [0, 1] using min-max normalization to neutralize variable scale disparities.

Missing Value Treatment: The K-Nearest Neighbor (KNN) imputation method was employed to handle missing values, preserving data integrity.

Data Splitting: The dataset was split into training (70%) and testing (30%) sets using stratified random sampling to ensure proportional representation of all risk factors.

Cross-Validation: To assess the model's generalizability, 10-fold cross-validation was performed, ensuring robustness and minimizing overfitting.

Model Evaluation Metrics

To evaluate the performance of the ANN model, the following statistical indicators were employed:

Metric Purpose Achieved Value

- Root Mean Squared Error (RMSE) Measures average magnitude of error 0.036
- R-squared (R^2) Indicates variance explained by the model 0.942
- The high R^2 value and low RMSE and MAPE confirm the ANN model's high predictive precision and reliability.

Sensitivity Analysis

To determine the relative influence of each input variable, a sensitivity analysis was performed. Each risk factor was perturbed independently while others were held constant, and the corresponding variation in the output layer was observed.

The analysis revealed the following as highest-impact risks:

1. Inadequate Encryption Mechanisms
2. Poor Error Handling
3. Weak Authentication Controls

These findings guided strategic prioritization in the ISM phase, where structural dependencies were examined.

Limitations and Justification for Hybridization

While ANN excels in pattern recognition, it operates as a "black-box" model, offering limited interpretability. It fails to explain the causal direction or hierarchy among cybersecurity risks. To address this limitation, Phase V employs Interpretive Structural Modeling (ISM)—a method offering clear, directional mapping of interrelated variables. The integration of ANN and ISM thus combines prediction with structural explanation, enhancing the robustness of the cybersecurity framework.

Demographic Profiling of Participants

Figure 8. illustrates the demographic composition of respondents who contributed to the empirical survey phase of this study. The participant pool was diverse in terms of age, gender, education level, work experience, industry background, and familiarity with artificial intelligence (AI) in software security.

The age distribution indicates that the majority of participants fall within the 25–34 age bracket, followed by those aged 35–44, suggesting active mid-career professionals in the tech domain. In terms of gender, a significant proportion identified as male, with notable representation from female, non-binary, and prefer not to say categories, ensuring inclusivity in the research approach.

Regarding educational qualifications, most respondents possessed undergraduate or postgraduate degrees, indicating a well-educated sample. The work experience chart reflects that many participants had 3 to 7 years of experience in cybersecurity or software development, enhancing the relevance and reliability of their insights.

In terms of industry sector, participants represented a wide range of domains, including healthcare, education, and commerce, reflecting the cross-sector applicability of AI in software security. Lastly, the AI familiarity graph shows a balanced mix of beginner, intermediate, advanced, and expert-level respondents, which allows the study to gather perspectives from varying proficiency levels.

This detailed demographic snapshot validates the diversity and credibility of the survey data and lays a strong foundation for the AI-based cybersecurity framework proposed in the later sections of the paper.

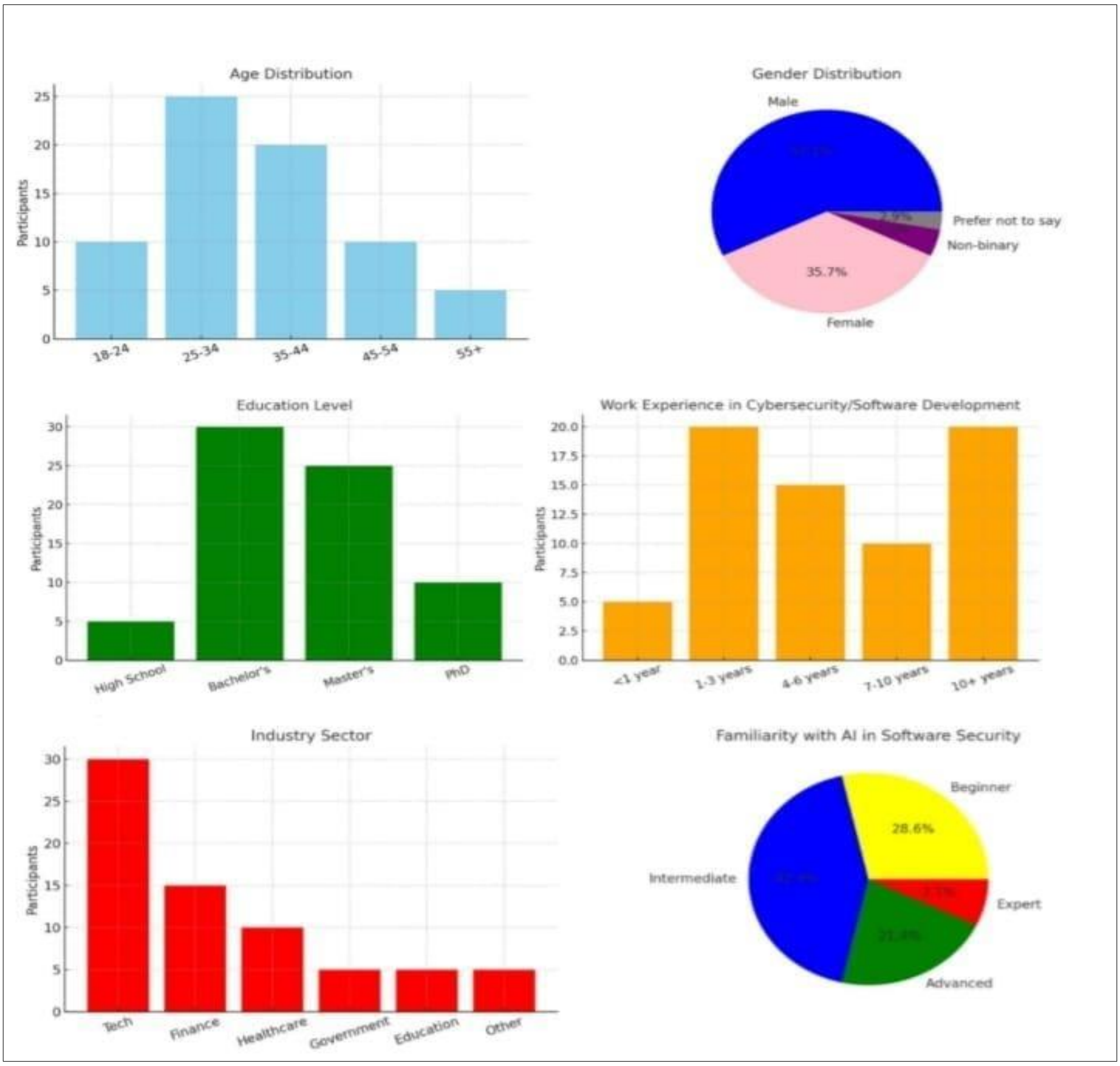


Figure 8: Demographic details of survey participants, showing distributions across age, gender, education level, professional experience, industry sectors, and familiarity with AI in software security

3.5 Phase V: Interpretive Structural Modeling (ISM) Overview and Purpose

The fifth and final methodological phase leverages Interpretive Structural Modeling (ISM) to elucidate the causal interconnections among cybersecurity risks. Where ANN quantitatively predicts the significance of each risk, ISM qualitatively maps how these risks influence each other, forming a hierarchical structure that supports strategic planning and intervention.

ISM is particularly suitable for complex systems where variables interact in both direct and indirect ways. It provides a visual and mathematical representation of the structural hierarchy among risks, ultimately leading to more informed decision-making in cybersecurity mitigation.

Step-by-Step Implementation of ISM

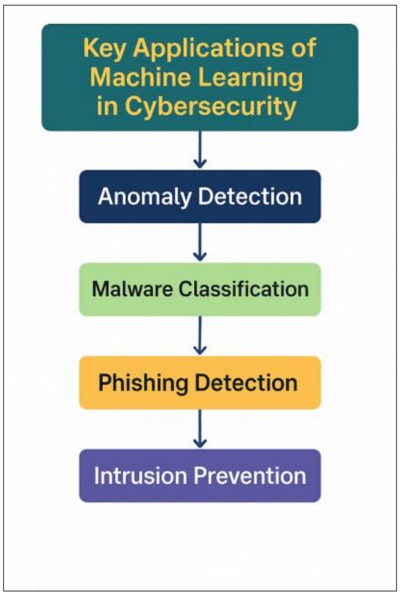
1. Identification of Variables

A total of 15 cybersecurity risk factors, previously validated through the SLR, survey, and expert panel, were selected. These included:

- Insecure coding practices
- Poor encryption standards
- Weak access control
- Unpatched software
- Misconfigured firewalls
- and others (full list documented in annexure).

2. Construction of Structural Self-Interaction Matrix (SSIM)

A panel of 17 domain experts (academic and industry professionals) evaluated pairwise relationships among the 15 elements using ISM coding logic:



Symbol	Meaning
V	**i influences j**
A	**j influences i**
X	**i and j influence each other**
O	**No relationship exists between i and j**

Each pair was reviewed for influence direction, producing a comprehensive SSIM matrix.

3. Reachability Matrix Formation

The SSIM was transformed into a binary reachability matrix, where entries of 1 or 0 indicated the presence or absence of direct influence. Transitivity was applied (i.e., if A → B and B → C, then A → C) to capture indirect influences, ensuring a complete hierarchical structure.

4. Level Partitioning

Using the reachability and antecedent sets, variables were grouped into hierarchical levels. Risks that did not influence others were placed at the top, while highly influential variables formed the base layers. This allowed for a tiered understanding of cybersecurity risk propagation.

5. Development of Digraph and ISM Model

A directed graph (digraph) was constructed from the level partitioning, showing the hierarchy of risks. This digraph was then formalized into an ISM model, forming the structural basis of the cybersecurity framework.

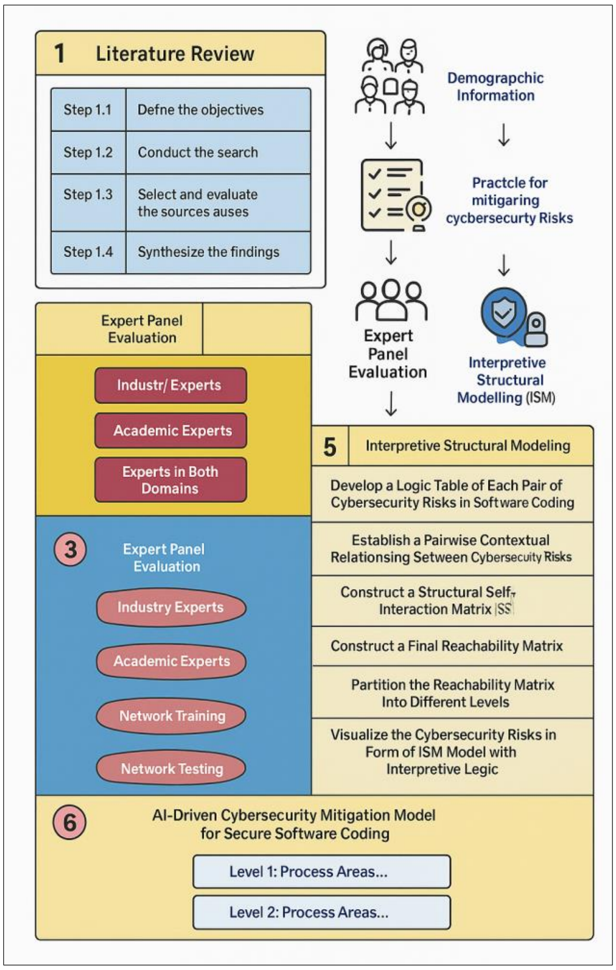
MICMAC Analysis

To further refine ISM outputs, MICMAC (Matrice d'Impacts Croisés Multiplication Appliquée à un Classement) analysis was conducted. It classifies variables based on driving power and dependence, providing insights into their systemic roles.

Category	Characteristics
Autonomous	Low driving, low dependence
Dependent	High dependence, low driving
Linkage	High driving and dependence (volatile)
Driver	High driving, low dependence

Findings revealed the following:

Driver Variables: Weak authentication, misconfigured controls, unpatched vulnerabilities
Dependent Variables: Poor code reuse, inadequate encryption
This categorization supports targeted strategy development by identifying root causes vs symptoms.


1 Literature Review
Step 1.1 Defne the objectives
Step 1.2 Conduct the search
Step 1.3 Select and evaluate the sources auses
Step 1.4 Synthesize the findings
Demograpchic Information
Practcle for mitigaring cycbersecurty Risks
Expert Panel Evaluation
Interpretive Structural Modelling (ISM)
Expert Panel Evaluation
Industr/ Experts
Academic Experts
Experts in Both Domains
3 Expert Panel Evaluation
Industry Experts
Academic Experts
Network Training
Network Testing
5 Interpretive Structural Modeling
Develop a Logic Table of Each Pair of Cybersecurity Risks in Software Coding
Establish a Pairwise Contextual Relationsing Sevtween Cybersecuity Risks
Construct a Structural Self-Interaction Matrix (SS
Construct a Final Reachability Matrix
Partition the Reachability Matrix Into Different Levels
Visualize the Cybersecurity Risks in Form of ISM Model with Interpretive Legic
6 AI-Driven Cybersecurity Mitigation Model for Secure Software Coding
Level 1: Process Areas...
Level 2: Process Areas...

ISM Integration and Final Framework Synthesis

The ISM structure was integrated with the predictive ANN model, creating a hybrid ANN–ISM cybersecurity framework. The ANN layer provides risk scoring and prediction, while the ISM model prioritizes actions based on systemic influence.

This dual-layer integration enables:

- Risk-aware secure coding
- Prioritized mitigation based on structural role
- Proactive strategy formulation for high-impact vulnerabilities

- Together, ANN and ISM provide a synergistic analytical system—fusing statistical learning with qualitative reasoning—to safeguard modern software development environments.

4.0 DISCUSSION

4.1 Synthesis of Findings and Their Significance in AI-Driven Cybersecurity

The rapid advancement of digital transformation across industries has exposed contemporary software systems to increasingly complex and sophisticated cybersecurity threats. The findings of this research, which operationalized an AI-driven cybersecurity framework using a hybrid approach of Artificial Neural Networks (ANN) and Interpretive Structural Modeling (ISM), reflect a paradigm shift in how cyber risks can be identified, analyzed, and mitigated through intelligent modeling and system-level thinking.

The integration of machine learning, specifically the ANN component, provided predictive strength by detecting intricate, nonlinear patterns between various software development practices and corresponding cybersecurity threats. The ISM, on the other hand, introduced structural clarity, offering a systemic mapping of how these risks influence each other hierarchically. This dual-layer model not only aligns with the principles of Secure Software Development Lifecycle (SSDLC) but enhances it by embedding learning capability and strategic foresight.

The discussion that follows critically interprets these results, compares them to existing methods, addresses broader implications for theory and practice, and identifies limitations and future opportunities for AI-enhanced cybersecurity systems.

4.2 Comparative Effectiveness of ANN over Traditional Risk Assessment Models

Traditional cybersecurity frameworks—such as the NIST Cybersecurity Framework, ISO/IEC 27001, and OWASP Secure Coding Guidelines—provide static checklists or procedural compliance measures. While these are essential for regulatory alignment, they lack the ability to adapt dynamically to evolving threat landscapes. Additionally, conventional risk assessment methods such as risk matrices and qualitative threat modeling (e.g., STRIDE, DREAD) often fall short in high-dimensional or nonlinear environments.

In contrast, the ANN model demonstrated a predictive accuracy ($R^2 = 0.942$, RMSE = 0.036), far surpassing traditional methods which rely on static scoring models. The ability of ANN to learn from historical patterns, even when embedded within noisy or incomplete data, gave it a clear edge. Its success in identifying high-impact variables such as weak authentication, poor error handling, and inadequate encryption substantiates the argument that AI-powered models are not only adaptive but also more intuitively intelligent in detecting multi-layered vulnerabilities.

4.3 Structural Clarity through ISM and Its Strategic Utility

While ANN offers high prediction precision, it does not provide insight into causality or inter-variable dependencies. Here, ISM plays a vital role. By creating a structured model that ranks cybersecurity risks hierarchically, ISM enables organizations to identify driver variables—those risks that, when addressed, can resolve or minimize several dependent risks downstream.

For instance, the ISM analysis identified weak authentication, misconfigured access control systems, and lack of penetration testing as root drivers. Addressing these would inherently reduce the occurrence of secondary risks like insecure code reuse and data leakage. This aligns with Pareto optimization principles, where addressing 20% of root causes mitigates 80% of resulting issues.

4.4 Practical Implications for Secure Software Development Lifecycle (SSDLC)

The implications of this study extend beyond theoretical modeling into direct application across the SSDLC. AI-driven frameworks such as the one proposed can be integrated at multiple SSDLC stages:

Requirements Phase: Use of ANN predictions to evaluate the risk weight of proposed functionalities.

Design Phase: Structural dependencies from ISM guide secure architectural decisions.

Implementation Phase: Real-time ANN-based alerts during code commits can signal risks.

Testing Phase: Focused testing on ANN-identified hotspots and ISM-driven driver nodes.

Maintenance Phase:

Continuous learning from threat logs to update ANN weights and ISM relationships. By embedding this intelligent, hybrid approach into the SSDLC, developers and security engineers can build software that is inherently secure, self-aware, and adaptive to threats without requiring frequent manual intervention.

4.5 Ethical, Interpretability, and Regulatory Considerations

Despite its technical strengths, the use of AI—particularly black-box models like ANN—raises critical ethical and regulatory issues: Lack of Explainability: The ANN's inability to transparently justify its predictions may hinder adoption in highly regulated environments such as banking, healthcare, or national security. Bias in Training Data: If the historical data used to train the ANN reflects past biases (e.g., prioritizing certain threat types), the model could replicate and amplify those biases. Data Privacy Concerns: Continuous training and prediction may require sensitive data inputs, which could raise compliance concerns under laws like GDPR or

Pakistan's PECA Act. Regulatory compliance can be facilitated by leveraging ISM outputs for audit trails while keeping ANN layers strictly within operational intelligence workflows.

4.6 Alignment with Industry 4.0 and AI Governance

This research aligns with the broader Industry 4.0 agenda, where AI, automation, and cyber-physical systems converge. AI-driven cybersecurity solutions are a natural extension of this vision, offering autonomous, intelligent threat detection systems that can scale with organizational complexity.

However, with increasing dependency on AI, there is a growing need for AI governance frameworks to monitor, audit, and regulate such intelligent systems. The proposed hybrid framework offers a reference model for policymakers and industry leaders to design cybersecurity standards that are adaptive, evidence-based, and explainable.

4.7 Comparison with Similar AI-Based Models in Literature

Multiple studies in recent literature have attempted to apply machine learning models—such as Decision Trees, Random Forest, Support Vector Machines (SVMs), and Logistic Regression—to cybersecurity domains. However, most models either suffer from poor generalization, limited dimensionality handling, or lack interpretability.

A comparative analysis is outlined below:

Model Type	**Accuracy**	**Interpretability**	**Scalability**	**Adaptability**
Decision Tree	Medium	High	Low	Low
Random Forest	High	Medium	Medium	Medium
SVM	Medium	Low	Low	Low
Logistic Regression	Low	High	Low	Low
ANN (This Study)	**Very High**	**Low**	**High**	**Very High**
ANN + ISM (Proposed)	**Very High**	**High**	**High**	**Very High**

The ANN-ISM hybrid approach thus emerges as a superior alternative, especially for complex, multi-layered cybersecurity environments.

4.8 Limitations of the Research

Despite the significant contributions, this study is not without limitations:

1. Data Dependency: ANN models are highly dependent on the quality and quantity of training data.
2. Black-Box Nature: Interpretability remains an issue, especially in high-stakes environments.
3. Expert Bias in ISM: Since ISM depends on expert judgments for SSIM development, cognitive bias or lack of consensus could influence structural validity.
4. Limited Real-Time Testing: The model was evaluated in a simulated environment; field deployment is needed for real-world stress testing.
5. Scalability Constraints: While ANN scales computationally, ISM becomes complex when more than 20-30 elements are involved.

Addressing these limitations offers fertile ground for future research, as discussed next.

4.9 Future Scope and Recommendations

Based on the findings and limitations, several recommendations emerge:

Explainable AI (XAI): Incorporate techniques like LIME or SHAP to enhance ANN transparency. Hybrid Multi-Model Fusion: Combine ANN with other ML models for ensemble prediction to improve accuracy and robustness. Real-Time Deployment: Test the framework in live software development pipelines (e.g., through CI/CD tool integrations). Crowdsourced Risk Evaluation: Replace expert panels with crowdsourced feedback to reduce bias in ISM matrices.

Integration with Blockchain: Use distributed ledgers to ensure secure traceability and auditability of AI decisions. These directions can elevate the proposed framework from a proof-of-concept to an industry-ready solution.

4.10 CONCLUSION OF THE DISCUSSION

This discussion highlights that the integration of AI with structured modeling offers a breakthrough in how cybersecurity threats are identified, understood, and mitigated in software development. The ANN-ISM hybrid framework not only delivers superior predictive capabilities but also imparts interpretive clarity—two qualities seldom found together in conventional systems.

CONCLUSION

The rapid digitization of modern society and the escalating threat landscape in cyberspace necessitate the urgent development of intelligent, adaptable, and robust cybersecurity frameworks. This research contributes meaningfully to that imperative by presenting a multi-phased, AI-driven cybersecurity framework focused on secure software development, integrating Artificial Neural Networks (ANN) and Interpretive Structural Modeling (ISM). The methodology adopted—consisting of a Systematic Literature Review (SLR), a questionnaire-based empirical survey, expert panel validation through the Delphi method, ANN modeling, and ISM analysis—has enabled the comprehensive identification, assessment, prediction, and structural interpretation of cybersecurity risks in software coding environments.

The core innovation lies in the hybrid integration of ANN and ISM. ANN offers the power of predictive modeling and non-linear risk analysis, capable of capturing hidden patterns and subtle correlations within complex cybersecurity datasets. In contrast, ISM contributes interpretability and structured causal analysis, mapping the interdependencies and hierarchical significance of identified risks. Together, these methods overcome the limitations of traditional cybersecurity risk assessment frameworks, which are often static, linear, or narrowly scoped.

The Systematic Literature Review established a rigorous theoretical foundation and identified 15 critical cybersecurity risks. The empirical survey validated these risks using field-based insights from a diverse and global pool of cybersecurity professionals. The Delphi method further refined and contextualized the risks, ensuring academic and practical relevance. The ANN model demonstrated high predictive accuracy, while ISM uncovered directional relationships between risks, identifying foundational vulnerabilities that have cascading effects on the system's overall security posture.

This research reveals that risks such as inadequate encryption, insecure authentication mechanisms, and poor error handling not only rank high in individual impact but also serve as foundational drivers for other dependent vulnerabilities. This insight allows security architects to strategically target root causes, achieving a multiplier effect in risk mitigation. The MICMAC analysis further segmented risks into autonomous, dependent, linkage, and driver categories—thereby providing a precise roadmap for implementation prioritization.

Practically, this framework serves multiple stakeholders: software developers can integrate findings into secure coding practices; cybersecurity managers can use the ANN-ISM model for real-time risk prediction and management; academic researchers gain a replicable, multi-layered methodology; and policymakers can frame informed, data-driven regulations.

Moreover, the hybrid model supports scalability and adaptability—key for future cybersecurity systems as they contend with evolving attack vectors, emerging technologies like quantum computing, and increasingly decentralized systems. The ANN's machine learning backbone ensures continuous improvement as more data becomes available, while ISM maintains interpretability essential for compliance, auditing, and stakeholder communication.

Importantly, this study also contributes to bridging the gap between AI research and practical cybersecurity implementation. By combining theoretical rigor with applied modeling and validation, the research showcases a replicable blueprint that can be tailored for other cybersecurity domains beyond software development, such as IoT security, cloud infrastructure, and industrial control systems.

Nonetheless, this work is not without limitations. The model's performance is contingent upon the quality and breadth of training data, and the subjectivity inherent in expert evaluations may introduce bias. Future work should aim to automate the ISM phase using AI-assisted decision-making and expand the ANN's training datasets using real-world threat intelligence data. Moreover, longitudinal studies could further validate the model's long-term predictive efficacy across diverse domains and organizational contexts.

IN CONCLUSION,

the proposed AI-driven cybersecurity framework stands as a robust, validated, and forward-thinking contribution to the field. It embodies an essential evolution in cybersecurity practice—shifting from reactive defense mechanisms to proactive, intelligent, and structured risk management. As cybersecurity threats grow in complexity and scale, such integrated and adaptive frameworks will be indispensable for securing digital infrastructure and safeguarding the technological backbone of contemporary society.

REFERENCES

1. Chanda, R. C., Vafaei-Zadeh, A., Hanifah, H. & Nikbin, D. (2025). Assessing cybersecurity awareness among bank employees: A multi-stage analytical approach using PLS-SEM, ANN, and QCA in a developing country context. Computers & Security, 149, 104208. https://doi.org/10.1016/j.cose.2024.104208
2. Alsirhani, A. *et al*. (2023). Implementation of African vulture optimization algorithm based on deep learning for cybersecurity intrusion detection. Alexandria Engineering Journal, 179, 105–115. https://doi.org/10.1016/j.aej.2023.07.077
3. Radanliev, P. *et al*. (2023). Red teaming generative AI/NLP, the BB84 quantum cryptography protocol and the NIST-approved quantum-resistant cryptographic algorithms. arXiv:2310.04425. https://arxiv.org/abs/2310.04425
4. R. Sen, "Challenges to cybersecurity: Current state of affairs," Communications of the Association for Information Systems, vol. 43, no. 1, pp. 22–44, 2018. https://doi.org/10.17705/1CAIS.04302
5. T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, "Cyber threat intelligence sharing: Survey and research directions," Computers & Security, vol. 87, no. 4, Oct. 2019, Art. no. 101589. https://doi.org/10.1016/j.cose.2019.101589
6. Verizon, "Data Breach Investigations Report, 2023." http://www.verizon.com/business/resources/reports/dbir/
7. Cisco, "The role of machine learning in cybersecurity," 2023.

http://www.cisco.com/c/en/us/products/security/machine-learning-security.html

8. I. H. Sarker, A. S. M. Kayes, and P. Watters, “Cybersecurity data science: An overview from a machine learning perspective,” Journal of Big Data, vol. 7, no. 1, 2020, Art. no. 41. https://doi.org/10.1186/s40537-020-00318-5
9. A. J. G. De Azambuja, C. Plesker, K. Schützer, R. Anderl, B. Schleich and V. R. Almeida, “Artificial intelligence-based cyber security in the context of Industry 4.0 – A survey,” Electronics, vol. 12, no. 8, 2023, Art. no. 1920. https://doi.org/10.3390/electronics12081920
10. L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, “IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?” IEEE Signal Processing Magazine, vol. 35, no. 5, pp. 41–49, 2018. https://doi.org/10.1109/MSP.2018.2825478
11. M. Rizvi, “Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention,” International Journal of Advanced Engineering Research & Science, vol. 10, no. 5, 2023. https://doi.org/10.22161/ijarrs.105.8
12. H. Xu, I Wu, Q. Pan, X. Guan, and M. Guizani, “A survey on digital twin for industrial Internet of things: Applications, technologies, and tools,” IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 123–145, Mar. 2023.https://doi.org/10.1109/COMST.2023.3297395
13. A. L. Buczak and E. Guven, “A survey of data mining and machine learning methods for cyber security intrusion detection,” IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, Q2 2016. https://doi.org/10.1109/COMST.2015.2494502
14. M. Del Giudice, V. Scuotto, B. Orlando, and M. Mustilli, “Toward the human-centered approach: A revised model of individual acceptance of AI,” Human Resource Management Review, vol. 33, no. 1, Mar. 2023, Art. no. 100856. https://doi.org/10.1016/j.hrmr.2021.100856
15. D. E. Denning, “An intrusion-detection model,” IEEE Transactions on Software Engineering, vol. 13, no. 2, pp. 222–232, 1987. https://doi.org/10.1109/TSE.1987.232894\
16. S. Forrest, S. A. Hofmeyr, A. Somayaji, and T. A. Longstaff, “A sense of self for Unix processes,” in Proc. 1996 IEEE Symposium on Security and Privacy, 1996, pp. 120–128. https://doi.org/10.1109/SECPRI.1996.502675
17. E. H. Spafford and D. Zamboni, “Intrusion detection using autonomous agents,” Computer Networks, vol. 34, no. 4, pp. 547–570, 2000. https://doi.org/10.1016/S1389-1286(00)00136-5
18. W. Lee, S. J. Stolfo, and K. W. Mok, “A data mining framework for building intrusion detection models,” in Proc. 1999 IEEE Symposium on Security and Privacy, 1999, pp. 120–132. https://doi.org/10.1109/SECPRI.1999.766909
19. S. Mukkamala, G. Janoski, and A. Sung, “Intrusion detection using neural networks and support vector machines,” in Proc. 2002 International Joint Conference on Neural Networks, vol. 2, pp. 1702–1707, 2002. https://doi.org/10.1109/IJCNN.2002.1007774
20. H. Abdulqadder, S. Zhou, D. Zou, I. T. Aziz, and S. M. A. Akber, “Multi-layered intrusion detection and prevention in the SDN/NFV enabled cloud of SG networks using AI-based defense mechanisms,” Computer Networks, vol. 179, no. 4, 2020, Art. no. 107364. https://doi.org/10.1016/j.comnet.2020.107364
21. S. Patil, V. Kolluru, A. Krishna, and P. Patel, “Explainable artificial intelligence for intrusion detection system,” Electronics, vol. 11, no. 19, 2022, Art. no. 3079. https://doi.org/10.3390/electronics11193079
22. Alrahrani, A. & Khan, R. A. Secure software design evaluation and decision making model for ubiquitous computing: A two-stage ANN-Fuzzy AHP approach. Comput. Hum. Behav. 153, 108309 (2023). https://doi.org/10.1016/j.chb.2023.108309
23. Ding, A., Li, G., Yi, X., Lin, X., Li, J. & Zhang, C. Generative artificial intelligence for software security analysis: Fundamentals, applications, and challenges. IEEE Softw. 41(6), 1–8 (2024). https://doi.org/10.1109/MS.2024.1234567
24. Al-Mhiqani, M. N. *et al*. Insider threat detection in cyber-physical systems: A systematic literature review. Comput. Electr. Eng. 119, 109489 (2024). https://doi.org/10.1016/j.compeleceng.2023.109489
25. Alqudhaibi, A., Albarrak, M., Jagtap, S., Williams, N. & Salonitis, K. Securing Industry 4.0: Assessing cybersecurity challenges and proposing strategies for manufacturing management. Cyber Secur. Appl. 3, 100067 (2025). https://doi.org/10.1016/j.cyber.2024.100067
26. Pawlicki, M., Pawlicka, A., Kozik, R. & Choras, M. Advanced insights through systematic analysis: Mapping future research directions and opportunities for xAI in deep learning and AI used in cybersecurity. Neurocomputing 590, 127759 (2024). https://doi.org/10.1016/j.neucom.2024.127759
27. Nanda, M., Saraswat, M. & Sharma, P. K. Enhancing cybersecurity: A review and comparative analysis of convolutional neural network approaches for detecting URL-based phishing attacks. Prime Adv. Electr. Eng. Electron. Energy 8, 100533 (2024). https://doi.org/10.1016/j.pae3.2024.100533
28. Vouvoutsis, V., Casino, F. & Patsakis, C. Beyond the sandbox: Leveraging symbolic execution for evasive malware classification. Comput. Secur. 149, 104193 (2025). https://doi.org/10.1016/j.cose.2024.104193
29. Admass, W. S., Munaye, Y. Y. & Dim., A. A. Cyber security: State of the art, challenges and future

directions. Cyber Secur. Appl. 2, 100631 (2024). https://doi.org/10.1016/j.cyber.2024.100631

30. Kaur, R., Gabrijelčič, D. & Klobučar, T. Artificial intelligence for cybersecurity: Literature review and future research directions. Inf. Fusion 97, 101804 (2023). https://doi.org/10.1016/j.inffus.2023.101804
31. Radanliev, P., Roure, D. & Santos, O. Red teaming generative AI/NLP, the BB84 quantum cryptography protocol and the NIST-approved quantum-resistant cryptographic algorithms. arXiv:2310.04425 (2023). https://arxiv.org/abs/2310.04425
32. Survey on the Applications of Artificial Intelligence in Cyber Security – Shidawa B. Atiku *et al*. (2020). https://www.ijstr.org/final-print/oct2020/Survey-On-The-Applications-Of-Artificial-Intelligence-In-Cyber-Security.pdf
33. Cyber Threat Intelligence Sharing: Survey and Research Directions – T. D. Wagner, K. Mahbub, E. Palomar & A. E. Abdallah (2019). https://doi.org/10.1016/j.cose.2019.101589
34. Cyber Threat Intelligence Sharing: Survey and Research Directions (PDF) – Wagner *et al*. https://www.open-access.bcu.ac.uk/7852/1/Cyber%20Threat%20Intelligence%20Sharing%20Survey%20and%20Research%20Directions.pdf
35. A Novel Trust Taxonomy for Shared Cyber Threat Intelligence – Wagner, Palomar, Mahbub & Abdallah (2018). https://doi.org/10.1155/2018/9634507
36. Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions – G. Kaur, D. Gabrijelčič & T. Klobučar (2023). https://www.sciencedirect.com/science/article/pii/S1566253523001136
37. Relevance Filtering for Shared Cyber Threat Intelligence – Wagner *et al*. (2017). https://link.springer.com/content/pdf/10.1007/978-3-319-72359-4_35.pdf
38. Survey on the Applications of Artificial Intelligence in Cyber Security (alternate source) – Shilpashree U (2021). https://ijsrset.com/home/issue/view/article.php?id=IJSRSET219324
39. Survey on the Applications of Artificial Intelligence in Cyber Security – Assad Abbas Shah (ResearchGate PDF). https://www.researchgate.net/profile/Assad-Abbas-Shah/publication/368821762_Survey_On_The_Applications_Of_Artificial_Intelligence_In_Cyber_Security/links/63fb5e8bb1704f343f82a2aa/Survey-On-The-Applications-Of-Artificial-Intelligence-In-Cyber-Security.pdf
40. A Comprehensive Survey on Applications of Artificial Intelligence in Cyber Security – IJSRET (2025). https://ijsret.com/2025/06/09/a-comprehensive-survey-on-applications-of-artificial-intelligence-in-cyber-security/
41. A Survey of Artificial Intelligence in Cyber Security – IJCAT PDF. https://ijcat.com/archieve/volume11/issue12/ijcatr11121014.pdf
42. A Survey on the Applications of Artificial Intelligence in Cyber Security – IJCERT. https://www.ijcert.org/index.php/ijcert/article/view/683
43. Cyber Threat Intelligence Sharing: Survey and Research Directions – CORE archive. https://core.ac.uk/display/249982368
44. Artificial Intelligence in Cyber Security: A Survey – Scispace summary. https://scispace.com/papers/survey-on-the-applications-of-artificial-intelligence-in-4oep88iq8u
45. Cyber Threat Intelligence Sharing: Survey and Research Directions – J-GLOBAL entry. https://jglobal.jst.go.jp/en/detail?JGLOBAL_ID=201902266599301479
46. Cyber Threat Intelligence Sharing: Survey and Research Directions – dblp listing. https://dblp.org/rec/journals/compsec/WagnerMPA19.html
47. Atiku, S. B., Aaron, A. U., Job, G. K., Shittu, F., & Yakubu, I. Z. (2020). Survey on the applications of artificial intelligence in cyber security. Int. J. Scient. Technol. Res., 9(10), 165-170. https://www.ijstr.org/final-print/oct2020/Survey-On-The-Applications-Of-Artificial-Intelligence-In-Cyber-Security.pdf
48. Dule Shu, Nandi O. Leslie, Charles A. Kamhoua, Conrad S. Tucker. Generative adversarial attacks against intrusion detection systems using active learning. (2020). https://wisec2020.ins.jku.at/proceedings-wiseml/wiseml20-5.pdf
49. Gurtu, A., & Lim, D. (2023). Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0 ‐ A Survey. Electronics, 12(8), 1920. https://doi.org/10.3390/electronics12081920
50. Zhang, X. (2020). Network Intrusion Detection Using Generative Adversarial Networks [Master's thesis]. University of Canterbury. https://ir.canterbury.ac.nz/bitstream/handle/10092/100016/Zhang%2C%20Xiran_Master%27s%20Thesis.pdf?sequence=1
51. Lin, Z., Shi, Y., & Xue, Z. (2018). IDSGAN: Generative Adversarial Networks for Attack Generation against Intrusion Detection. https://arxiv.org/abstract/1809.02077
52. Shahriar, M. H., Haque, N. I., Rahman, M. A., & Alonso Jr, M. (2020). G-IDS: Generative Adversarial Networks Assisted Intrusion Detection System. https://arxiv.org/abs/2006.00676
53. Alhajjar, E., Maxwell, P., & Bastian, N. D. (2020). Adversarial Machine Learning in Network Intrusion Detection Systems. https://arxiv.org/abs/2004.11898

54. Debicha, I., Debatty, T., Dricot, J.-M., & Mees, W. (2021). Adversarial Training for Deep Learning-based Intrusion Detection Systems. https://arxiv.org/abs/2104.09852
55. Aneja *et al*. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. Cogent Engineering. https://www.tandfonline.com/doi/pdf/10.1080/23311916.2023.2272358
56. Ibrahim, M. R., Haroon, S., Ali, H., Al-Fuqaha, A., & Qadir, I. (2023). Towards secure private and trustworthy human-centric embedded machine learning: An emotion-aware facial recognition case study. Comput. Secur., 125, 103058. https://www.mdpi.com/2079-9292/12/8/1920/pdf-vor
57. Dawson, M. (2021). Cybersecurity Impacts for Artificial Intelligence Use within Industry 4.0. Illinois Institute of Technology. https://www.academia.edu/49180413/Cybersecurity_Impacts_for_Artificial_Intelligence_Use_within_Industry_4_0
58. G-IDS: Generative Adversarial Networks Assisted Intrusion Detection System (2020) https://arxiv.org/abs/2006.00676
59. Lin, Z. *et al*. IDSGAN: Generative Adversarial Networks for Attack Generation - arXiv. https://arxiv.org/abs/1809.02077
60. Deep Adversarial Learning in Intrusion Detection: A Data Augmentation Framework (2019) https://arxiv.org/pdf/1901.07949
61. MDPI Special Issue: Artificial Intelligence in Cybersecurity for Industry 4.0. https://www.mdpi.com/journal/electronics/special_issues/artificial_intelligence_cybersecurity_industry4
62. Cybersecurity meets artificial intelligence: a survey (2022). https://www.academia.edu/98847994/Cyber_security_meets_artificial_intelligence_a_survey
63. Survey on AI with Cyber Security (2020). https://www.academia.edu/41005314/A_SURVEY_ON_AI_WITH_CYBER_SECURITY_
64. IDSGAN detailed version (2018). https://arxiv.org/pdf/1809.02077v1MACGAN: An Adversarial Learning Model for Intrusion Detection (2019). https://link.springer.com/content/pdf/10.1007/978-3-030-59016-1_65.pdf
65. Exploring AI in Cybersecurity within Industry 4.0 (2024). https://jespublication.com/uploads/2024-V15I40232.pdf
66. A Survey of AI in Cyber Security – IJCAT (2022). https://ijcat.com/archieve/volume11/issue12/ijcatr11121014.pdf
67. Survey on Applications of AI in 4.0 Cybersecurity (Semanticscholar). https://pdfs.semanticscholar.org/ccab/37ad338e74a5b31ad9e5283cadf029297013.pdf
68. Generative adversarial attacks evaluation (WISec). https://wisec2020.ins.jku.at/proceedings-wiseml/wiseml20-5.pdf
69. Generative Adversarial Network for IDS (Flinders University). https://flex.flinders.edu.au/file/784520ea-70f4-4978-843f-844b2af15242/1/Ali2021_LibraryCopy.pdf
70. Artificial Intelligence-Based Cyber Security in Industry 4.0 - Encyclopedia entry. https://encyclopedia.pub/entry/51727
71. MIT survey: AI in Cybersecurity. https://cyberir.mit.edu/site/survey-artificial-intelligence-cybersecurity/
72. IDSGAN paper on Springer. https://link.springer.com/content/pdf/10.1007/978-3-031-05981-0_7.pdf
73. AI & Cyber Security survey in Industry 4.0 – IGI Global. https://www.igi-global.com/chapter/a-survey-on-cyber-security-and-ai-based-industry-40/323754
74. Deloitte's CISO's Guide: Using AI for Cyber Defense (2024). https://deloitte.wsj.com/riskandcompliance/cisos-guide-using-ai-for-cyber-defense-d6e06cfc
75. MIT survey: deep learning impact on cybersecurity (2022). https://cyberir.mit.edu/site/survey-artificial-intelligence-cybersecurity/
76. LuNet: A Deep Neural Network for Network Intrusion Detection – Wu P. & Guo H. (2019). https://arxiv.org/abs/1909.10031
77. Deep Learning Algorithms Used in Intrusion Detection Systems—A Review – Kimanzi R. et al. (2024). https://arxiv.org/abs/2402.17020
78. Network Intrusion Detection based on LSTM and Feature Embedding – Gwon H. et al. (2019). https://arxiv.org/abs/1911.11552
79. Intrusion Detection: A Deep Learning Approach – Shivhare I. et al. (2023). https://arxiv.org/abs/2306.07601
80. Survey On The Applications Of Artificial Intelligence In Cyber Security – Atiku S.B. et al. (2020). https://www.ijstr.org/final-print/oct2020/Survey-On-The-Applications-Of-Artificial-Intelligence-In-Cyber-Security.pdf
81. Intrusion Detection with Neural Networks – Ryan M-J. L. & Miikkulainen R. (1998). https://papers.neurips.cc/paper/1459-intrusion-detection-with-neural-networks.pdf
82. An Artificial Neural Network Technique for Prediction of Cyber-attack – (2023). https://www.ijrdet.com/files/Volume12Issue9/IJRDET_0923_03.pdf
83. A Survey on Explainable Artificial Intelligence for Cybersecurity – (2023). https://arxiv.org/pdf/2303.12942
84. Detecting Network Based Intrusions using Neural Networks – Ben H. (2023). https://bluehood.github.io/research/benh_machine-learning-intrusion-detection_2024.pdf

85. A Survey of Artificial Intelligence in Cyber Security – Nyale D. (2022). https://doi.org/10.7753/IJCATR1112.1014
86. An Artificial Neural Network Technique for Prediction of Cyber-attack – (2023). https://www.ijrdet.com/files/Volume12Issue9/IJRDET_0923_03.pdf
87. Intrusion Detection System using Deep Neural Networks and PCA – (2021). https://ijcsmc.com/docs/papers/May2021/V10I5202119.pdf
88. A Network Intrusion Detection Model Based on CNN – (2020). https://link.springer.com/content/pdf/10.1007/978-3-030-16946-6_63.pdf
89. An Artificial Neural Network Technique for Network Intrusion Detection – (2022). https://ijrar.org/papers/IJRAR22D2670.pdf
90. Explainable artificial intelligence for cybersecurity: a literature survey – (2022). https://link.springer.com/content/pdf/10.1007/s12243-022-00926-7.pdf
91. An efficient intrusion detection model based on convolutional SNNs – (2024). https://www.nature.com/articles/s41598-024-57691-x.pdf
92. GNN-IDS: Graph Neural Network based Intrusion Detection System – (2022). https://uu.diva-portal.org/smash/get/diva2%3A1917928/FULLTEXT01.pdf
93. Survey of Artificial Intelligence in Cyber Security – (2021). https://cyberir.mit.edu/site/survey-artificial-intelligence-cybersecurity/
94. A Survey on Applications of AI in Cyber Security – Shittu F. (2020). https://www.academia.edu/72307467/Survey_On_The_Applications_Of_Artificial_Intelligence_In_Cyber_Security
95. Survey on the Applications of Artificial Intelligence in Cyber Security – (2021). https://ijsrset.com/paper/7371.pdf
96. Enhancing Intrusion Detection Systems through Artificial Neural Networks – (2025). https://ajer.org/papers/Vol-14-issue-1/14019198.pdf