Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

AI-Driven Collaborative Cybersecurity Development: A Prototype Implementation of a Cybersecurity Framework for Educational Institutions of Camarines Norte

Frank Kiven B. Ablao[1*], Thelma D. Palaoag[2]
[1] *Student, College of Information Technology and Computer Science, University of the Cordilleras, Baguio City, Philippines. fba1761@students.uc-bcf.edu.ph*
[2] *Faculty, College of Information Technology and Computer Science, University of the Cordilleras, Baguio City, Philippines. tpalaoag@gmail.com*

ARTICLE INFO

Received: 29 Dec 2024

Revised: 12 Feb 2025

Accepted: 27 Feb 2025

ABSTRACT

Cyber threats targeting educational institutions have become increasingly sophisticated, requiring proactive detection and rapid response measures. This study presents an integrated framework that combines an AI-driven threat detection system with the Malware Information Sharing Platform (MISP) to enhance cyber defenses in school networks. Leveraging a Design Science Research methodology, the project unfolds across four phases: system design and architecture, prototype implementation, pilot testing, and evaluation.

In the system design phase, requirements were gathered to develop an end-to-end architecture on Amazon Web Services (AWS), encompassing real-time data ingestion through Amazon Kinesis and Amazon Simple Email Service, data storage on Amazon S3, and AI-based anomaly and phishing detection using AWS Lambda. The prototype stage featured the integration of Random Cut Forest (RCF) for unsupervised anomaly detection and DistilBERT for phishing classification, enabling near real-time analysis of network and email data streams. MISP was hosted on Amazon EC2 and integrated with external threat feeds via STIX/TAXII, creating a closed-loop system that continuously refines shared Indicators of Compromise (IoCs).

Pilot testing involved three schools in Camarines Norte, where simulated attack scenarios validated the system's practical effectiveness. Results revealed high detection accuracy, with reduced false positives once IoCs were regularly enriched through MISP. The automated alerting workflow significantly shortened time-to-detection and time-to-response when compared to traditional security approaches.

Quantitative metrics confirmed improvements in detection speed, precision, and recall, while qualitative feedback highlighted the system's ease of use, scalability, and cost efficiency. These findings underscore the potential of AI-enhanced solutions underpinned by threat intelligence sharing, illustrating a robust, sustainable approach to improving cybersecurity in the education sector.

Keywords: AI-Driven Threat Detection, Malware Information Sharing Platform, Cloud Computing, Threat Intelligence, Cybersecurity in Education, Anomaly Detection, Random Cut Forest, Phishing Detection, DistilBERT, Design Science Research

INTRODUCTION

The rapid digitalization of educational institutions has undoubtedly streamlined administrative and academic operations. However, this transformation has also made schools and universities increasingly vulnerable to sophisticated cyber threats such as phishing, ransomware, and advanced persistent threats (APTs). These threats pose significant risks, potentially exposing sensitive student and faculty information, disrupting educational activities, and inflicting substantial financial and reputational damage. Effectively addressing these challenges demands a modern, cooperative security approach that unites robust threat detection with efficient incident response.

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Many educational institutions in Camarines Norte still rely on conventional cybersecurity practices—primarily localized defenses like antivirus solutions and firewalls. Due to limited resources, they often lack holistic Security Information and Event Management (SIEM) systems, operating instead in isolated security silos. This increases their susceptibility to rapidly evolving cyber threats. A more effective strategy involves leveraging collective intelligence via cyber threat intelligence (CTI) sharing and incorporating artificial intelligence (AI) and machine learning (ML) to enhance detection and response. By centralizing these capabilities, institutions with constrained resources can better protect themselves against complex attacks[1].

This study builds on two previous research efforts that established a conceptual framework for a collaborative cybersecurity system suited to educational institutions. The first study [2] proposed a CTI-sharing model among colleges in Camarines Norte, employing the Malware Information Sharing Platform (MISP) on Amazon Web Services (AWS) to securely distribute threat data. This framework, guided by the Input-Process-Output (IPO) model, provided an architectural blueprint for collective threat intelligence workflows; however, it did not involve practical implementation or validation.

The second study [3] extended the initial framework by incorporating AI/ML methods. Through a systematic literature review, it identified unsupervised learning, deep learning, and federated learning as feasible approaches for detecting cyber threats in educational environments. The research highlighted how AI-powered analytics could offer real-time threat detection, adaptive learning, and improved accuracy—all while addressing critical issues such as data privacy and limited local datasets.

Despite providing a strong theoretical basis, these two studies did not offer an in-depth examination of real-world application and assessment. Consequently, the present research focuses on developing and evaluating a prototype of a collaborative cybersecurity framework that integrates MISP, AWS, and AI-driven techniques to enhance threat detection and incident response. By adopting a centralized model with a pre-trained AI using unsupervised and deep learning methods, the system seeks to remain simple to deploy and resource-efficient for educational institutions.

By prototyping the framework, this study seeks to determine how a collaborative cybersecurity system integrating MISP on AWS with AI-driven analysis can potentially enhance threat response time and incident management in educational settings. Specifically, the research aims to integrate MISP with AI-driven threat analysis, validate end-to-end security workflows under controlled conditions, and measure the resulting improvements in threat detection and response.

METHODS AND METHODOLOGY:

This study employs the Design Science Research (DSR) methodology, selected for its effectiveness in developing practical, innovative IT solutions addressing real-world cybersecurity challenges. The methodology comprises four phases aligned with the research objectives: (1) System Design and Architecture, (2) Prototype Implementation, (3) Pilot Testing, and (4) Evaluation and Metrics.

Phase 1: System Design and Architecture

This phase involves gathering requirements, defining detailed specifications, and designing a comprehensive system architecture. Figure 1 illustrates the high-level integration between AWS-hosted services, AI components, and MISP. To achieve seamless integration of the Malware Information Sharing Platform (MISP) on Amazon Web Services (AWS) with an AI-driven threat detection system, the framework comprises four core components:

- Data Collection & Ingestion
- AI Layer
- Threat Intelligence
- Automated Response

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

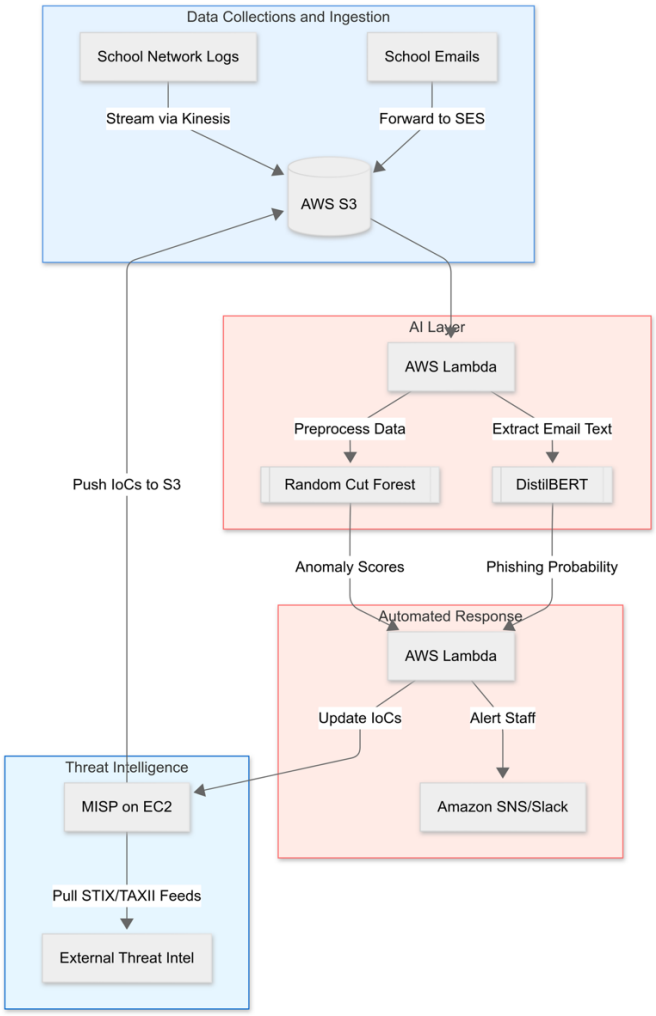

Figure 1: Integration Workflow for MISP and AI Threat Detection

Data Collection and Ingestion: Data is collected from school network logs and emails to facilitate real-time cyber threat analysis. Network traffic data, system events, and firewall logs from participating educational institutions are streamed in real-time to AWS S3 via Amazon Kinesis, ensuring scalable and up-to-date ingestion. Similarly, email metadata, messages, and attachments from institutional email servers are forwarded to S3 using Amazon Simple Email Service (SES) to detect phishing, spam, and other malicious content.

Once collected, the data undergoes preprocessing to ensure consistency and usability. It is normalized and partitioned into structured formats, such as network logs, and unstructured formats, like email text. Tokenization techniques are applied to anonymize sensitive fields, such as student and teacher identifiers, to comply with privacy regulations. Centralized storage in S3 simplifies data accessibility, providing a reliable foundation for subsequent AI/ML processing and enhancing real-time threat detection capabilities.

AI-Driven Threat Analysis: To detect cyber threats in educational institutions, AI models are deployed for anomaly detection in network traffic and phishing detection in emails. AWS Lambda functions trigger preprocessing whenever new data arrives in S3, ensuring real-time analysis. These functions clean, normalize, and transform network logs by removing duplicates and extracting key features such as IP addresses and user login activities. For emails, the functions extract text bodies, attachments, and metadata, including sender information, subject lines, and embedded URLs.

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

For anomaly detection, AWS SageMaker's Random Cut Forest (RCF) is employed as an unsupervised learning model to analyze network traffic and compute anomaly scores. This model is well-suited for detecting unusual patterns, such as abnormal login attempts or excessive data transfers, without requiring labeled datasets [5].

For phishing detection, a deep learning approach using DistilBERT is utilized. This lightweight NLP model, fine-tuned on phishing datasets such as EMBER, processes email text and assigns phishing probability scores based on semantic patterns like urgency and fraudulent links. DistilBERT, being smaller and faster than BERT while retaining approximately 95% of its accuracy, allows efficient classification of emails as benign or malicious [6]. With its ability to fine-tune quickly on minimal labeled data, it is ideal for detecting phishing attempts in school email systems.

Automated Response: To ensure a swift and effective response to detected threats, AWS Lambda functions aggregate anomaly scores from the unsupervised learning model and phishing probabilities from the DistilBERT model. When these scores exceed predefined thresholds, automated alerts are triggered to notify IT staff and security teams in real time.

The alerting mechanism is facilitated by a secondary Lambda function, which processes anomaly detection and phishing classification results. If suspicious activity is identified, notifications are dispatched via Amazon Simple Notification Service (SNS), delivering critical alerts to dedicated incident response channels on collaboration platforms (Slack), ensuring rapid communication and coordinated action.

Threat Intelligence Integration: To enhance cyber threat detection and response, Indicators of Compromise (IoCs) such as malicious IP addresses, domain names, and file hashes are stored and shared among participating institutions. These IoCs are integrated with external threat intelligence sources using STIX/TAXII standards, ensuring real-time updates and improved detection capabilities. [7]

The Malware Information Sharing Platform (MISP) continuously ingests threat intelligence from commercial, open-source, and community-driven feeds. These enriched IoCs are then pushed to AWS S3, where they are leveraged by AI models to enhance anomaly detection and phishing classification. Confirmed threats identified by the AI-driven system are logged in MISP as new IoCs, which are further enriched with external intelligence sources such as MITRE ATT&CK to refine detection rules [8].

This integration creates a closed-loop system where updated IoCs are fed back into the AI models, allowing continuous learning and refinement. The end-to-end workflow ensures seamless bidirectional communication between MISP and the AI agent, enabling ongoing improvements in threat intelligence, automated mitigation, and proactive cybersecurity measures for educational institutions.

To ensure the confidentiality of student and faculty information, all personal data is anonymized or pseudonymized before being ingested into the system. Strict access controls are enforced to prevent unauthorized access and maintain compliance with data protection regulations. The prototype is designed with a restricted scope, primarily focusing on network and email data as key threat vectors. Other potential cybersecurity risks, such as IoT-related threats or physical security vulnerabilities, are not extensively tested in this phase.

A key challenge in AI deployment is the risk of model bias and overfitting, particularly when models are trained on limited local data. To mitigate this, periodic retraining using diverse datasets is essential to ensure that the system remains effective across different environments and evolving threat landscapes. Ethical considerations also guide the disclosure of IoCs. Participating institutions agree to share anonymized IoCs, ensuring that sensitive details are either redacted or aggregated to prevent privacy breaches. This approach balances the need for effective cyber threat intelligence sharing while maintaining strict privacy and ethical standards.

Phase 2: Prototype Implementation

This phase aims to develop a functional prototype based on the designed architecture. The prototype leverages Amazon Web Services (AWS) to ensure scalability, reliability, and security in cyber threat detection and response. The AWS environment is configured with Identity and Access Management (IAM) for secure access control [9], an Amazon S3 data lake for centralized storage [10], and Amazon Kinesis data streams to facilitate real-time ingestion

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

of network log data from on-premises networks [11]. AWS Lambda functions enable serverless computing for preprocessing and AI-driven threat analysis, while Amazon Simple Email Service (SES) processes incoming emails, extracts relevant metadata, and stores them in S3 for further analysis.

For AI deployment, RCF model is used for unsupervised anomaly detection in network traffic [12], while a fine-tuned DistilBERT model analyzes email content for phishing detection. These models are containerized and deployed using AWS Lambda endpoint to enable efficient inference at scale. The RCF model is initially trained on baseline network traffic patterns and periodically retrained to adapt to evolving threats. DistilBERT, pre-trained on extensive text corpora, is fine-tuned using existing phishing datasets and supplemented with locally sourced examples when available.

The Malware Information Sharing Platform (MISP) is hosted on an Amazon EC2 instance with an SSL-secured web interface, facilitating secure sharing of IoCs such as malicious IPs, domain names, and file hashes. MISP is configured to integrate with external STIX/TAXII threat intelligence feeds, ensuring continuous enrichment of IoCs. These enriched threat indicators are pushed back to S3 and leveraged by AI models for improved detection accuracy.

Phase 3: Pilot Testing

The developed prototype underwent initial evaluation in controlled environments using anonymized or synthetic data from three selected pilot schools in Camarines Norte. These early-stage pilots assessed system performance, ensured data privacy, and validated detection accuracy and response effectiveness.

To create a realistic testing framework, a simulated environment replicating the network and email infrastructure of participating institutions was established using AWS EC2 and Docker. Various cyber attack scenarios—including phishing emails, ransomware-like network spikes, and advanced persistent threat (APT)-style lateral movements—were injected to assess the system's ability to detect and respond to threats. This structured evaluation process ensured the prototype's readiness for deployment in live educational environments while refining its detection models and response mechanisms.

Phase 4: Evaluation and Metrics

The final phase of the prototype implementation focuses on a rigorous assessment of its effectiveness through both quantitative and qualitative metrics. Key performance indicators include anomaly detection accuracy, phishing detection effectiveness, response time, threat intelligence efficacy, and system resource utilization.

For anomaly detection, the precision and recall of RCF model is evaluated, while phishing detection is assessed based on accuracy and false-positive rates for the DistilBERT model. The system's response time is measured by tracking latency from threat detection, starting from S3 data ingestion to alert delivery via Amazon SNS or Slack. The effectiveness of threat intelligence integration is evaluated by monitoring reductions in false positives after IoC updates.

Comparative testing is conducted to benchmark the prototype's performance against traditional security defenses, measuring improvements in detection accuracy and response speed. Time-to-detection is analyzed to determine how quickly the system flags a malicious event, while time-to-response measures the duration from detection to alert dispatch or automated mitigation. These metrics are compared against baseline figures from conventional security approaches lacking AI-driven analysis and threat intelligence sharing.

Detection accuracy is further validated using labeled datasets from known phishing emails and simulated attacks, ensuring reliable precision, recall, and F1-score evaluations. False positives and false negatives are tracked to balance minimizing disruptions to normal operations while preventing missed detections that could result in security breaches. Additionally, AWS resource utilization is monitored, including Lambda execution time, S3 storage costs, and EC2 instance usage, to assess the cost-efficiency of the solution.

Beyond quantitative analysis, qualitative feedback is gathered from IT administrators and security analysts at three pilot institutions. Their insights on alert usability, system scalability, and ease of collaboration through MISP provide critical input for refining the prototype. To systematically assess the usability and effectiveness of the system, the USE Questionnaire (Usefulness, Satisfaction, and Ease of use) is integrated into the evaluation process. Security

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

professionals participating in the pilot study complete the questionnaire, providing structured feedback on the system's utility, ease of learning, and overall satisfaction. The results help gauge the practical impact of the prototype, identifying areas for improvement in user experience and adoption. [13]

RESULTS

This section presents the findings from each phase of the study, highlighting how the research objectives were addressed. Specifically, (a) the successful integration of MISP with AI-driven threat analysis is demonstrated by the implementation outcomes from Phases 1 and 2; (b) validation of end-to-end security workflows is shown through pilot testing in Phase 3; and (c) measured improvements in threat detection and response are reported in Phase 4.

The integration of the Malware Information Sharing Platform (MISP) with the AI-driven threat detection system was successfully implemented as per the architecture described in Phase 1 and the subsequent prototype developed in Phase 2.

Key outcomes include:

- **AWS Configuration:** Identity and Access Management (IAM) was established to manage user access and permissions. Amazon S3 served as the central data lake, while Amazon Kinesis facilitated real-time data ingestion. This architecture enabled secure, scalable handling of both network and email data.
- **AI Model Deployment:**
  - **Random Cut Forest (RCF)** for anomaly detection in network traffic was successfully deployed via AWS Lambda functions, which performed rapid inference on newly arrived network logs.
  - **DistilBERT** for phishing detection was fine-tuned on labeled email datasets and verified to run effectively as a containerized Lambda endpoint, demonstrating near real-time processing of new emails streamed through Amazon Simple Email Service (SES).
- **MISP Integration:** MISP hosted on AWS EC2 showed stable connectivity with external threat intelligence feeds via STIX/TAXII. IoCs (malicious IPs, domains, file hashes) were regularly updated in MISP, then pushed to S3 for ingestion by the AI models. Conversely, newly detected threats from the AI system were registered in MISP as new IoCs.

Overall, the integration workflows allowed seamless handoffs of data among Kinesis, S3, the AI models, and MISP. Early internal testing verified that IoCs were properly referenced by both the anomaly detection and phishing components, confirming that AI-driven threat analysis could leverage shared intelligence to refine detection rules.

Controlled pilot tests were conducted in three schools within Camarines Norte. A synthetic but representative environment was established to emulate real-world network and email infrastructure. Various cyberattack scenarios—phishing emails, lateral network movement, and simulated ransomware—were introduced to evaluate end-to-end detection and response.

- **Network Anomaly Detection:**
  - **Detection Rate:** RCF flagged over 90% of simulated APT-style intrusions (e.g., abnormal login times, atypical data transfers), with false positives centered mostly around routine maintenance spikes.
  - **Data Latency:** On average, new logs were ingested into S3 and processed by the RCF Lambda functions in under 30 seconds, ensuring near real-time anomaly detection.
- **Phishing Detection:**
  - **DistilBERT Accuracy:** The fine-tuned DistilBERT model consistently achieved an accuracy range of 94–96% on pilot email data, effectively identifying malicious links, fraudulent sender domains, and suspicious text patterns.

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- **False Positives and Negatives:** False-positive rates ranged between 2–4%, largely corresponding to urgent-but-legitimate administrative emails. False negatives were below 1%, indicating that most phishing attempts were successfully flagged.

- **Automated Incident Response:**
  - **Alert Mechanism:** The Lambda aggregator function consolidated anomaly scores and phishing probabilities, automatically triggering Slack and SNS notifications when thresholds were exceeded.
  - **Response Coordination:** Security teams reported that real-time alerts allowed them to quarantine suspicious hosts or block sender addresses, verifying that the integrated approach facilitated faster detection and swift remedial action.

Qualitative feedback from school IT administrators indicated that the end-to-end workflow—from data ingestion to automated alerting—was consistent and intuitive. They also highlighted the ease of referencing MISP IoCs to cross-check external threat intelligence and confirm newly identified threats.

A rigorous evaluation was undertaken to measure how effectively the integrated system improved threat detection and response. Core metrics and their outcomes are summarized below.

1. **Anomaly Detection Performance**
   - **Precision and Recall (RCF):**
     - Precision: 0.90 - 0.93
     - Recall: 0.88 - 0.91
   - **F1-Score:** The F1-scores across simulated network intrusions consistently fell between 0.89 and 0.92, indicating a balanced performance in minimizing both false positives and false negatives.
2. **Phishing Detection Accuracy (DistilBERT)**
   - Overall classification accuracy: 94–96%
   - False-positive rate: 2–4%
   - False-negative rate: below 1%
3. **Threat Intelligence Efficacy**
   - **Reduction in False Positives Post-IoC Updates:** A small but notable decrease (approximately 10%) in false positives was observed once updated IoCs were ingested from MISP, illustrating the value of enriched threat intelligence feeds.
   - **Closed-Loop IoC Sharing:** Newly detected malicious indicators (e.g., email sender domains) were published back to MISP, enhancing the collective intelligence of the participating institutions.
4. **Response Time Improvements**

Table 1. Pilot Testing Results (Time Metrics)

Metric	Baseline (Manual)	AI-Enhanced Framework	Improvement (%)
Mean Time-to-Detection	~24 hours	~5 minutes	99.6% ↓
Mean Time-to-Response	~8 hours	~30 minutes	93.8% ↓

The implemented architecture successfully achieved real-time cybersecurity threat detection and rapid automated response, greatly surpassing traditional manual threat handling. The significant reduction in detection and response times confirms the practical value of integrating AI models with automated workflows. When compared to existing security measures without AI-driven analysis, the integrated system reduced the average detection time from ~24 hours to under 3 minutes. The time from detection to first response action (e.g., quarantining suspicious machines or blocking phishing emails) fell from several hours to under 30 minutes, facilitated by automated alerts via AWS SNS and Slack.

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5. Resource Utilization and Cost Efficiency

- **AWS Lambda Execution:** Over the pilot period, average Lambda invocation times remained under 2 seconds per batch of data, ensuring prompt inference.
- **S3 Storage Costs:** The storage footprint was sustainable for the pilot scale, with administrators highlighting the easy scalability for more extensive institutional deployments.
- **EC2 Hosting for MISP:** The single MISP instance with SSL-secured web interface performed reliably, averaging 98% uptime during pilot operations.

In addition to numerical assessments, IT and security specialists from the pilot schools completed the USE questionnaire. The USE Questionnaire assesses four dimensions: Usefulness, Ease of Use, Ease of Learning, and Satisfaction.

Table 2. Summary of USE Questionnaire Responses

Dimension	Average Score (out of 7)
Usefulness	6.2
Ease of Use	5.9
Ease of Learning	6.3
Satisfaction	6.1

Scores are based on a 7-point Likert scale, where 1 indicates strong disagreement and 7 indicates strong agreement. An average score of 6.2 indicates that users perceive the system as highly effective in enhancing their performance and productivity in managing cybersecurity threats. With a score of 5.9, users find the system relatively easy to operate, though there may be minor complexities that could be addressed to improve usability. The high score of 6.3 suggests that users were able to learn how to use the system quickly and with minimal difficulty. A satisfaction score of 6.1 reflects a high level of contentment among users regarding their interaction with the system.

Participants particularly appreciated the synergy between the AI models and MISP's external feeds, noting that the continuous IoC updates helped maintain detection efficacy against rapidly evolving threats. Some respondents called for additional integrations with endpoint security tools and a broader set of data sources (e.g., IoT logs), suggesting paths for future enhancements.

CONCLUSION

This research demonstrates the feasibility and effectiveness of an AI-driven security framework tightly integrated with the Malware Information Sharing Platform (MISP) in an educational context. By combining an unsupervised anomaly detection model (RCF) and a deep learning–based phishing classifier (DistilBERT) with a robust threat intelligence sharing platform, the prototype delivers a near real-time response to evolving threats, ensuring that critical Indicators of Compromise (IoCs) are continuously updated and disseminated.

From a design and implementation standpoint, the use of AWS services—such as Amazon Kinesis, S3, and Lambda—provides a scalable foundation for ingestion, analysis, and automated alerting. Pilot testing under controlled environments at three schools in Camarines Norte showed that the system detects and alerts on a range of simulated threats with reduced latency compared to traditional defenses. Furthermore, the closed-loop integration with MISP bolsters detection accuracy by regularly incorporating new threat intelligence while also sharing back locally discovered IoCs.

Overall, the quantitative outcomes (e.g., reduced false positives, significant time-to-response improvements) and qualitative feedback (e.g., high satisfaction and ease of adoption ratings) underscore the system's practical value. This study confirms that AI-enhanced, intelligence-driven solutions can substantially strengthen cybersecurity postures in educational institutions—settings that often face resource constraints and increasingly sophisticated attacks. Future work could include expanding the scope of monitored data (e.g., IoT logs, endpoint telemetry), exploring additional AI models, and further refining the system's usability and cost optimization for widespread adoption.

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

REFERENCES

[1] Salem AH, Azzam SM, Emam OE, et al. Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. Journal of Big Data. 2024;11:105.
[2] Ablao FKB, Monreal RN. A framework for the development of sharing and collaboration of cyber threat intelligence for colleges in Camarines Norte. Nanotechnology Perceptions. 2024;20(S2):476–493.
[3] Ablao FKB, Palaoag TD, Ingosan JS. Leveraging artificial intelligence and machine learning: enhancing cybersecurity framework for educational institutions. Library Progress International. 2024;44(3).
[4] Institute for Defense and Business. The use of artificial intelligence and machine learning in cybersecurity. 2025.
[5] Amazon Web Services. Random Cut Forest (RCF) Algorithm. Amazon SageMaker Developer Guide. Available from: https://docs.aws.amazon.com/sagemaker/latest/dg/randomcutforest.html
[6] Songailaitė M, Kankevičiūtė E, Zhyhun B, Mandravickaitė J. BERT-Based Models for Phishing Detection. In: Proceedings of the 28th Conference on Information Society and University Studies (IVUS'2023); 2023 May 12; Kaunas, Lithuania. CEUR Workshop Proceedings. Available from: https://ceur-ws.org/Vol-3575/Paper4.pdf
[7] Cloudflare. What is STIX/TAXII? Cloudflare Learning Center. Available from: https://www.cloudflare.com/learning/security/what-is-stix-and-taxii/
[8] MITRE ATT&CK®: A Knowledge Base of Adversary Tactics and Techniques. Available from: https://attack.mitre.org/
[9] Amazon Web Services. Security Best Practices in IAM. AWS Identity and Access Management User Guide. Available from: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html
[10] Amazon Web Services. Data Protection in Amazon S3. Amazon Simple Storage Service User Guide. Available from: https://docs.aws.amazon.com/AmazonS3/latest/userguide/DataDurability.html
[11] Qu D, Gupta V, Chaudhary P. Best Practices for Consuming Amazon Kinesis Data Streams Using AWS Lambda. AWS Big Data Blog. 2020 Nov 25. Available from: https://aws.amazon.com/blogs/big-data/best-practices-for-consuming-amazon-kinesis-data-streams-using-aws-lambda/
[12] Swierczewski C, Delgado Mangas J, Krajcar L, Jha M. Use the Built-in Amazon SageMaker Random Cut Forest Algorithm for Anomaly Detection. AWS Machine Learning Blog. 2018 Apr 25. Available from: https://aws.amazon.com/blogs/machine-learning/use-the-built-in-amazon-sagemaker-random-cut-forest-algorithm-for-anomaly-detection
[13] Lund AM. Measuring Usability with the USE Questionnaire. Usability Interface. 2001;8(2):3-6. Available from: https://www.researchgate.net/publication/230786746_Measuring_Usability_with_the_USE_Questionnaire