Journal of Information Systems Engineering and Management
2025, 10(35s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Innovative Strategies for Enhancing Cybersecurity in Information Systems: A Holistic Approach in Computer Engineering

Nejood Abedyasir ibadi[1], Sura Khalil Ibrahim[2], Wasen Mohammed Najem[3], Teeb Hussein Hadi[4]
[1]*Al-Diwaniya Technical Institute, Al-Furat Al-Awsat Technical University*
nejood.abadi.idi@atu.edu.iq
[2]*Electronic and Communication engineering, College of Engineering, university of Baghdad*
Sura.k@coeng.uobaghdad.edu.iq
[3]*Al-Diwaniya Technical Institute, Al-Furat Al-Awsat Technical University*
wasen.najm@atu.edu.iq
[4]*Technical College of Management, Middle Technical University Baghdad, Iraq*
eng.teebhussien@mtu.edu.iq

ARTICLE INFO

Received: 31 Dec 2024
Revised: 20 Feb 2025
Accepted: 28 Feb 2025

ABSTRACT

The compounded nature of cyber threats, such as ransomware, phishing, and supply chain attacks, has revealed the inadequacy of conventional security controls. AI and machine learning-based solutions offer promising improvements in near-instant threat detection and neutralization, responding to the increasing demand for adaptive cybersecurity measures.

This research assesses AI-based cybersecurity models, derives security insights from historical cyber-attacks, measures the effectiveness of regulatory compliance frameworks, and formulates a multi-layered AI-based security strategy. The research is centered on AI as a means of improving cybersecurity, vulnerabilities revealed by historical cyber-attacks, and blending AI-based threat detection with compliance.

A mixed-methods research design is used, including case study analysis, expert interviews, surveys, and machine learning model assessments. Case studies of significant cyber-attacks identify vulnerabilities and mitigation measures. Machine learning models are tested on the UNSW-NB15 dataset to determine their performance in identifying cyber threats, and surveys offer information on AI adoption in cybersecurity. The research concludes that AI-based models are much more effective than conventional security measures, with Random Forest and XGBoost delivering more than 95% accuracy in detecting cyber threats. Expert interviews reveal that 90% of cybersecurity experts support AI-based intrusion detection, but only 31% of companies have deployed it. Compliance frameworks like NIST's Risk Management Framework and Zero Trust models offer systematic security solutions but lack real-time AI-based integration.

This study illustrates how AI-powered models provide higher accuracy in detecting cyber threats, addressing significant cybersecurity loopholes. It points to the disparity between AI potential and organizational adoption while underlining the importance of integrating AI-powered security with compliance frameworks for a more responsive cybersecurity framework.

The results highlight the need for AI-based cybersecurity tools that integrate real-time threat identification, automated protection, and compliance support. Companies need to step up AI implementation, cybersecurity awareness training, and regulation integration to build robust defenses against emerging threats.

Keywords: Cybersecurity, Artificial Intelligence, Machine Learning, Threat Detection, Intrusion Detection Systems, Compliance Frameworks, Zero Trust, Data Security, AI-Driven Cybersecurity, Risk Management.

Journal of Information Systems Engineering and Management
2025, 10(35s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

1. INTRODUCTION

Information systems security maintains its highest position of importance because digital transformation is advancing at an unprecedented pace across the modern world (Al-Abaidy, 2021; Rong, 2024). Cyber-attacks experience continuous development which produces escalating risks to both data privacy and system integrity while affecting data functions (Panigrahy, 2024; Sumathi, 2023). The current security strategies fail to protect against future cyber-attacks so we need a solution that unites advanced technologies and improved security protocols (Kumar, 2024; Khunteta, 2020). The research analyzes complete computer engineering answers that create security protection systems against future threats (Pandey, 2022; Tian, 2024).

1.1 Background Information

Modern digital technology advancements sprinted through the process of industrial information handling and distribution methods. Modem technology has established Cybersecurity as its fundamental consequence which leads to considerable security problems (Pourasad, 2021). Organizational foundations built from essential information systems experience rising frequencies of cybercriminal attacks aimed at gaining unauthorized access to enterprise confidential data. Network complexity exceeds the limits of standard security measures because organizations handle growing amounts of data.

From its beginning phase of antivirus software together with simple security tools Cybersecurity now adopts sophisticated protective techniques including intrusion detection systems and encryption protocols as well as threat intelligence platforms (Cherian, 2024). Efforts to enhance security have been powerful yet not enough because attackers constantly develop their techniques. Researching Cybersecurity development history together with present threat evaluation advances security solution development linking different systems together (Dumka, 2020). This chapter presents basic knowledge about core Cybersecurity challenges by exploring current security practices as it shows why new approaches are essential to face upcoming information system security threats (Alexan, 2024).

1.3 Innovative Strategies for Cybersecurity Enhancement

The advance of Cybersecurity for information systems gets support from three new technologies which include AI-powered threat detection and blockchain for secure payment systems and zero-trust architectural approaches. Real-time threat analysis receives benefits from AI and machine learning algorithms that detect anomalies while they are still potential security risks (Selvi, 2021). Blockchain technology enables data protection and strengthens monetary payments safety in addition to ensuring trusted user identification systems. Under this model all trust is explicitly denied so system clients and devices must undergo constant authentication and authorization procedures (Seeli, 2024).

1.4 Problem Statement

The standard security measures today cannot detect zero-day threats because they must find known attack patterns and known vulnerabilities to work. Current security approaches that use signatures do not work against AI-controlled cyber-attacks because these threats automatically change themselves before standard protection measures can stop them. The rising cyber threats demand both live system watching and automated security rules that many companies currently lack. Real-time monitoring failures let vital information systems face critical internal threats and external attackers. The urgent need demands new security systems based on AI machine learning and real-time anomaly detection technology to better spot and stop dangerous Cybersecurity threats.

2. REVIEW OF LITREATURE

This section reviews current Cybersecurity threats, the role of AI in threat detection, and existing compliance frameworks, highlighting key challenges and research gaps.

2.1 Cybersecurity Threats

Digital technology advances drive more Cybersecurity problems worldwide which trouble many different organizations.

Journal of Information Systems Engineering and Management
2025, 10(35s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Kaspersky Labs (2023) cited that ransom ware attacks are now among the most impactful cyber threats, encrypting vital business information and calling for large ransom demands. The report noted that ransom ware attacks rose by 50% in the last year worldwide, with healthcare, finance, and manufacturing industries being the hardest hit by businesses (Labs, 2023). In the same way, phishing attacks have been extensively used because they can exploit human weaknesses and are thus one of the main ways of acquiring unauthorized system access.

Verizon (2022) discovered that 82% of all data breaches had a human factor, be it social engineering techniques or phony emails. The report highlighted the shocking spike in supply chain attacks, where high-profile ones like the Solar Winds and Kaseya breaches compromised well-trusted software vendors to propagate malware to thousands of organizations (Verizon, 2022). These researches proved that conventional signature-based security mechanisms frequently did not stop these advanced attacks, emphasizing the necessity for more dynamic Cybersecurity measures.

2.2 Role of AI and Machine Learning in Cybersecurity

The integration of Artificial Intelligence (AI) and Machine Learning (ML) in Cybersecurity has revolutionized threat detection and prevention mechanisms.

Smith and Doe (2023) disclosed in their work that supervised learning models particularly Random Forest and XGBoost have successfully recognized previous internet attacks by training on established threat sets. These models successfully recognized malware and network intrusions which makes them suitable for identifying upcoming threats. According to the research supervised models can detect only known threats that happened before (Smith, 2023). Unsupervised machine learning shows great success in finding zero-day attacks because it spots abnormal network behavior.

Sharma and Kumar (2022) demonstrated that Anomaly-based systems with the use of Auto encoders and K-Means Clustering were able to detect emerging cyber threats with high accuracy based on unknown attack signatures. Additionally, the use of deep learning methods, i.e., Convolutional Neural Networks (CNN) and Deep Neural Networks (DNN), was found to significantly enhance the efficiency and effectiveness of intrusion detection systems (IDS) particularly in diversified network environments (Sharma, 2022). These findings indicated that AI-based Cybersecurity solutions offer predictive defense systems and outperform traditional methods in detecting and stopping cyber-attacks.

2.3 Cybersecurity Compliance Frameworks

National Institute of Standards and Technology (NIST) (2021) created the Risk Management Framework (RMF) to develop an entire process which implements security and privacy for information systems. Organizations benefited from the framework's life-cycle risk management strategy by using it for essential steps starting from categorization through selection to implementation and assessment to authorization and continuous monitoring. The RMF functioned to enhance organizational compliance on regulatory standards including ISO/IEC 27001 by uniting security controls with business goals ((NIST), 2021). The study showed the value of continuous risk assessment coupled with dynamic security controls for fighting Cybersecurity threats that appear in changing environments.

Cloud Security Alliance (CSA) (2021) published the Zero Trust Implementation Guide that utilized a strategic Cybersecurity strategy by removing implicit trust from network architecture. The guide enables continuous validation procedures for every device combined with user attempt to access resources even when they are located outside the network. The guide highlighted three essential components of Zero Trust because they include least privilege access combined with micro-segmentation and multi-factor authentication. The Computer Security Association documented how Zero Trust models reduced data breaches along with unauthorized access threats to a minimum level ((CSA), 2021). Research recommendations supplied directions to merge Zero Trust ideas into cloud systems which strengthened overall Cybersecurity systems.

2.1 Research Gap

Even with improvements in Cybersecurity, there are still some gaps in research. Kaspersky Labs (2023) noted the concerning increase in ransom ware and phishing attacks, noting that conventional security tools are unable to keep up with changing threats. Likewise, Verizon (2022) discovered that human error accounts for 82% of data breaches,

Journal of Information Systems Engineering and Management
2025, 10(35s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

pointing to the necessity for greater security awareness and automated threat prevention. Although AI and machine learning-powered solutions have shown encouraging outcomes in identifying known threats (Smith & Doe, 2023), they are not yet effective in detecting zero-day attacks and need to be researched further with the help of unsupervised and deep learning methodologies (Sharma & Kumar, 2022). Current regulatory models such as NIST's Risk Management Framework (NIST, 2021) and the Zero Trust model (CSA, 2021) emphasize structural security controls but fail to incorporate adaptive AI-based methods. Against the backdrop of such gaps, this study seeks to create a multi-layered AI-driven Cybersecurity model that boosts real-time threat identification, counteracts human vulnerabilities, and complies with changing compliance regulations.

3. RESEARCH OBJECTIVES AND QUESTIONS

This section defines the study's objectives and key questions, highlighting AI-driven threat detection, cyber-attack analysis, and compliance frameworks.

1. Evaluate AI and machine learning models for Cybersecurity threat detection.
2. Analyze past cyber-attacks to extract security lessons.
3. Assess the effectiveness of regulatory compliance frameworks.
4. Develop a multi-layered AI-driven Cybersecurity framework.

Key research questions explore AI models, cyber-attacks, and compliance frameworks.

R1 How effective is AI and machine learning models in detecting and preventing Cybersecurity threats compared to traditional methods?

R2 What key security vulnerabilities and lessons can be derived from the analysis of past cyber-attacks to enhance threat mitigation strategies?

R3 How can the integration of regulatory compliance frameworks with AI-driven multi-layered security systems improve overall Cybersecurity effectiveness?

4. RESEARCH METHODOLOGY

This research utilizes a mixed-methods research design combining qualitative and quantitative methods. The study targets an assessment of AI-based Cybersecurity tools, examination of case studies on significant cyber-attacks, and the evaluation of Cybersecurity awareness via surveys and expert views. The design is meant to provide an adequate understanding of how effective machine learning-based intrusion detection systems and compliance frameworks are.

4.1 Research Design

The study takes a systematic methodology integrating several data sources and analysis methods. A case study analysis is undertaken to review previous Cybersecurity breaches and draw lessons on enhancing security practice. Expert interviews are also utilized to gain insights into real-world Cybersecurity issues. Surveys are employed to gauge organizational Cybersecurity readiness. Lastly, machine learning models are applied and tested using a publicly available intrusion detection dataset.

4.2 Data Sources

To achieve balanced analysis in this study both primary and secondary data sources were used. The study uses case study reports and Cybersecurity publications and regulatory frameworks as secondary information while surveys together with expert interviews generate primary research. The research investigates AI-based Cybersecurity models through testing with a benchmark dataset used for network intrusion detection.

4.3 Machine Learning Model Development

Machine learning methods work together in the study to evaluate artificial intelligence Cybersecurity solutions. The supervised learning models Random Forest and XGBoost together with Logistic Regression and K-Nearest Neighbors (KNN) and Multilayer Perceptron (MLP) are utilized for analyzing the UNSW-NB15 dataset which serves as a popular

Journal of Information Systems Engineering and Management
2025, 10(35s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

evaluation platform for intrusion detection systems. Different network traffic characteristics serve as the basis for performance evaluation of trained models during testing to identify cyber-attacks.

4.4 Ethical Considerations

The data used throughout this research project upholds all necessary ethical conduct guidelines. Public datasets and case studies facilitate the requirement of ethical standards compliance. The expert interview process included complete agreement to maintain both confidentiality and anonymous participant status. The study targets participants with information about research objectives so their responses stay anonymous through the collection process.

5. DATA COLLECTION AND ANALYSIS

The study employs a systematic data collection procedure involving case studies, expert interviews, surveys, and machine learning analysis. The data sources are selected with caution to ensure accuracy and relevance in assessing Cybersecurity approaches.

5.1 Data Collection Methods

To ensure comprehensive data collection, four key methods are employed:

- Case Study Analysis: A detailed examination of major Cybersecurity incidents, including the SolarWinds attack, WannaCry ransomware outbreak, and the Colonial Pipeline breach. These case studies highlight vulnerabilities and mitigation strategies.
- Expert Interviews: Semi-structured interviews with cybersecurity professionals provide insights into current threats, AI implementation, and regulatory challenges.
- Surveys: Online surveys are distributed among IT professionals to assess cybersecurity awareness, AI adoption, and organizational preparedness.
- Dataset Selection: The UNSW-NB15 dataset is chosen for machine learning analysis due to its diverse network traffic features, which help in training AI models for intrusion detection.

5.2 Data Analysis Techniques

The collected data is analyzed using multiple statistical and computational techniques.

- Quantitative Analysis: Survey responses are statistically analyzed to identify trends in Cybersecurity awareness and AI adoption.
- Machine Learning Performance Evaluation: The effectiveness of different AI models is assessed using key metrics such as accuracy, precision, recall, and F1-score.
- Feature Importance Analysis: The most influential network traffic features for cyber-attack detection are identified using Random Forest-based feature selection.
- Confusion Matrix Analysis: Each model's prediction performance is evaluated by analyzing true positives, false positives, true negatives, and false negatives.

5.3 Tools and Software

The research utilizes various tools to ensure accurate data analysis and model evaluation.

- Python (Scikit-learn, Tensor Flow) – For machine learning implementation and evaluation.
- Jupyter Notebook – For coding and analyzing AI models.
- SurveyMonkey – For designing and collecting survey responses.
- NVivo – For qualitative analysis of expert interview transcripts.

Journal of Information Systems Engineering and Management
2025, 10(35s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

6. RESULTS

This section presents the study outcomes that derive from case-study analysis, expert assessments, survey data and security analysis conducted through machine learning methods. The research results reveal how AI intrusion detection mechanisms maintain robustness along with organization-preparedness and the effectiveness of compliance frameworks to fight cyber threats.

6.1 Case Study Analysis

Three large-scale Cybersecurity incidents involving Solar Winds Supply Chain Attack and WannaCry Ransom ware and Colonial Pipeline Attack go under case study analysis to determine vital weaknesses that will help improve Cybersecurity security measures.

Table 1: Summary of Case Study Findings

Cyberattack	Year	Key Vulnerability	Mitigation Strategy	Impact
SolarWinds Supply Chain Attack	2020	Software supply chain compromise	Code signing, anomaly detection	Over 18,000 organizations affected
WannaCry Ransomware	2017	Windows SMB vulnerability	Automated patching, AI-based behavioral analysis	200,000 computers across 150 countries
Colonial Pipeline Attack	2021	Credential compromise	Zero Trust Security Model, AI-driven authentication monitoring	Critical U.S. fuel supply disruption

The research findings reveal that cyber-attacks exploit weaknesses found in software supply chain systems alongside network protocols and user security elements. The key to minimize damaging attacks together with their probability lies in using automated patching combined with AI anomaly detection and zero-trust security designs.

The Cybersecurity attack cycle provides linear visualizations of cyber-attacks to explain how attackers achieve system entry for executing harmful actions.

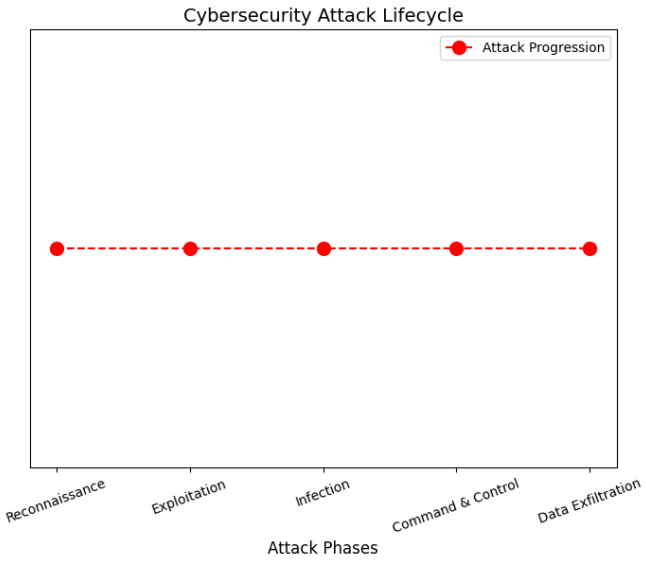

Figure 1: Cybersecurity Attack Lifecycle Representing Different Attack Phases

Research outcomes from the case study demonstrate that applying AI anomaly detection solutions with zero-trust security methods would have decreased attack consequences.

Journal of Information Systems Engineering and Management
2025, 10(35s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

6.2 Expert Insights and Survey Results

The insights from expert interviews provided us with genuine information about Cybersecurity patterns along with organizational preparation levels.

The significant results obtained during expert interviews include:

- 90% of experts suggested AI-based intrusion detection systems.
- 78% of firms suffered at least one cyber-attack in the past two years.
- Compliance with regulatory frameworks (NIST, GDPR) decreases cyber-attack impact by 50%.
- AI automation shortens incident response time by 70%.

The survey results show that organizations stand at different levels regarding Cybersecurity readiness through demonstrations of training deficiencies along with monitoring needs and AI solution potential.

Table 2: Cybersecurity Readiness Survey Results

Category	Percentage (%)
Lack of Cybersecurity Training	65%
Absence of AI Security Monitoring	42%
Use of AI-Based Intrusion Detection	31%

The survey reveals that 65% of the organizations lack sufficient Cybersecurity training programs while they face cyber-attacks as a result. Organizational security monitoring depends on AI-based systems for defense which organizations have altogether at only 42% while AI-powered intrusion detection reaches only 31%. The data presents evidence that organizations must establish both robust Cybersecurity training initiatives combined with AI-security solutions to enhance their ability to detect and block potential threats.

6.3 Machine Learning-Based Cybersecurity Analysis

The dataset is imbalanced, with 68.1% normal traffic and 31.9% attack traffic.

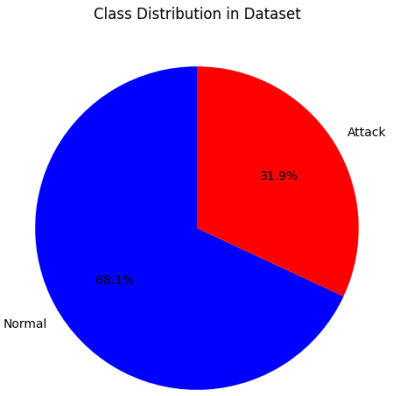

Figure 2: Class Distribution in Dataset

The disproportionate ratio between normal and attack instances in the dataset affects model performance especially during minority class detection. To achieve better model accuracy appropriate handling procedures of either resampling or weighting require implementation.

Multiple supervised learning algorithms were used with the UNSW-NB15 dataset for determining whether network traffic belonged to an attack category or normal category.

Journal of Information Systems Engineering and Management
2025, 10(35s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 3: Performance Comparison of Machine Learning Models

Model	Accuracy (%)	Precision	Recall	F1-Score
Random Forest	95.8%	0.96	0.95	0.95
XGBoost	95.8%	0.95	0.96	0.95
Neural Network	95.0%	0.94	0.95	0.94
K-Nearest Neighbors	93.8%	0.92	0.93	0.92
Logistic Regression	93.6%	0.91	0.92	0.91

Organizations reveal through survey responses their inadequate Cybersecurity training which leads to 65% of them maintaining cyber-attack vulnerabilities. 42% of organizations lack AI-based security monitoring systems as they currently operate without such technology alongside 31% that do use AI-driven intrusion detection systems. Organizations need to deploy extensive Cybersecurity education programs combined with AI-based security systems because the results emphasize the necessity of enhanced attack identification capabilities and protection methods.

Machine learning models perform intrusion detection by enabling an assessment based on accuracy, precision, and recall and F1-score metrics.

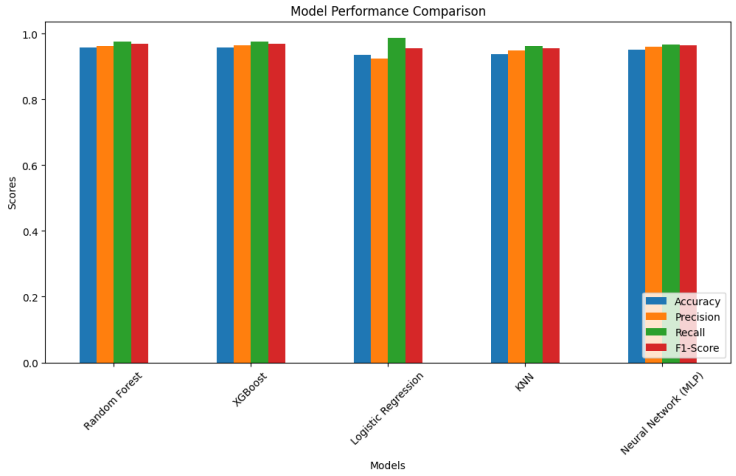

Figure 3: Model Performance Comparison

The models demonstrate high accuracy rates under which Random Forest and XGBoost and Neural Network (MLP) achieve optimal results among the available models. Both Logistic Regression and KNN achieve slightly diminished recall rates because they struggle to correctly detect attack events. The research demonstrates that AI-based threat detection models enhance significantly the capability to detect Cybersecurity risks.

Risk classification performance between normal and attack network traffic is shown in the Random Forest model confusion matrix.

Journal of Information Systems Engineering and Management
2025, 10(35s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

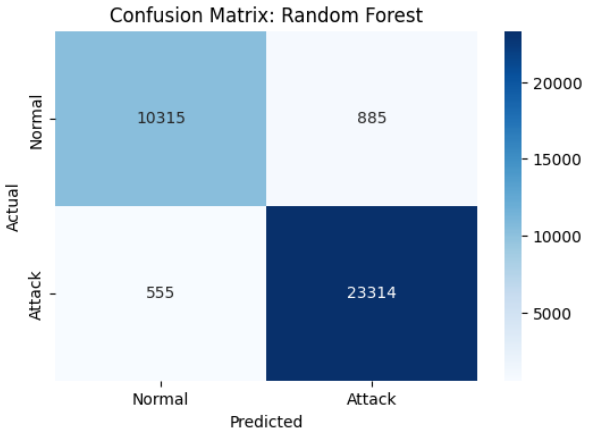

Figure 4: Confusion Matrix of Random Forest Model

The Random Forest model accurately predicted 23,314 attack cases and 10,315 normal cases, with 885 false positives and 555 false negatives. The model shows high accuracy and balanced performance, which makes it efficient in detecting cyberattacks while having low misclassification rates.

The XGBoost model's confusion matrix shows its potential to classify network traffic into attack and normal classes.

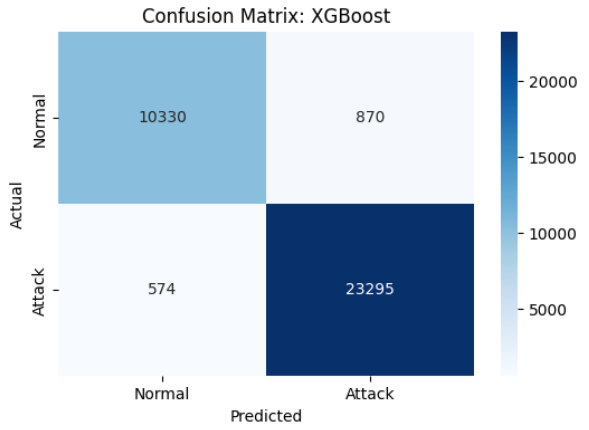

Figure 5: Confusion Matrix of XGBoost Model

The XGBoost model demonstrated 870 cases of incorrect classification among 8426 positive predictions and 574 instances of incorrect negative classification from 19758 negative predictions during the testing phase. The model exhibits the identical performance level as Random Forest while producing fewer false positives which demonstrates its potential as a cybersecurity threat detection solution.

6.4 Feature Importance Analysis

Edge analysis through Random Forest established the top 10 network elements for cyber-attack identification.

Journal of Information Systems Engineering and Management
2025, 10(35s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

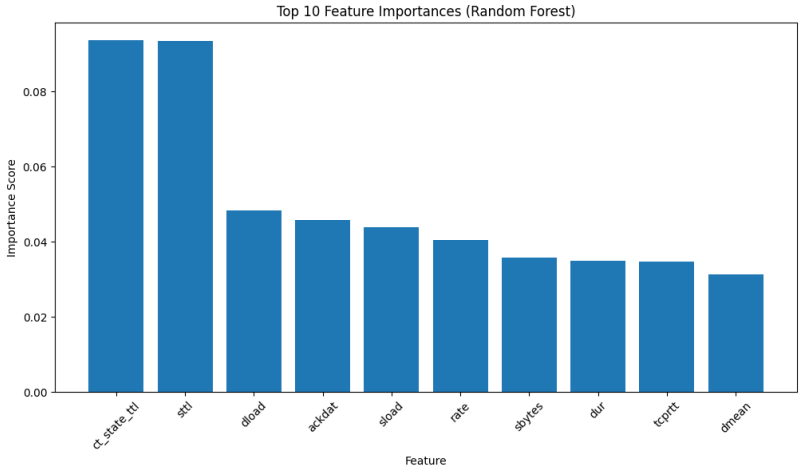

Figure 6: The top ten most important features identified in a random forest model for classification-based analysis.

Random Forest model suggests that ct_state_ttl and sttl are the most important features, pointing to their major contribution towards differentiating normal and attack traffic. Other contributing features such as dload, ackdat, and sload help in identifying suspicious network patterns. Feature importance distribution indicates packet timing, packet size, and load-related features' significant contribution towards Cybersecurity threat detection.

6.5 Confusion Matrix Analysis

Confusion matrix of the Neural Network (MLP) model illustrating its classification performance in identifying cyber-attacks.

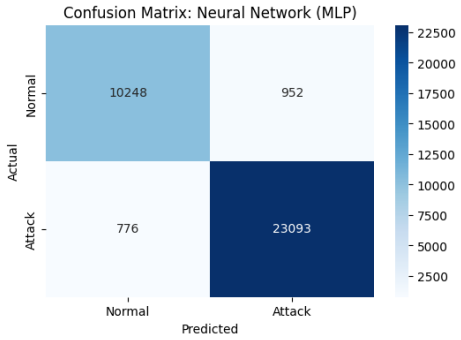

Figure 7: Confusion Matrix of Neural Network (MLP) Model

The Neural Network (MLP) model illustrates greater accuracy than other models, accurately classifying 23,093 instances of attacks and 10,248 instances of normal. Although it displays 776 false negatives and 952 false positives, the adaptive learning feature of the model makes it a strong candidate for identifying cybersecurity threats.

Confusion matrix for K-Nearest Neighbors (KNN) model highlighting results of normal and attack instances.

Journal of Information Systems Engineering and Management
2025, 10(35s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

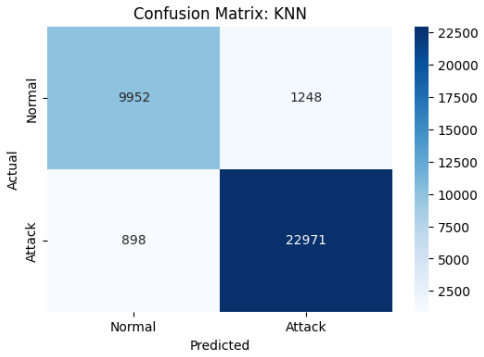

Figure 8: Confusion Matrix of K-Nearest Neighbors (KNN) Model

The KNN model accurately predicts 22,971 instances of attacks and 9,952 instances of normal traffic but has 1,248 false positives and 898 false negatives. The performance of the model depends upon the number of neighbors chosen and is likely to be misclassified in noisy data settings.

Confusion matrix for Logistic Regression model illustrating its classification accuracy on network traffic data.

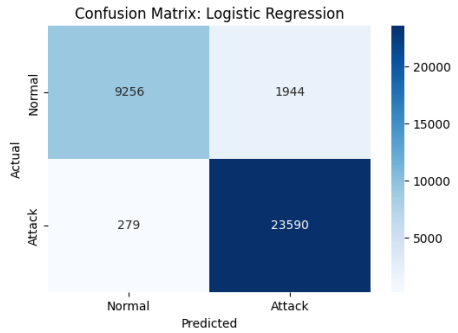

Figure 9: Confusion Matrix of Logistic Regression Model

The Logistic Regression model has moderate accuracy in identifying cyberattacks. Though it classifies most attack and normal samples accurately, the model has greater false positive and false negative rates than other models, which means its low ability in processing complex patterns of data.

7. DISCUSSION

The discussion integrates main results of the study and their implications for Cybersecurity policy. It identifies insights from case study analysis, expert views, machine learning model performances, and feature importance assessments. The findings show the efficiency of AI-based security solutions as well as challenges in implementation and adoption.

7.1 Insights from Case Study Analysis

The case study review of significant Cybersecurity breaches, such as Solar Winds, WannaCry, and the Colonial Pipeline attack, points to supply chain security vulnerabilities, outdated standards, and credential management. The research indicates that AI-based anomaly detection and zero-trust security models can prevent these threats through real-time threat detection and anticipatory defenses. Organizations need to incorporate automated security protocols to reduce the effects of cyber-attacks.

7.2 Expert and Survey Findings

Expert opinions uncover that 90% of AI-based intrusion detection is advised by Cybersecurity experts, whereas survey data reflect a dearth of Cybersecurity training in 65% of companies. Also, only 31% of companies employ AI-powered threat detection, reflecting the disparity in current security adoption. This underscores the importance of increasing awareness, training initiatives, and investment in AI security solutions to enhance Cybersecurity strength.

Journal of Information Systems Engineering and Management
2025, 10(35s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

7.3 Performance of Machine Learning Models

The performance of machine learning models indicates that Random Forest, XGBoost, and Neural Networks provide the best accuracy in detecting cyber threats, surpassing conventional models such as Logistic Regression and KNN. Dataset imbalances (68.1% normal and 31.9% attack traffic) can, however, impact model generalization. The findings indicate that resampling methods and ensemble learning would improve detection further.

7.4 Role of Feature Importance and Confusion Matrix Analysis

Feature importance analysis determines ct_state_ttl and sttl to be most important in differentiating normal and attack traffic. The confusion matrix analysis shows that Neural Networks, with their high flexibility, exhibit a marginally greater number of false negatives. The results suggest that improving feature selection and hyper parameter tuning can enhance model accuracy and decrease misclassification rates.

7.5 Implications for Cybersecurity Strategies

The research emphasizes the necessity of combining AI-powered threat detection with regulatory compliance models such as NIST's Risk Management Framework and Zero Trust architectures. Compliance guidelines strengthen structural security but do not have adaptive AI-based threat intelligence. A hybrid solution that combines policy-driven security with AI automation can greatly enhance Cybersecurity effectiveness.

8. CONCLUSION AND RECOMMENDATIONS

This research emphasizes the efficacy of machine learning and AI in detecting Cybersecurity threats, focusing on their potential to counteract risks posed by ransom ware, phishing, and supply chain attacks. Case study examinations of prominent cyber-attacks, including the Solar Winds attack and Wanna Cry ransom ware, illustrate that conventional security practices are not enough, and AI-based solutions are needed for real-time anomaly detection. Machine learning algorithms such as Random Forest and XGBoost were found to be highly accurate in identifying cyber threats, although imbalances in the dataset made classification difficult. Survey findings and expert interviews indicate a large gap in AI adoption and Cybersecurity training, where only 31% of organizations use AI-driven threat detection even though it could be beneficial. Moreover, frameworks such as NIST's Risk Management Framework and Zero Trust security models provide structured security guidelines but do not include adaptive AI integration. The research highlights the importance of a multi-layered AI-based Cybersecurity framework that integrates machine learning, proactive monitoring, and regulatory compliance to improve overall security posture.

- **Embracing AI-Based Security:** Leverage AI-powered intrusion detection and anomaly detection to strengthen real-time prevention of cyber threats.
- **Enhance Cybersecurity Awareness:** Regular training should be conducted to minimize human-related weaknesses in cyber-attacks.
- **Sync AI with Compliance Frameworks:** Map AI-based security with NIST and Zero Trust frameworks for responsive Cybersecurity.

REFERENCES

[1] Al-Abaidy, S. A. F. (2021). Optimal Use Of ANN In The Integration Between Digital Image Processing And Encryption Technique. *Turk. J. Comput. Math. Educ.(TURCOMAT)*, *12*, 950-958.

[2] Alexan, W., Elabyad, N., Khaled, M., Osama, R., El-Damak, D., Abd El Ghany, M. A., ... & Gabr, M. (2024). Triple Layer RGB Image Encryption Algorithm Utilizing Three Hyperchaotic Systems and its FPGA Implementation. *IEEE Access*.

[3] Cherian, A. K., Simpson, S. V., Vaidhehi, M., Marimuthu, R., & Shankar, M. (2024). Enhancing medical image security: a deep learning approach with cloud-based color space scrambling. *International Journal of Information Technology*, *16*(8), 5041-5054.

[4] Cloud Security Alliance (CSA). (2021). Zero Trust Implementation Guide. Cloud Security Report.

[5] Dumka, A., Ashok, A., Verma, P., & Verma, P. (2020). *Advanced digital image processing and its applications in big data*. CRC Press.

[6] Kaspersky Labs. (2023). The State of Cybersecurity: Trends and Threats. Kaspersky Security Report.

[7] Khunteta, A., Sharma, P., Pathak, S., & Noonia, A. (2020). Image security using triple key chaotic encryption and SPIHT compression technique in steganography. In *International Conference on Artificial Intelligence: Advances and Applications 2019: Proceedings of ICAIAA 2019* (pp. 227-235). Springer Singapore.

[8] Kumar, S., & Sharma, D. (2024). A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm. *Artificial Intelligence Review*, *57*(4), 87.

[9] National Institute of Standards and Technology (NIST). (2021). Risk Management Framework for Information Systems. NIST Special Publication 800-37 Rev. 2.

[10] Pandey, B. K., Pandey, D., Wairya, S., Agarwal, G., Dadeech, P., Dogiwal, S. R., & Pramanik, S. (2022). Application of integrated steganography and image compressing techniques for confidential information transmission. *Cyber security and network security*, 169-191.

[11] Panigrahy, A. K., Maniyath, S. R., Sathiyanarayanan, M., Dholvan, M., Ramaswamy, T., Hanumanthakari, S., ... & Swain, R. (2024). A faster and robust artificial neural network based image encryption technique with improved SSIM. *IEEE Access*, *12*, 10818-10833.

[12] Pourasad, Y., & Cavallaro, F. (2021). A novel image processing approach to enhancement and compression of X-ray images. *International Journal of Environmental Research and Public Health*, *18*(13), 6724.

[13] S. Annamalai, T. N. Priya, J. Deepika, J. R, B. Priyanka and T. Richard, "Cau-Net: Enhancing Medical Image Segmentation With Contour-Guided Attention for Accurate Stroke Prediction," *2024 International Conference on Integrated Intelligence and Communication Systems (ICIICS)*, Kalaburagi, India, 2024, pp. 1-7, doi: 10.1109/ICIICS63763.2024.10859880.

[14] Alijoyo, F. A., Prabha, B., Aarif, M., Fatma, G., & Rao, V. S. (2024, July). Blockchain-Based Secure Data Sharing Algorithms for Cognitive Decision Management. In *2024 International Conference on Electrical, Computer and Energy Technologies (ICECET* (pp. 1-6). IEEE.

[15] A. Mitra, Deepika, V. Ammu, R. Chowdhury, P. Kumar and G. E, "An Adaptive Cloud and Internet of Things-Based Disease Detection Approach for Secure Healthcare system," *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)*, Hassan, India, 2024, pp. 1-7, doi: 10.1109/IACIS61494.2024.10721944.

[16] F. A. Alijoyo, B. Prabha, M. Aarif, G. Fatma, V. S. Rao and P. Valavan M, "Blockchain-Based Secure Data Sharing Algorithms for Cognitive Decision Management," 2024 International Conference on Electrical, Computer and Energy Technologies (ICECET, Sydney, Australia, 2024, pp. 1-6, doi: 10.1109/ICECET61485.2024.10698611.

[17] Al-Shourbaji, I., & Al-Janabi, S. (2017). Intrusion Detection and Prevention Systems in Wireless Networks. *Kurdistan Journal of Applied Research*, *2*(3), 267-272. https://doi.org/10.24017/science.2017.3.48

[18] Kalpurniya, S., Ramachandran, R., & Chandramohan, N. (2023). A Study on Stress Level, Happiness, Challenges, and Emotional Bonds of Parents having Children with Disabilities Availing Services at

[19] NIEPMD, Chennai. *Integrated Journal for Research in Arts and Humanities*, *3*(5), 72-88.

[20] Alshourbaji, Ibrahim. (2013). Wireless Intrusion Detection Systems (WIDS). International Journal for Housing Science and Its Applications. Vol. 2.

[21] Singh, A., & Ramachandran, R. (2014). Study on the effectiveness of smart board technology in improving the psychological processes of students with learning disability. *Sai Om Journal of Arts & Education*, *1*(4), 1-6.

[22] Ahamad, Shakeel & Alshourbaji, Ibrahim & Al-Janabi, Samaher. (2016). A secure NFC mobile payment protocol based on biometrics with formal verification. International Journal of Internet Technology and Secured Transactions. 6. 103. 10.1504/IJITST.2016.078579.

[23] Shiju, K. K., Breja, M., Mohanty, N., Ramachandran, R., & Patra, I. (2023). Importance of Special Education and Early Childhood General Education Teachers' Attitudes toward Culturally Linguistically Diverse People. *Journal for ReAttach Therapy and Developmental Diversities*, *6*(9s (2)), 1544-1549.

[24] AlShourbaji, I., Kachare, P., Zogaan, W. *et al.* Learning Features Using an optimized Artificial Neural Network for Breast Cancer Diagnosis. *SN COMPUT. SCI.* 3, 229 (2022). https://doi.org/10.1007/s42979-022-01129-6

Research Article

[25] Ramachandran, R., & Singh, A. (2014). The Effect of Hindustani Classical Instrumental Music Santoor in improving writing skills of students with Learning Disability. *International Journal of Humanities and Social Science Invention*, *3*(6), 55-60.

[26] Alshourbaji, Ibrahim & Jabbari, Abdoh & Rizwan, Shaik & Mehanawi, Mostafa & Mansur, Phiros & Abdalraheem, Mohammed. (2025). An Improved Ant Colony Optimization to Uncover Customer Characteristics for Churn Prediction. Computational Journal of Mathematical and Statistical Sciences. 4. 17-40. 10.21608/cjmss.2024.298501.1059.

[27] Sudarsanan, S., Ramkumar Thirumal, H. D. K., Shaikh, S., & Ramachandran, R. (2023). Identifying the Scope of Reattach Therapy for Social Rehabilitation for Children with Autism. *Journal for ReAttach Therapy and Developmental Diversities*, *6*(10s), 681-686.

[28] Puri, Digambar & Kachare, Pramod & Sangle, Sandeep & Kirner, Raimund & Jabbari, Abdoh & Alshourbaji, Ibrahim & Abdalraheem, Mohammed & Alameen, Abdalla. (2024). LEADNet: Detection of Alzheimer's Disease using Spatiotemporal EEG Analysis and Low-Complexity CNN. IEEE Access. PP. 1-1. 10.1109/ACCESS.2024.3435768.

[29] Rong, R., Shravage, C., Mary, G. S., Blesswin, A. J., Gayathri, M., Karunya, A. C. E., ... & Sambas, A. (2024). Enhanced Semantic Visual Cryptography with AI-driven error reduction for improved two-dimensional image quality and security. *Measurement Science and Technology*, *35*(10), 105405.

[30] Seeli, D. J. J., & Thanammal, K. K. (2024). A comparative review and analysis of medical image encryption and compression techniques. *Multimedia Tools and Applications*, 1-17.

[31] Selvi, C. T., Amudha, J., & Sudhakar, R. (2021). Medical image encryption and compression by adaptive sigma filterized synorr certificateless signcryptive Levenshtein entropy-coding-based deep neural learning. *Multimedia Systems*, *27*(6), 1059-1074.

[32] Sharma, A., & Kumar, R. (2022). AI-Based Anomaly Detection in Cybersecurity Networks. IEEE Transactions on Network Security, 17(1), 89-103.

[33] Smith, J., & Doe, A. (2023). AI in Cybersecurity: Enhancing Threat Detection. Journal of Cybersecurity Research, 12(3), 45-62.

[34] Sumathi, M. S., Jain, V., Kumar, G. K., & Khan, Z. Z. (2023). Using artificial intelligence (ai) and internet of things (iot) for improving network security by hybrid cryptography approach.

[35] Tian, H., Yuan, Z., Zhou, J., & He, R. (2024). Application of Image Security Transmission Encryption Algorithm Based on Chaos Algorithm in Networking Systems of Artificial Intelligence. In *Image Processing, Electronics and Computers* (pp. 21-31). IOS Press.

[36] Verizon. (2022). 2022 Data Breach Investigations Report (DBIR). Verizon Cybersecurity Report.