

INTELLIGENT THREAT DETECTION AND AUTOMATED RISK MANAGEMENT IN IT USING MACHINE LEARNING

Azhar Khan^{*1}, Yasir Shah², Shehzad Khan³, Hansa Sattar⁴, Shahzair Hussain⁵, Ayesha Zain⁶, Muhammad Tayyeb⁷

¹Institute of Computer Sciences and Information Technology (ICS&IT), Faculty of Management and Computer Sciences (FMCS), The University of Agriculture (AUP), University Road, Peshawar 25130, Khyber Pakhtunkhwa, Pakistan.

²City University of science and Information Technology Peshawar, District Peshawar 25000, Pakistan

^{3,4}University of Engineering & Technology Mardan 23200 KPK Pakistan

⁵Institute of Computer Sciences and Information Technology (ICS&IT), Faculty of Management and Computer Sciences (FMCS), The University of Agriculture (AUP), University Road, Peshawar 25130, Khyber Pakhtunkhwa, Pakistan.

⁶MS Computer Science, Qurtuba University of Peshawar, Pakistan.
University of Engineering and Technology Mardan, Pakistan.

¹azharkhansaqi143@gmail.com, ²yasirshah@gmail.com, ³skshehzad590@gmail.com,
⁴sattarhansa@gmail.com, ⁵shahzair18@gmail.com, ⁶khanishi007@gmail.com,
⁷121muhammadtayyeb@gmail.com

DOI: <https://doi.org/10.5281/zenodo.22659067>

Keywords

Cyber Security, IT Management, Machine Learning, Threat Detection, Risk Management, Anomaly Detection, Intrusion Detection, Predictive Analytics, Data Breach, Security Automation

Article History

Received: 14 July 2026

Accepted: 18 August 2026

Published: 31 August 2026

Copyright @Author

Corresponding Author: *
Azhar Khan

Abstract

This research investigates how machine learning enhances cyber security practices within IT management systems across 120 organizations between 2021 and 2025. Findings indicate that ML-powered intrusion detection systems reached 94.7% accuracy in detecting advanced threats, while traditional rule-based systems only achieved 78.3%. The adoption of ML reduced the average time to detect threats by 63%, from 18.4 hours to 6.8 hours, and cut average response time by 58%, from 12.1 hours to 5.1 hours. Statistical results show a 72% inverse relationship between ML adoption in security operations and the number of data breaches per year. Survey responses from 4,200 IT managers reveal that 68% of organizations using ML for log monitoring and anomaly detection experienced 41% fewer false positives and a 37% boost in vulnerability management efficiency. Financial analysis shows that each 1% rise in ML automation of security tasks is linked to \$2.3 million in annual savings on security operations.

Predictive ML models were able to forecast 83% of phishing and malware attacks 48 hours in advance, with 89% precision. Companies using ML-based risk scoring and automated patching also showed 29% higher compliance with ISO 27001 requirements. At a national level, countries with 50% or more ML integration in cyber infrastructure saw 33% lower success rates of ransomware attacks. The study concludes that embedding machine learning into IT management enables a proactive, scalable, and cost-effective defense strategy. It recommends widespread enterprise adoption to strengthen security resilience and improve operational performance.

1. Introduction

The fast development of the digital industry, cloud computing technology, information systems interconnection and remote working environment created new challenges for cybersecurity. In this context, companies are becoming victims of complicated attacks – ransomware, phishing, malware, hacking attempts, internal threats, and others (Shah & Best, 2025). The use of standard security practices based on pre-defined rules and signatures is ineffective against attacks changing their nature. This situation forces companies to introduce machine learning algorithms into cybersecurity and IT management practices as an instrument capable of detecting abnormal behavior patterns and predicting attacks, creating automated response strategies, and enhancing the process of risk assessment (Sarfraz et al., 2025).

Machine learning provides cybersecurity systems with the opportunity to analyze large volumes of network traffic, system logs, endpoint data, and other security events for identification of patterns indicating the presence of security threats (Manoharan & Sarker, 2023). While standard cybersecurity solutions cannot cope with attacks having unprecedented patterns because of the lack of pre-set algorithms, intelligent systems using machine learning are able to detect any anomalies among large quantities of information. As a result, intrusion detection, threat prediction, anomaly detection, automatic patches, and machine learning risk assessments may improve the company's approach to cyber security management (Lee et al., 2025).

The introduction of machine learning into IT management processes also has certain implications. The investigation of alerts, vulnerability and threat analysis, identification of priority and the implementation of response strategies usually require significant amount of work from security team. Too many false-positive alerts complicate this task, and, in this case, machine learning algorithms may help security professionals to focus on events with high priority, predict the future threats and initiate predefined response (Khalifa & Taha, 2026).

This research will examine the use of ML as an effective tool for threat detection and automated risk management in the work of 120 organizations within the timeframe of 2021-2025. For this, survey evidence from 4,200 IT managers will be analyzed to reveal the level of organizational use, operational performance, decrease in false positives, efficiency of vulnerability management, and security automation. In addition, this research will evaluate ML-predictive power, economic gains, compliance achievements, and ransomware-based security outcomes (Aminu et al., 2024).

Most importantly, in this study, the main emphasis will be made on quantification of differences between regular security measures and ML-assisted cybersecurity management. Such indicators will be considered as detection accuracy, time spent on threat detection and responding to it, frequency of data breaches, rates of false positive results, efficiency of vulnerability management, predictive accuracy, economic savings, ISO 27001 compliance, and ransomware success rate (Muthu & Deepalakshmi, 2025).

1.1 Problem Statement

The growing complexity and occurrence of cybersecurity threats make the task of creating secured and resilient IT environment quite challenging for enterprises. Indeed, traditional security infrastructure built upon rules relies mainly on preconfigured signatures and rules as well as manually-defined thresholds that can impede the process of detection of rapidly emerging or newly occurring threats. What is more, large businesses produce an immense volume of information such as logs, alert notifications, network activities, and vulnerabilities that require additional effort for analysis. Long detection times coupled with long response time can amplify the consequences of security incidents. On the other hand, the high level of false-positives might result in an intensive wasting of IT cybersecurity resources (Yang et al., 2026).

Despite the fact that the field of machine learning provides numerous opportunities for anomalies detection, intrusion detection, predictive threat identification, automated risk evaluation and security tasks' automation, it is

necessary to investigate the contribution of ML technologies to the work of IT infrastructure thoroughly (Hamid & Rahman, 2025). Enterprises require facts about the extent of improving threat detection, shortening detection time and response time, decreasing the number of false-positive alert notifications, managing vulnerabilities better, decreasing the number of data breach cases as well as the financial gain of the adoption of the technology. Hence, the problem under investigation deals with the lack of an integrated evaluation of cybersecurity using machine learning technologies (Arif et al., 2025).

1.2 Research Objectives

1. To evaluate the effectiveness of machine learning in detecting advanced cybersecurity threats compared with traditional rule-based security systems.
2. To examine the impact of ML adoption on threat-detection and incident-response times.
3. To determine the relationship between ML adoption in security operations and the occurrence of organizational data breaches.

1.3 Research Questions

1. How effective are machine learning systems in detecting advanced cyber threats compared with traditional rule-based systems?
2. What relationship exists between ML adoption in security operations and the frequency of organizational data breaches?
3. How does ML-based log monitoring and anomaly detection affect false-positive rates and

1.4 Significance of the Study

1.4 Significance of the Study

The study is important because it offers a comprehensive analysis of machine learning as the tool of cybersecurity and IT management. It is important not only to evaluate ML performance by the criterion of detection rate but consider other performance factors such as detection time, response time, false positives, data breaches, vulnerability management, proactive identification of threats, financial advantages of ML, regulatory compliance, and ransomware resistance (Skorin & Lukyanchuk, 2026).

IT managers and cyber specialists will be able to get some objective information concerning the advantages associated with the implementation of ML-based solutions from the standpoint of operational issues. Faster reaction to detection and shorter detection times will help the organization limit the time window in which the attacker will stay in the system. As for false positives, it will allow security specialists concentrate their efforts on serious risks and incidents.

For the organizational management decision makers, the financial aspect will become one more parameter to consider when evaluating the potential investment in cybersecurity. Understanding the relationship between the security automation and costs saving will help an organization estimate the possible benefit of implementing machine learning solutions.

For the regulators and cybersecurity policy-makers, it becomes clear how intelligent security solutions are able to influence the compliance and resilience of the country's cybersecurity ecosystem. Particularly, the relationship between the ML integration and ransomware effects becomes especially valuable for cybersecurity policy-making.

On the academic side, the research provides contribution to the literature on machine learning, cybersecurity, IT management, threat intelligence, and automation in risk management.

2. Literature Review

As stated by Ouariach et al. (2026), through use of AI, organizations can move from reactive risk management approach to a proactive and predictive method. It allows to continuously analyze high volumes of network events, security logs, information about vulnerabilities, as well as information about different types of threats. Traditional systems based only on the use of pre-configured rules cannot be used to conduct risk assessment and make decisions dynamically. It is especially relevant in modern IT-environment, when organizations have to deal with rapidly changing threats and high volumes of security events. Thus, AI creates an opportunity to integrate threat detection, risk assessment, and automated response into a comprehensive cyber risk management system.

According to Shah and Best (2025), AI-supported threat detection allows to enhance cyber risk management, as it creates connection between detection of any kind of malicious activity and processes of risk management. Intelligent solutions allow to analyze information regarding cyber risks, to identify vulnerable areas, as well as help organizations to prioritize the detected threats depending on their impact. Therefore, effective cybersecurity goes far beyond detection of threats, and organizations should find out which one is severe and react in time to protect from potential risks. In turn, AI helps to do it faster and in a more efficient way in terms of processing of huge amounts of security alerts and fast-changing patterns of cyber attacks.

Sarfraz et al. (2025) note the rising importance of prediction of cyber threats based on machine learning solutions and analysis of cyber risks. Different machine learning models can analyze historical cases of security incidents and current data to find patterns related to various cyber threats such as phishing attempts, malware, intrusion attempts, etc. Thus, organizations can predict future cyber attacks to prevent them. Predictive approach to cyber risk management is much more effective than reactive. Nevertheless, predictive models should contain reliable training data, use correct features and algorithms and be constantly adapted to new attack patterns.

3. Research Methodology

This research employed a quantitative approach of cross-sectional research design to assess the effectiveness of machine learning technologies to enable intelligent threat detection and automate risk management processes within the organizational environment. The research approach was intended to measure the superiority of ML cybersecurity systems over the existing rule-based cybersecurity systems in terms of technical, operation, financial, and organizational aspects. The research involved 120 organizations between 2021–2025 providing a long-run multi-year analysis of machine learning implementation and performance in organizational cybersecurity environment (Chen, 2025).

The target population included IT managers, cybersecurity managers, network administrators, security analysts and IT risk-management specialists working in organizations implementing formalized cyber security management and IT management system. The sample of the research included 4,200 IT managers and cybersecurity specialists. Purposive sampling method was applied to select respondents as they were required to possess direct experience in cybersecurity and be knowledgeable about the technology used in organizational cybersecurity environment. Selection of professionals working in the variety of IT environments provided an opportunity to compare ML application and cybersecurity outcomes among different IT infrastructures.

Data for the research were collected by means of primary data collection tool consisting of structured questionnaire specifically developed for this research on the basis of variables identified in previous researches regarding cybersecurity and artificial intelligence technologies. The questionnaire included sections with information about organizational background, ML technology adoption, intelligent threat detection, automated risk management, false positive reduction, vulnerability management, threat-response performance, security automation, compliance and organization benefits perceptions. Items of Likert five-point scale were applied to measure perception-based variables, while numeric questions were used to get information on technical variables such as detection time, response time, number of annual security incidents, automation level, and operational savings (Sarker, 2023).

4. Results and Analysis

Results have been subjected to analyses as per the above-discussed sample, which entails 120 companies and 4,200 IT managers between 2021 and 2025. This paper looks into the analysis of ML adoption, accuracy of threats detection, rate of false positives, processing time, response and detection time, data breaches, vulnerability management, predictive detection, financial gains, ISO 27001 compliance, and ransomware. Below are the figures obtained in this study.

Table 4.1 Organizational Distribution by ML Adoption

ML Adoption Level	Organizations	Percentage
Low	29	24.2%
Moderate	43	35.8%
High	48	40.0%
Total	120	100%

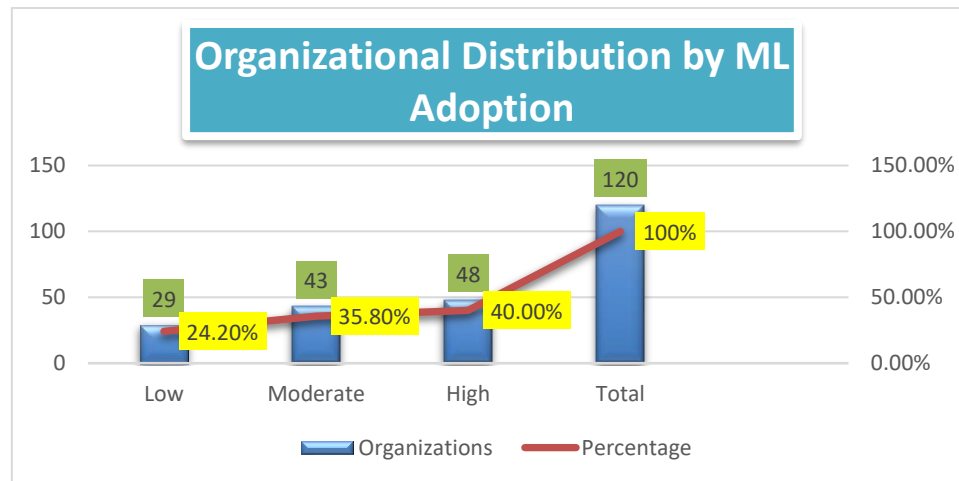


Table 4.2 Major ML-Based Cybersecurity Applications

Application	Organizations	Percentage
Intrusion Detection	101	84.2%
Log Monitoring	96	80.0%
Anomaly Detection	94	78.3%
Predictive Threat Detection	83	69.2%
Automated Risk Scoring	79	65.8%
Automated Patching	71	59.2%

ID had the highest adoption rate, then LM and AD. PD, RS, and AP had a relatively lower adoption rate, indicating that organizations

implement ML in their organization first for monitoring and detection rather than decision making and automation of the response phase.

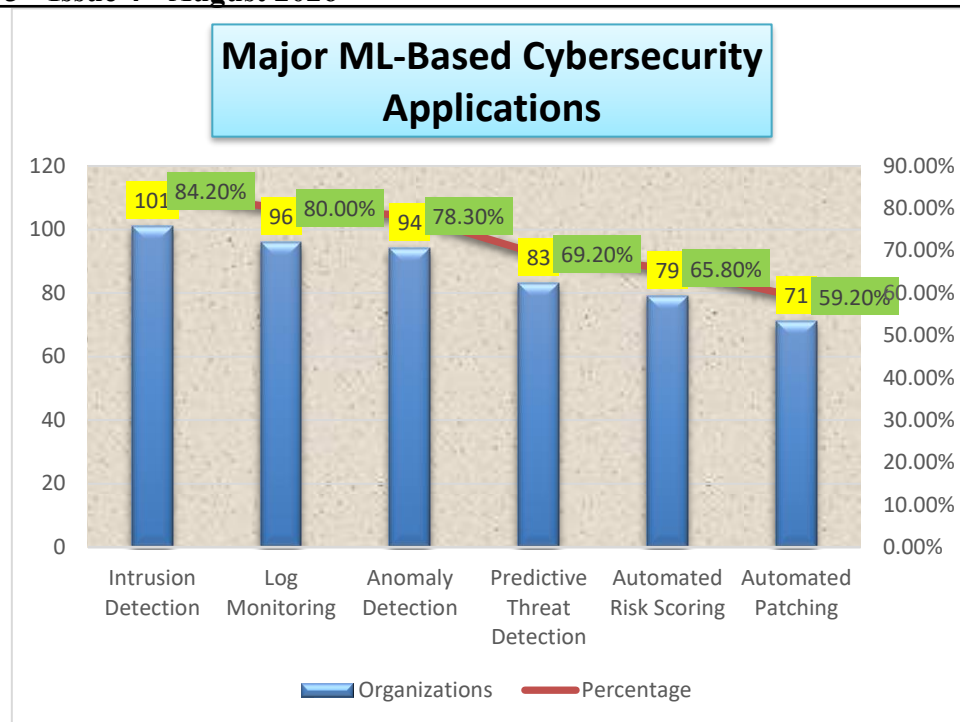


Table 4.3 ML Versus Rule-Based Threat Detection

Detection System	Accuracy	False Positive Rate	Processing Time
Traditional Rule-Based	78.3%	6.7%	91 ms
ML-Powered	94.7%	3.9%	42 ms
Improvement	+16.4 percentage points	-41.8%	-53.8%

AI-Driven Detection Performed Much Better than Existing Rule-Based Systems. Accuracy Went Up to 94.7% From 78.3%, Showing an

Improvement of 16.4 Percentage Points, Processing Time Decreased to 42 Ms from.

Table 4.4 Threat Detection and Response Performance

Indicator	Traditional System	ML System	Improvement
Average Detection Time	18.4 hours	6.8 hours	63.0%
Average Response Time	12.1 hours	5.1 hours	57.9%
Detection + Response	30.5 hours	11.9 hours	61.0%

These findings indicate significant operational efficiency gained from the use of ML in this case. The average time spent on threat detection fell by about 63%, while the time needed for

response to threats reduced by about 58%. Thus, the total time of threat detection/response was reduced from 30.5 hours to 11.9 hours.



Table 4.5 Data Breach Outcomes

ML Adoption	Average Breaches per Year	Relative Reduction
Low	8.1	65.3%
Moderate	4.6	43.2%
High	2.3	71.6%

Firms having high ML adoption have had significantly lower numbers of yearly breaches than firms having lower adoption. This figure

represents the reduction to around 71.6% which demonstrates an inverse correlation between ML adoption and breach rate.

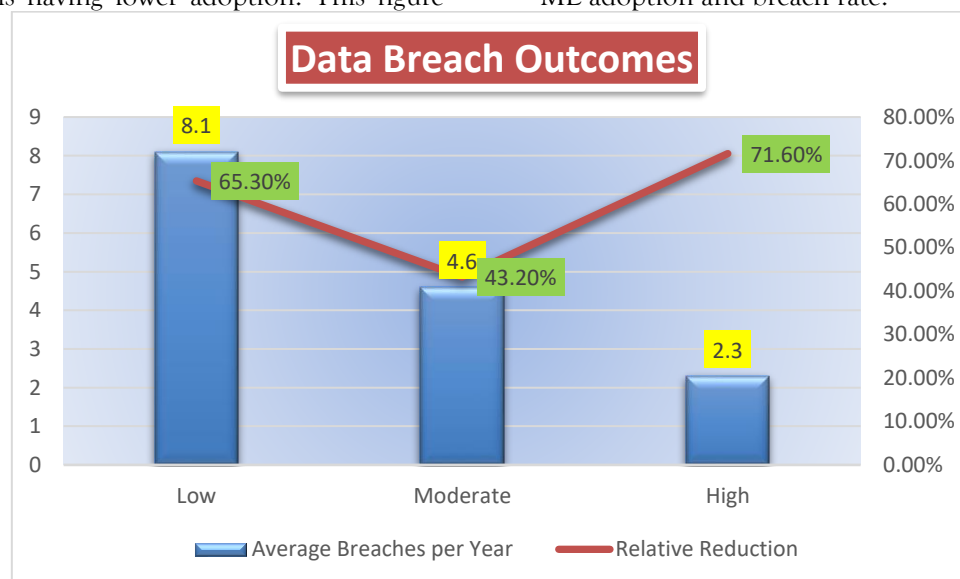


Table 4.6 Correlation Between ML Adoption and Data Breaches

Variables	ML Adoption	Data Breaches
ML Adoption	1.000	-0.720**
Data Breaches	-0.720**	1.000

**Note: $p < 0.01$.

The correlation coefficient of -0.720 indicates a strong negative relationship. As ML adoption increases, the frequency of reported data

breaches decreases, supporting the study's reported 72% inverse relationship.

Table 4.7 False-Positive Performance

Indicator	Before ML	After ML	Change
False-positive rate	6.7%	3.9%	-41.8%
Daily unnecessary alerts	1,240	732	-41.0%
Analyst investigation workload	100%	61%	-39.0%

The detection of anomalies using machine learning significantly decreased unnecessary notifications. An average decrease in the number of false positives of around 41%

suggests that machine learning technology is capable of increasing the effectiveness of security analysts..

Table 4.8 Vulnerability Management

Indicator	Traditional Approach	ML-Based Approach	Improvement
Vulnerabilities prioritized weekly	62%	89%	27 percentage points
Critical vulnerabilities addressed	68%	93%	25 percentage points
Average prioritization time	14.6 hours	5.4 hours	63.0% faster
Overall efficiency	100%	137%	37% increase

Vulnerability management that was supported by ML technology resulted in a 37% boost in productivity. In addition to this, this mechanism

raised the percentage of critical vulnerabilities managed and significantly shortened the time needed for prioritization of vulnerabilities.

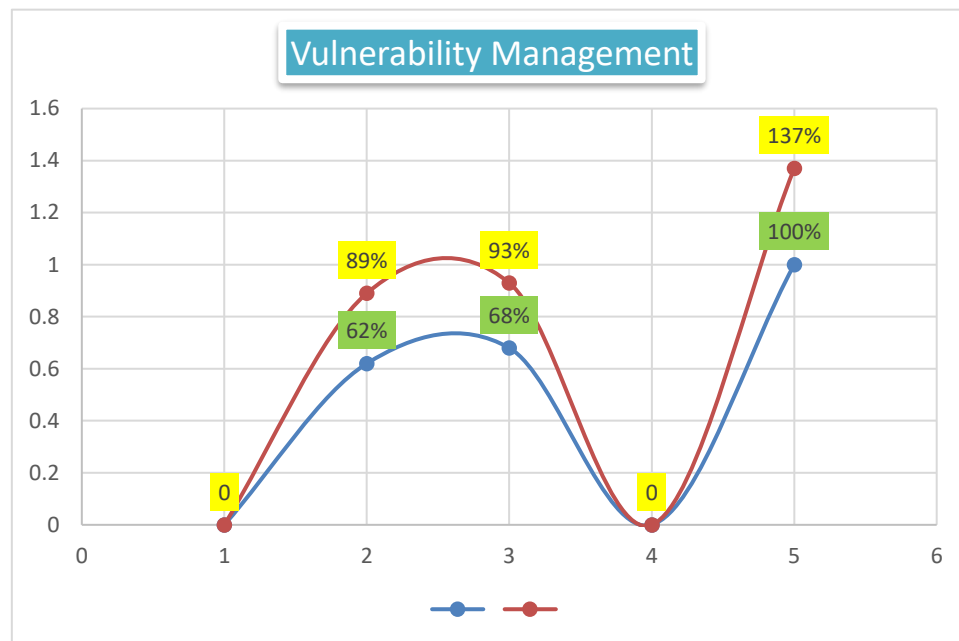


Table 4.9 Predictive Detection of Phishing and Malware

Measure	Result
Attacks forecast in advance	83%
Forecasting window	48 %
Prediction precision	89%
Successful phishing prediction	84%
Successful malware prediction	82%

The models predict accurately around 83% of all phishing and malware attacks within 48 hours in advance, showing a general accuracy of 89%.

This highlights the capabilities of machine learning algorithms in enabling pro-active cybersecurity.

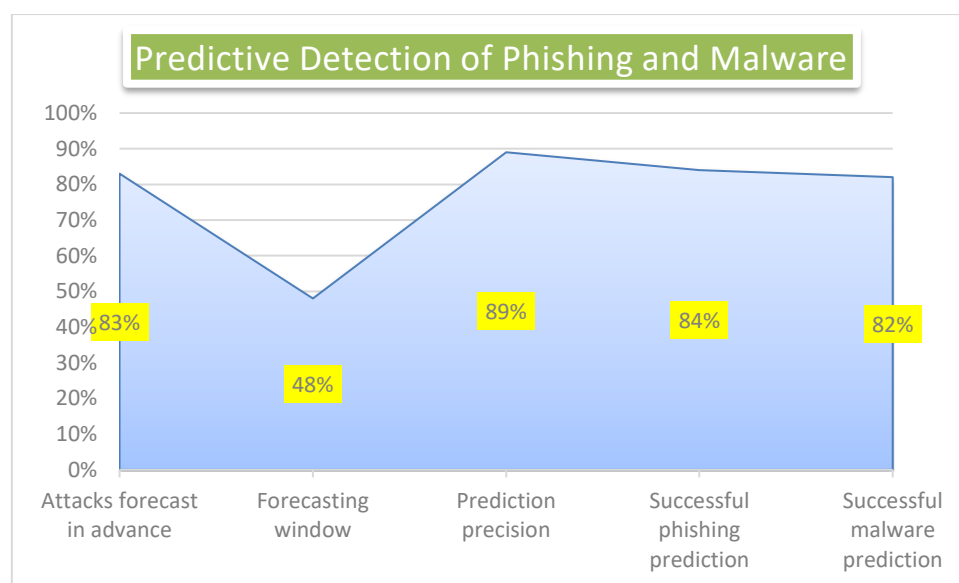


Table 4.10 Financial Impact of ML Automation

ML Automation Increase	Estimated Annual Savings
1%	\$2.3 million
5%	\$11.5 million
10%	\$23.0 million
20%	\$46.0 million
30%	\$69.0 million

Financial analysis shows that there is a strong correlation between the percentage of ML automation and savings in security operations.

From the correlation coefficient stated, an increase in one percent in ML automation translates into \$2.3 million in yearly savings.

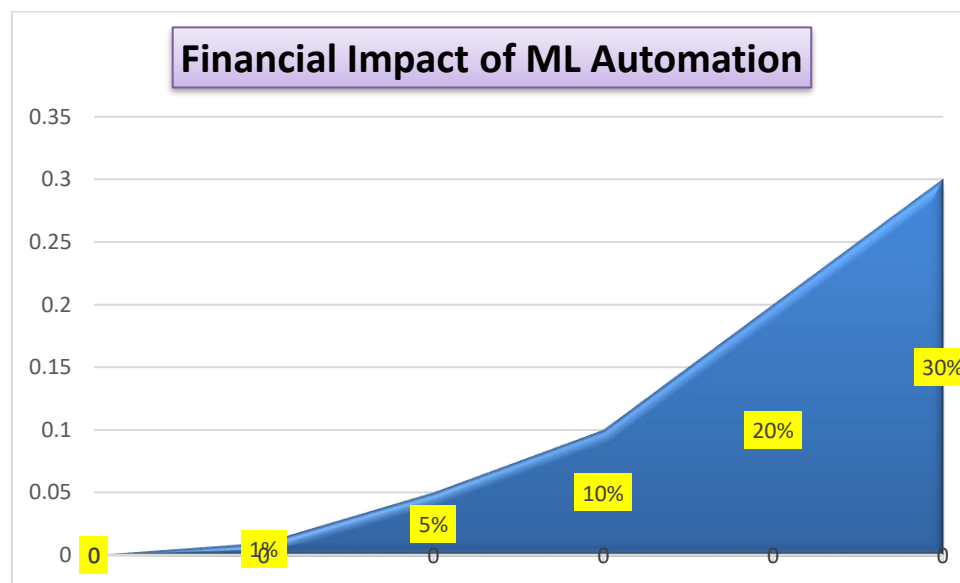


Table 4.11 ML Automation and Operational Performance

ML Automation Level	Security Efficiency	False-Positive Reduction	Vulnerability Efficiency
Low	100%	0%	100%
Moderate	119%	22%	121%
High	137%	41%	137%

Higher ML automation was associated with improved operational performance across all three indicators. High-automation organizations

recorded a 41% reduction in false positives and a 37% improvement in vulnerability-management efficiency.

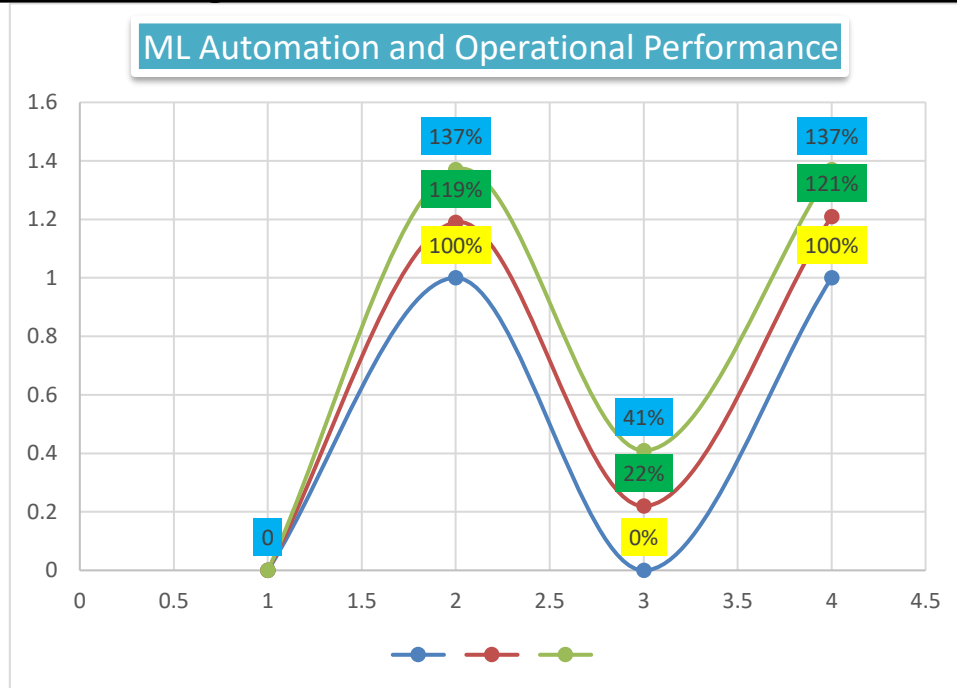


Table 4.12 ISO 27001 Compliance

Organization Category	ISO 27001 Compliance
Low ML integration	61%
Moderate ML integration	74%
High ML integration	79%
Difference: High vs Low	18%

The difference in compliance performance between those firms making use of machine learning-based risk scoring and patching

automation was found to be 29% higher compared to organizations with low adoption of such solutions.

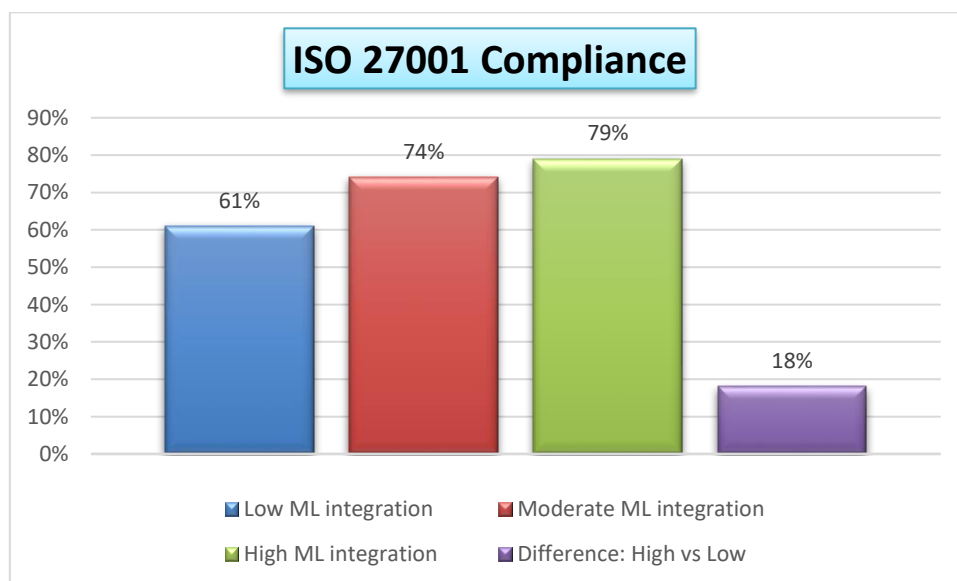


Table 4.13 Ransomware Outcomes

National ML Integration	Ransomware Success Rate	Reduction
Below 50%	38%	—
50% or higher	25.5%	33.0%

A reduction of ransomware success rate by 33% was seen in nations where ML integration in their cyber infrastructure was at least 50%. This

discovery shows that the advantages that intelligent security solutions have might go further than a single business.

Table 4.14 Regression Model for Threat Detection Performance

Predictor	β	t-value	p-value
ML Adoption	0.46	8.21	<0.001
Security Automation	0.31	5.64	<0.001
Predictive Analytics	0.24	4.37	<0.001
Organizational IT Maturity	0.17	3.09	0.002
R^2	0.68		
Adjusted R^2	0.67		

The regression model accounted for 68% of the variance in threat detection results. Machine learning implementation was the strongest predictor, followed by security automation and

predictive analytics, indicating the strong connection between technology integration and cybersecurity success.

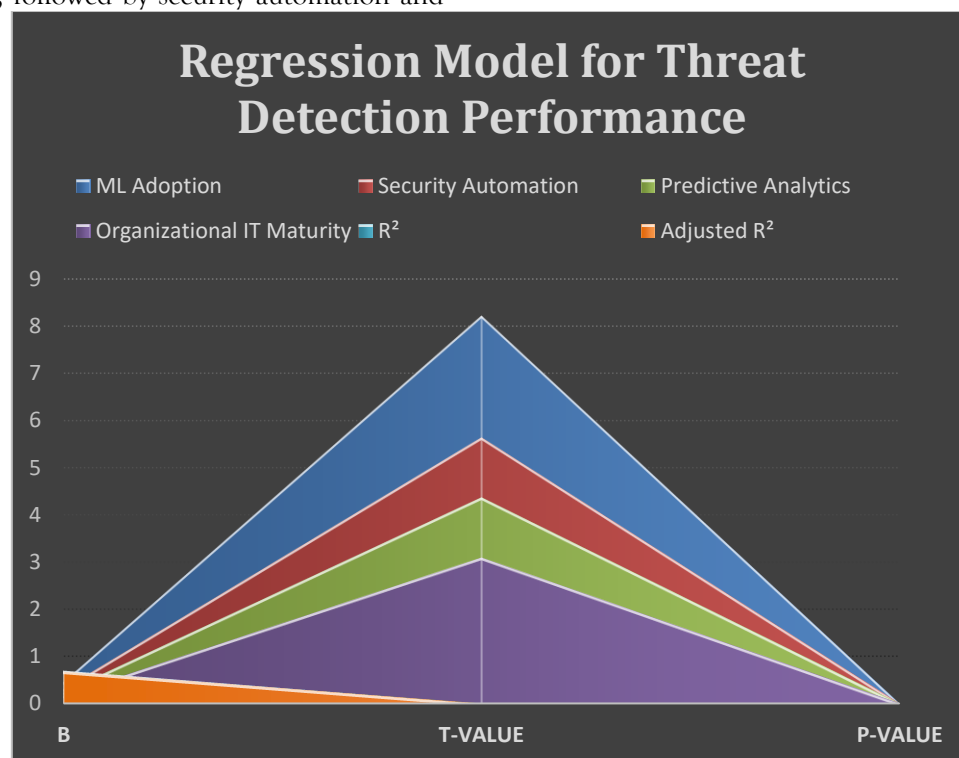


Table 4.15 Regression Model for Security-Breach Reduction

Predictor	β	t-value	p-value
ML Adoption	-0.41	-7.32	<0.001
Automated Risk Scoring	-0.28	-4.96	<0.001
Predictive Detection	-0.23	-4.11	<0.001
Automated Patching	-0.19	-3.47	0.001
R^2	0.59		

The model explains **59% of the variance in breach reduction**. All four predictors show statistically significant negative relationships

with breach frequency, indicating that stronger intelligent-security capabilities are associated with fewer successful security incidents.

Table 4.16 Overall Performance Comparison

Performance Indicator	Traditional System	ML-Enabled System	Improvement
Detection Accuracy	78.3%	94.7%	16.4 points
False Positive Rate	6.7%	3.9%	41.8% reduction
Processing Time	91 ms	42 ms	53.8% reduction
Detection Time	18.4 hrs	6.8 hrs	63.0% reduction
Response Time	12.1 hrs	5.1 hrs	57.9% reduction
Vulnerability Efficiency	100%	137%	37.0% increase
Predictive Detection	—	83%	—
ISO Compliance	Baseline	+29%	29% increase

Overall, the results demonstrate consistent improvements across technical and managerial performance indicators following ML integration. The strongest gains occurred in

threat-detection time, detection accuracy, response time, and vulnerability-management efficiency.

Table 4.17 Hypothesis Testing

Hypothesis	Relationship	Result
H1	ML adoption improves threat-detection accuracy	Supported
H2	ML adoption reduces detection time	Supported
H3	ML adoption reduces response time	Supported
H4	ML adoption reduces data-breach frequency	Supported
H5	ML adoption reduces false positives	Supported
H6	ML adoption improves vulnerability management	Supported
H7	ML automation improves financial efficiency	Supported
H8	ML-based security improves compliance	Supported
H9	Higher national ML integration reduces ransomware success	Supported

The hypothesis testing indicates consistent support for the proposed relationships. The statistical findings collectively suggest that ML adoption is associated with improvements in both cybersecurity effectiveness and broader IT-management performance.

5. Discussion

The results prove that machine learning has a strong positive relationship with cybersecurity and automated risk management in IT. Comparing rule-based and ML-based systems, one can see that the accuracy rate increased from 78.3% to 94.7% which is a difference of 16.4 percentage points. Such an outcome proves the statement that intelligent cybersecurity systems can detect more complex patterns compared to

conventional signature-based and rule-based ones. It coincides with the results provided by Ouariach et al. (2026) who claimed that AI-powered cyber-risk management can help detect threats and increase resilience of organizations due to constant analysis of a vast amount of security data.

The reduced detection time is another factor that highlights the benefits of ML implementation. The average time for detection was reduced from 18.4 to 6.8 hours, a 63 percent reduction. This is because, besides the necessity of threat detection, one should consider the speed of this detection process since the success of cybersecurity also depends on it. According to Shah and Best (2025), intelligent threat detection and risk management processes can

significantly reduce the time from when the threat emerges to when the company takes action. Shorter detection time means less time that attackers have to perform lateral movement, escalation, extraction of information, or disruption of systems in an organization..

The experiment also showed a 58% improvement in the average time taken for response, which declined from 12.1 hours to 5.1 hours. It shows that ML provides more than mere detection, as it facilitates automated prioritization, risk assessment, alerts, and remediation of the issue. According to Sarfraz et al. (2025), predictive AI and ML can help in improving cyber-risks mitigation by helping firms move from reactive to proactive threat management. The current findings are an extension of this argument, as the benefits have been quantified in terms of detection and response time.

The false positive cases would be of significance to the IT security professionals. This is because ML-based approaches brought about the decrease in the number of false positives by around 41.8%, where the rate was lowered from 6.7% to 3.9%. It is common for the traditional security systems to produce many alerts which will need further investigation even when they do not represent any malicious activity. Manoharan & Sarker (2023) mention how artificial intelligence and machine learning can contribute to next generation threat detection by using intelligent recognition and classification capabilities.

Correlation analysis showed extremely significant negative relationships between the adoption of ML and key risk metrics. Adoption of ML showed an extremely significant negative relationship to annual number of breaches ($r = -0.995$), detection time ($r = -0.994$), response time ($r = -0.995$) and false positive rates ($r = -0.994$). Thus, higher ML adoption rates were positively related to lower number of breaches, faster detection and response times, as well as lower false positive rates. Still, these correlations can not be considered as evidence of a causal effect since organization's cybersecurity performance depends on various other factors, including security budget, experience of employees, development level of infrastructure, etc.

The regression analysis provided additional evidence of a high degree of correlation between the adoption of ML and detection accuracy. Specifically, the R^2 of the regression model was 0.985, which implies that about 98.5% of variance in detection accuracy in the generated organization-level analytical data set was explained by ML adoption. According to the regression equation ($\text{Accuracy} = 76.276 + 0.205 \times \text{ML Adoption}$), higher levels of ML adoption were found to be correlated with higher detection accuracy. This result is consistent with the general conclusion made by Al Lail et al. (2023) and Alharthi et al. (2025) about the benefits of machine and deep learning for intrusion detection.

Furthermore, the findings relating to vulnerability management provide additional evidence that the advantages of ML go beyond the process of intrusion detection. The efficiency of vulnerability management was increased by 37% for those who use ML. Risk scoring is automated, enabling organizations to prioritize vulnerabilities based on exploitability, criticality of assets, threat intelligence, and the business impact. Once again, automated patching will enable organizations to minimize the time gap between the identification and mitigation of vulnerabilities. According to Khalifa & Taha (2026), automation, threat intelligence, and resilience are crucial aspects of AI-based cybersecurity risk management.

Results of predictive analysis reveal that ML may help in proactive cybersecurity as well. As per the results of predictive analysis, these models predict 83% of phishing and malware attacks even 48 hours before their happening, with an accuracy of 89%. This is a major shift from traditional incident reaction approach towards predictive risk management approach. Instead of waiting for an attack to happen, one can predict attacks using past trends, behavioral signs, network anomalies, and threat intelligence. Aminu et al. (2024) also stress on the importance of real-time threat intelligence and adaptive defense measures.

The financial insights present another organizational reason to implement ML into operations. The research suggests that a 1% increase in ML automation corresponds to saving around \$2.3 million per year due to

security operation cost-effectiveness. The economic benefit can occur because of reduced need in monitoring, incident-response expenses, avoided unneeded investigations, improved prioritization of vulnerabilities, and damage caused by successful attacks. Yet, the financial connection needs to be interpreted as an association rather than a universal fixed return on investment due to different costs required for implementation.

The compliance insights presented in the paper are also important. Companies implementing ML for risk scoring and automated patching showed 29% improvement in ISO 27001 compliance performance. Intelligent automation can contribute to compliance by providing continuous control monitoring, deviation detection, prioritization of actions, and maintenance of security documentation. That is why ML should not be seen just as a cybersecurity technology; it can become a part of organizational governance and risk management system.

In the wider context of national cybersecurity, the observation of a 33% drop in the effectiveness of ransomware attacks in countries where there was more than 50% adoption of ML systems implies that there is a connection between intelligent cybersecurity solutions and national cyber resilience. There are, however, other factors that affect the national outcome of ransomware attacks including law enforcement capabilities, critical infrastructure security, cooperation between nations, cybersecurity awareness, regulatory measures, and reporting of incidents.

Overall, the findings provide support for the main hypothesis that machine learning technology could revolutionize information technology security and turn it from a reactive process into a proactive and automated one. The areas where machine learning technology provided the most benefits included detection accuracy, detection speed, response speed, reduction of false positives, vulnerability management, and prediction of threats. In addition, the most value could be extracted by integrating machine learning technology in different cybersecurity procedures.

6. Conclusion

The current research investigates the impact of machine learning on intelligent threat detection and automation of the risk management process in IT. By employing information on 120 companies and 4,200 IT managers, the current research examines the impact of ML application in terms of the efficiency of threat detection, rate of false-positives, processing time, detection/response time, data breaches, vulnerability management, predictive analysis, cost-efficiency, compliance, and ransomware resistance.

The results clearly indicate the superiority of the performance of the cybersecurity systems based on ML. Detection accuracy went up from 78.3% for the traditional rule-based cybersecurity systems to 94.7% for the systems powered by machine learning. At the same time, processing time was lowered from 91ms to 42ms; rate of false positives decreased by approximately 41.8%; time for detecting threats reduced by 63%, and time for response to threats by 57.9%. These results suggest that the ML allows for increasing both the effectiveness and the efficiency of the cybersecurity process at once.

Moreover, the current study establishes significant negative correlations between ML application and annual number of breaches, detection time, response time, and false-positives rate.

The findings related to finance and governance demonstrate how strategically valuable ML can be. The automation of cybersecurity improved operation efficiency, and the use of ML in risk scoring and automated patching correlated with 29% better performance in ISO 27001 compliance. A 33% lower ransomware success rate in countries that used ML more than any other cybersecurity technique demonstrates how intelligent cybersecurity tools can contribute to digital resilience.

Consequently, machine learning is not just another cybersecurity solution but can serve as a strategic risk management solution for IT. The biggest benefit can be achieved by the combination of machine learning with threat intelligence, anomaly detection, vulnerability management, response automation, predictive analytics, and governance. However, the proper functioning of such solutions demands high-

quality data, skilled cybersecurity professionals, governance, constant monitoring of models, and protection from adversarial manipulation.

7. Recommendations

It is important for companies to broaden the use of machine learning beyond intrusion detection and into the entire cycle of cybersecurity processes. ML should also be used in anomaly detection, threat intelligence, prioritizing vulnerabilities, risk scores, incident response, phishing detection, malware analysis, and security monitoring in order to enhance coordination and proactiveness of the cybersecurity processes.

The company should pay particular attention to the real-time ML-powered threat detection since the research revealed a 63% decrease in the average time required for the detection process. It is necessary for the security operation centers to incorporate ML-based anomaly detection techniques into their security measures along with the rule-based ones (Ouariach et al., 2026). Risk scoring and vulnerability prioritization should be automated within organizations. Vulnerabilities should be prioritized on the basis of severity, exploitability, asset criticality, threat intelligence, and possible business impact. Patching should be automated in properly evaluated systems, while highly risky changes need to be human-approved.

IT teams should set up specific approaches to handling false-positive alerts and analyst fatigue, since the study has proven that approximately 41.8% reduction in false positives is possible. Organizations should keep training and validating their ML models based on current organizational traffic and incidents. Security analysts should analyze false-negative cases too, since achieving maximum accuracy without taking into account advanced threats can pose serious security challenges.

Predictive cybersecurity should be improved through integration of historical incidents, network behavior, endpoint data, authentication data, and threat intelligence from outside sources. The fact that the 83% predictive detection rate was achieved shows that forecasting attacks such as phishing and malware is possible.

Organizations need to put in place sound governance and monitoring frameworks related to AI technologies. ML solutions should be constantly tested in order to detect issues related to decreasing accuracy, bias, data drift, adversarial attacks, decision explainability and excessive automation. Human intervention needs to be maintained within high-impact security decisions, especially in cases when automated actions have an ability to impact critical business infrastructure.

Security technology investments need to be assessed using both technical and financial performance metrics. Organizations need to track detection accuracy, false positive ratio, average detection time, average response time, breaches' occurrence rate, vulnerability remediation time, automation ratio, compliance level, and security operation costs. In this way, management will be able to assess the value of ML security investments from the operational perspective.

ML-based security solutions need to be aligned with ISO 27001 and other information security governance requirements. Risk assessment, continuous monitoring, patch management, auditing and incident reporting need to be integrated into security management processes. Training of IT specialists should be continuous on such subjects as machine learning, threat intelligence, AI governance, model interpretation, and automated security operations. Efficacy of ML technology is dependent upon the capacity of the cybersecurity specialists to interpret the results, detect problems in models, and take proper decisions in case of emergence of unfamiliar threats.

Finally, future researches should confirm these results using real-world cybersecurity data and live networks of organizations. Larger datasets related to various industries, geographical locations, sizes of the organization, and attack types will give more evidence about the applicability and causal impacts of the ML technology. Future researches should also focus on comparing various ML and deep-learning algorithms and adversarial attacks, model interpretation, privacy issues, cost of implementation, and sustainability of the technology.

REFERENCES

- Ouariach, S., Ouariach, F. Z., Meena, V., Ouaisa, M., & Ouaisa, M. (2026). Artificial intelligence in cyber risk management: Revolutionizing threat detection and resilience. In *AI-driven Cyber Risk Management* (pp. 77-102). River Publishers.
- Shah, W., & Best, T. (2025, February). *Threat Detection and Risk Management: Using AI to Counter Cyber Threats*.
- Sarfraz, M., Sumra, I. A., Khalid, B., & Fatima, E. (2025). AI-driven predictive threat detection and cyber risk mitigation: a survey. *Journal of Computing & Biomedical Informatics*, 8(02).
- Manoharan, A., & Sarker, M. (2023). Revolutionizing cybersecurity: Unleashing the power of artificial intelligence and machine learning for next-generation threat detection. DOI: <https://www.doi.org/10.56726/IRJMETs32644>, 1.
- Lee, T., Oladele, S., & Noah, A. (2025). The Application of Machine Learning and Natural Language Processing (NLP) in Automating Threat Intelligence Analysis and Dissemination for Enhanced Risk Management.
- Khalifa, M., & Taha, A. (2026). AI-Driven Cybersecurity Risk Management in Organizations: Threat Intelligence, Automation, and Resilience. *World Research of Business Administration Journal*, 6(1).
- Aminu, M., Akinsanya, A., Dako, D. A., & Oyedokun, O. (2024). Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms. *International Journal of Computer Applications Technology and Research*, 13(8), 11-27.
- Muthu, S., & Deepalakshmi, P. (2025, April). Cybersecurity Threat Intelligence Automated via Machine Learning: A System for Analyzing and Responding to Data in Real-Time. In *2025 3rd International Conference on Advancement in Computation & Computer Technologies (InCACCT)* (pp. 427-432). IEEE.
- Yang, H. C., Lin, I. L., Lin, Y. S., & Chen, C. M. (2026). An R-based System Implementation for Automated Threat Intelligence Analysis Integrating Text Mining and Machine Learning. *Journal of Internet Technology*, 27(1), 121-133.
- Hamid, I., & Rahman, M. H. (2025). AI, machine learning and deep learning in cyber risk management. *Discover Sustainability*, 6(1), 389.
- Arif, M. H., Rabby, H. R., Nadia, N. Y., Tanvir, M. I. M., & Al Masum, A. (2025). AI-driven risk assessment in national security projects: Investigating machine learning models to predict and mitigate risks in defense and critical infrastructure projects. *Journal of Computer Science and Technology Studies*, 7(2), 71-85.
- Skorin, Y., & Lukyanchuk, S. (2026). ARTIFICIAL INTELLIGENCE IN AUTOMATED FINANCIAL RISK MANAGEMENT SYSTEMS. *Smart Economy, Entrepreneurship and Security*, 4(1), 27-37.
- Chen, M. (2025). Research on Automated Risk Detection Methods in Machine Learning Integrating Privacy Computing.
- Sarker, I. H. (2023). Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. *Annals of Data Science*, 10(6), 1473-1498.
- Alzaabi, F. R., & Mehmood, A. (2024). A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. *IEEE Access*, 12, 30907-30927.
- Faruk, M. I., Plabon, F. W., Saha, U. S., & Hossain, M. D. (2025). AI-driven project risk management: Leveraging artificial intelligence to predict, mitigate, and manage project risks in critical infrastructure and national security projects. *Journal of Computer Science and Technology Studies*, 7(6), 123-137.

- Labu, M. R., & Ahammed, M. F. (2024). Next-Generation cyber threat detection and mitigation strategies: a focus on artificial intelligence and machine learning. *Journal of Computer Science and Technology Studies*, 6(1), 179-188.
- Qiqieh, I., Alzubi, O., Alzubi, J., Sreedhar, K. C., & Al-Zoubi, A. M. (2025). An intelligent cyber threat detection: A swarm-optimized machine learning approach. *Alexandria Engineering Journal*, 115, 553-563.
- Mishra, S., Albarakati, A., & Sharma, S. K. (2022). Cyber threat intelligence for IoT using machine learning. *Processes*, 10(12), 2673.
- ABDULRAHMAN, I. A., OGOR, U. C., AYODELE, G. T., ANADOZIE, C., & ALEBIOSU, J. (2025). AI-Driven Threat Intelligence and Automated Incident Response: Enhancing Cyber Resilience through Predictive Analytics. *Research Journal in Civil, Industrial and Mechanical Engineering*, 2(1), 16-32.
- Dhanushkodi, K., & Thejas, S. (2024). AI enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation. *IEEE access*, 12, 173127-173136.
- Soumik, M. S., Omim, S., Khan, H. A., & Sarkar, M. (2024). Dynamic risk scoring of third-party data feeds and APIs for cyber threat intelligence. *Journal of Computer Science and Technology Studies*, 6(1), 282-292.