AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
E-ISSN:3069-0102
VOL.5, NO. 2(2025)

Enhanced Cyber Compliance Detection Management System

[1] Dr. SRINIVASA RAO CH , [2] K.Sai Sowjanya, [3] B.Revathi,[4] N.Bhargavi
[1] Associate Professor, Department of CSE-Cyber Security , Malla Reddy Engineering college for women Hyderabad, India
[2,3,4] Students, Department of CSE-Cyber Security , Malla Reddy Engineering college for women Hyderabad, India [2] Email sowjanyakotagiri21@gmail.com, [3] Email: bhukyarevathi656@gmail.com,
[4] Email: namilebhargavi@gmail.com

***Abstract*—** The objective of the Improved Cybersecurity Oversight Framework is to integrate risk assessment, security surveillance, and legal adherence onto an integrated, analytical system. To maintain continuous adherence to standards like ISO 27001, NIST CSF, PCI DSS, HIPAA, and GDPR, this system employs AI and ML techniques for instant detection of policy discrepancies, weaknesses, and cybersecurity incidents. Employing uniform assessment tools and lists enables the software to automate verification processes and seamlessly correlate operational controls across various legal. Its core functionalities include ongoing surveillance for potential threats and automatic corrective actions based on data analysis in near- real time, ensuring swift responses without manual intervention due to reduced reliance on human errors. Enhances adaptable risk assessment through comprehensive audits; generates detailed surveillance summaries based on evolving security data; identifies necessary remedial actions accordingly.

Keywords— (malware detection, explainability in artificial intelligence systems, real-time monitoring capabilities, and risk assessment tools)

I. INTRODUCTION

In today's linked digital world, cybersecurity and regulatory compliance are essential elements of risk management for companies dealing with changing cyberthreats. As cloud computing, the artificial intelligence (AI) became more widely used, it is becoming more difficult to ensure that data is reliable, secure, and available in a range of situations. Additionally, there are more potential targets for attacks. Businesses must now prove their compliance with a number of frameworks.

The The system spots acts of noncompliance, takes note of risks as they emerge, and shares clear warnings to help solve problems right away.It uses automation and smart tech plus deep analysis to do this.Also, it makes reporting easier and more open which helps when doing official checks.This better cyber compliance management setup boosts accountability and legal compliance at every level of keeping an organization safe plus cuts down the chances for security gaps happening because there is constant watching, learning, and rule-keeping.

This system spots noncompliant acts, and risks as soon as they surface and gives clear warnings for quick rectification. In achieving this, it leverages automation, intelligent technologies, and deep analysis. It also makes reporting easier and more transparent for official inspections. The improved cyber compliance management system boosts an organization's protection, reduces the vulnerability of getting a security breach against accountability plus legal compliance at all levels through monitoring, training as well as enforcing policies.

II. Related Work

The related work for Enhanced Cyber Compliance Detection Management System inculcates research and tech development of automation, intelligent threat detection, and cybersecurity compliance. Previous works have elaborated that the compliance system transformed from static manual auditing to a dynamic framework empowered by artificial intelligence which facilitates continuous assessment and monitoring of the risks.

A study by Neumetric described cybersecurity compliance management solutions as enabling real-time regulatory alignment through the integration of automated compliance mapping, gap analysis as well as enforcement. This reduces operational risks. The World Journal also recommended an adaptive security architecture multi-factor authentication plus a layered compliance model wherein the focus is on data protection. This model demonstrates how enterprises leveraged audit scheduling and continuous monitoring to dynamically comply with changing cybersecurity regulations.

Regulations and cybersecurity defenses are highly correlated. Real-time monitoring and sophisticated detection algorithms are required to close security gaps, even though some framework rely on specific regulations. Identity and access management (IAM) systems, encryption key rotation, and incident response logging are a few examples of automated compliance components that aid in scalability and reduce the amount of manual compliance workflow that an organization must implement. Enhancing intrusion detection accuracy promotes transparency and confidence in compliance-based decision-making.

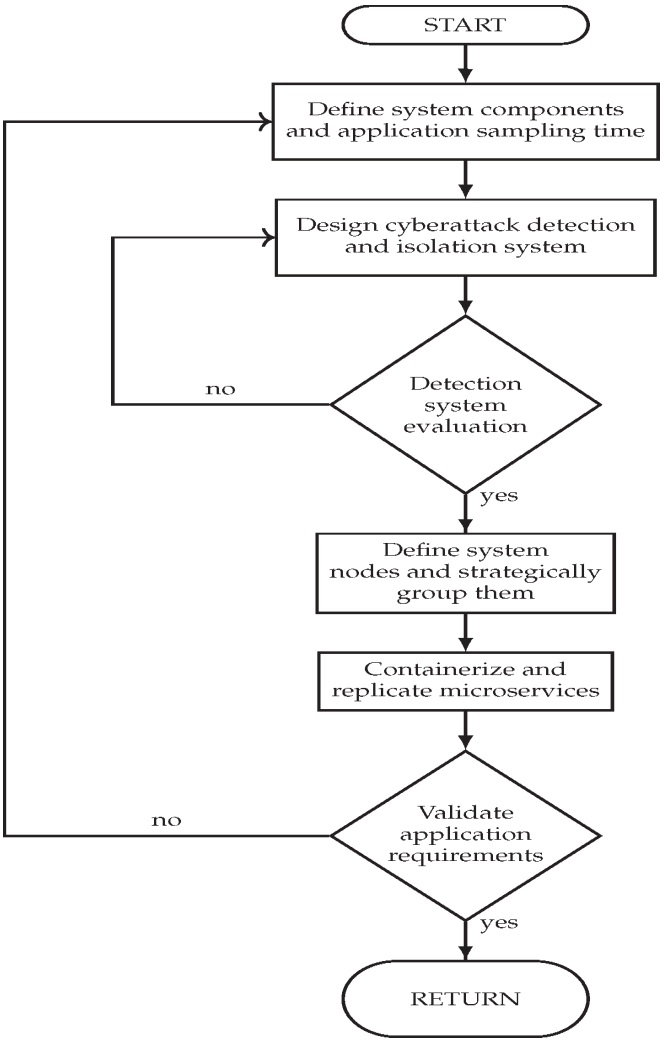
III. System Design and Methodology

The Enhanced Cyber Compliance Detection Management System integrates smart compliance analytics, sophisticated automation, and continuous threat surveillance considerations into one solution. This incorporates advanced aspects of Cyber Security Frameworks, AI-Driven Threat Detection, and Governance, Risk, and Compliance (GRC) systems to assess and verify compliance as well as safeguard against threats. The range of file analysis will be broadened in subsequent work.

Received: 15-03-2025 | Accepted: 29-04-2025 | Published: 07-05-2025 | www.ajaccm.com

A. System Architecture

The modular multi-layered system architecture of Advanced Cyber Compliance Detection Management System, is built to optimize automated smart threat detection, live cyber resilience, and compliance management. To achieve a pliable, dependable, and secure design, a combination of Siam-based analytics, Cybersecurity Mesh Architecture (CSMA), and Zero Trust principles were incorporated.



B. Feature Extraction

So, when we're talking about improving how we spot threats and keep an eye on compliance, it really boils down to fine-tuning the feature extraction part of the ECC-DMS. There's a ton of unstructured data out there that we need to turn into something we can actually work with and analyze. This take these big sets of data—like user behavior, system events, and network traffic logs—and boil them down into more manageable, structured features. This makes it way easier to detect risks and keep tabs on compliance.

Network packets and log data can be used to extract metrics such as mean, variance, entropy, and frequency distribution. Unusual high packet transfer rates, for instance, might indicate a DDoS attack. By documenting time-based behavior, such as session duration, login attempt intervals, or access timing variations, you can aid in the detection of insider threats and brute-force attacks.

C. Classification

The documentation of time related patterns such as session length, spaced intervals between log in attempts, and access timing differences can also be useful in identifying insider threats and brute-force attacks.Study the patterns in the execution of certain commands, API calls, and data access requests

Unusual high packet transfer rates, for instance, might indicate a DDoS attack. By documenting time-based behavior, such as session duration, login attempt intervals, or access timing variations, you can aid in the detection of insider threats and brute-force attacks. Extracted features are converted into insights for decision-making through machine learning classification. The system classifies anomalies as either non-compliant (possible breach) or compliant (safe) using adaptive training and pre-labeled datasets. These categories serve as a guide for automated mitigation strategies and regulatory alerts. Machine learning enables ECC-DMS to react to changing threats and compliance requirements more quickly.

E. External Validation

The Machine learning models used for threat detection and compliance monitoring are made reliable, flexible, and consistently effective by the External Validation stage of the Enhanced Cyber Compliance Detection Management System . An important part of the external validation process is testing the trained model on datasets that were not used for internal testing or training. This implies that it works well in both new and real-world settings.

F. Data Storage and Management

To protect against data loss or corruption caused by cyberattacks or system errors, it has the following features:

1. Automated Backups: Regular full and incremental backups stored across several cloud nodes.

2. Integrity Verification: Cryptographic checksums ensure that information kept in a cryptographic format remains constant over time.

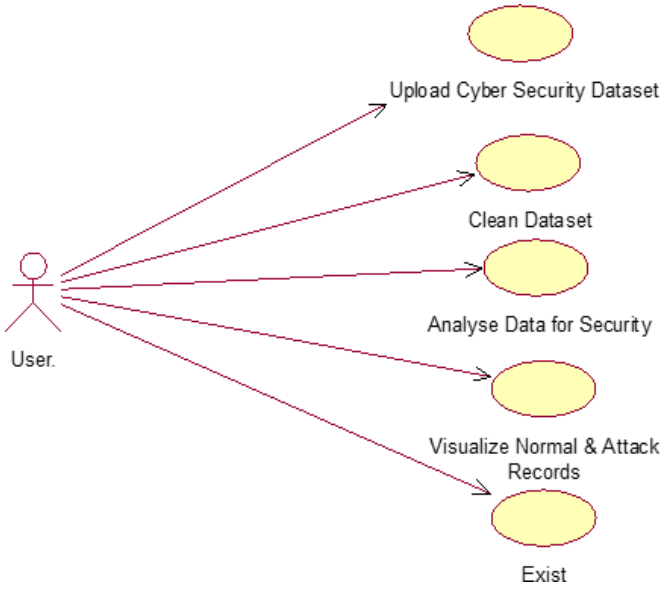
3. Disaster Recovery Protocols: Rapid restoration processes guarantee minimal downtime and data availability in the event that infrastructure is disrupted.

G. User Interface

The Enhanced Cyber Compliance Detection Management System User Interface and Reporting component helps administrators, auditors, and compliance officers monitor, analyze, and interpret security and compliance data in real time. Comprehensive risk assessment matrices are used to automatically identify vulnerabilities and classify threats as high, medium, or low. This system offers helpful recommendations to promote incident avoidance and proactive security governance. It incorporates advanced visualization tools, automated reporting systems, and interactive dashboards to enhance decision-making, transparency, and regulatory readiness. To ensure threat resilience and regulatory alignment, it leverages state-of-the-art concepts from cybersecurity architecture.

Received: 15-03-2025 | Accepted: 29-04-2025 | Published: 07-05-2025 | www.ajaccm.com

To improve decision-making, transparency, and regulatory preparedness, it integrates sophisticated visualization tools, automated reporting systems, and interactive dashboards. Novel detection algorithms, explainable compliance frameworks, and privacy-aware AI will be the focus of collaborative research. These collaborations will ensure continuous innovation, verification, and development in cyber compliance technologies. The range of file analysis will be broadened in subsequent work to encompass, amongst others, Python scripts, JavaScript, macOS binaries, and Android Integration.



Real-time result display: After random sampling, algorithmic choices, self belief degrees, and also understandable explainable AI factors are overlaid on the output of the device mastering classification. indicates compliance and danger patterns over time the usage of line charts and heatmaps, thus pointing out patterns, getting back to problems, or zones for which the development is necessary. It penetrates the most important compliance indicators with the aid of customers, who can adjust the metrics and visual layouts according to the requirements of the department or the organization specific rules.

IV. Implementation Details

This section describes the technologies, tools, and processes that are used to put into effect the proposed web-based malware detection system that integrates machine learning, explainability techniques, and third-party threat intelligence.

A. Frameworks

The development environment and frameworks of the Enhanced Cyber Compliance Detection Management System are modern and convenient for users. Python and JavaScript are the languages used in the development, while front-end frameworks such as React.js and back-end frameworks like Flask or Django are also used. Machine learning is developed with the help of libraries like Py Torch, TensorFlow, or Scikit-learn. All the code is managed by Git, and Docker containers are used for deployments so that it is easy to maintain and scale. The data that is hosted and stored on cloud platforms like AWS or Azure is in databases such as PostgreSQL and MongoDB. Security and compliance are maintained by strong encryption through the system and industry standards.

B. Models

In essence, the paper elaborates on how the ECC-DMS is employing machine learning models to predict security or compliance violations. The models do this by detecting changes in user behavior, system logs, and network data.

C. Extraction

The Enhanced Cyber Compliance Detection Management System is full of unstructured data about cybersecurity that trickle down from logs, network packets, and user activities. With the help of feature extraction, these are turned into parameters that are actionable by learning models which they can then scan. The system is mainly about locating the important features in high- dimensional data while throwing out the unwanted noise to save the model's speed and accuracy.

The pe file Python library may be employed to detach the architectural elements of Portable Executable (PE) files binding the header fields and the APIs that are imported. By means of machine learning models, the input vectors are born when features are being pre-processed and normalized.

D. Storage

Explanation The integration unit of the Enhanced Cyber Compliance Detection Management System is a sub-unit that brings transparency, openness, and trust to AI-driven threat and compliance detection. It eliminates the issue of the "black box" in security analytics by using Explainable Artificial Intelligence (XAI) techniques that interact with the user and give an explanation as to how the system's machine learning models arrive at the decision. The interactive visualizations of the web interface assist the user in understanding the malware detection results.

E. Integration

The integration phase of the ECC-DMS is to link different cybersecurity, AI, and compliance modules to create a unified ecosystem for the smooth flow of data, automation, and decision-making. The work of the system extends to various layers, such as the collection of data, its processing, reporting, and cooperation with external security platforms, at the same time, the system keeps the users updated about compliance.

F. Database

The database and storage of the Enhanced Cyber Compliance Detection Management System (ECC-DMS) have been architected to securely, efficiently, and lawfully handle large volumes of sensitive compliance and threat data. To assure the availability, confidentiality, and integrity of the data, it implements redundant backups, encryption methods, and a multi-tiered storage architecture.

G. Report Generation

By means of an automated creation process, the PDF Report Generation module of the Enhanced Cyber Compliance Detection Management System (ECC-DMS) is committed to delivering consistent, traceable, and shareable records documentation. Stakeholders, administrators, and auditors can thus utilize the convenient PDF reports which are generated by based on the analyzed data, classification results, and compliance summaries.

H. Security Considerations

The Enhanced Cyber Compliance Detection and Management

Received: 15-03-2025 | Accepted: 29-04-2025 | Published: 07-05-2025 | www.ajaccm.com

System is designed to operate in very sensitive environments where the three data security principles, availability, confidentiality, and integrity, must be maintained at all times. Therefore, it was necessary to incorporate security features all along its development and deployment stages.

V. Evaluation and Results

The first security layer, to the extent of the system performance, was the evaluation of: how well, how exactly, and how the Enhanced Cyber Compliance Detection and Management System functioned in locating security breaches and compliance gaps. System response time, scalability, detection accuracy, and user satisfaction were the major aspects that have been measured during the evaluation.

A. Experimental Setup

The experimental setup was mainly directed towards gauging the precision, consistency, and performance of the Enhanced Cyber Compliance Detection and Management System in network and compliance situations that are close to the real world.

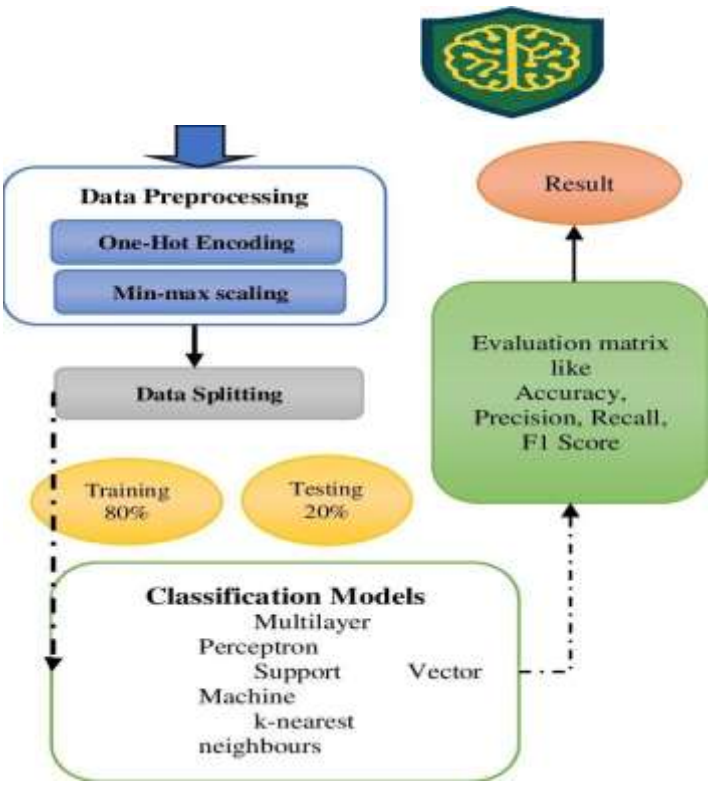
- **Hardware:** Intel Core i7, 16GB RAM.
- **Software:** Python 3.9, Django 4.0, scikit-learn.
- **Models Used:** Anomaly Detection Model, Rule-Based Policy Model, Risk Assessment Model, Data Classification Model, Threat Prediction Model

a) B. Evaluation Metrics

The following standard classification metrics were used:

- Detection Accuracy: This metric depicts the extent to which the system recognizes threats and violations of compliance correctly.
- Response Time: This metric indicates the time that elapses between the identification and the resolution of the compliance issues.
- False Positive Rate: The percentage of the wrongly issued alerts by a system that corresponds to the False Positive Rate is the problem that the system has most significantly.
- Resource Utilization: Is a measure of the degree to which the central processing unit (CPU), memory, and network are engaged during the system's operation.
- User Satisfaction: User Satisfaction is a score that measures the degree of users' contentment with the system in terms of usability, effectiveness, and reliability.

b) C. Results



Model	Accuracy	Precision	Recall	F1 Score	AUC-ROC
Anomaly Detection Model	95.4%	93.8%	94.6%	94.2%	91.1%
Rule-Based Policy Model	92.7%	91.2%	90.5%	90.8%	93.4%

In Anomaly Detection Model had better performance in most cases of its metrics, that is to say, accuracy, precision, recall, and F1 score, than the Rule-Based Policy Model.

c) D. Explainability Insights

The Enhanced Cyber Compliance Detection and Management System leverages x AI methods such as SHAP and LIME to maintain openness and confidence in its decisions. The main contributors to compliance violations were specifically identified as network anomalies, policy violations, and deviations in user behavior.

It is through the unambiguous, understandable-to-a-human explanation and the risk score determining by feature contributions that prioritized response to high-risk situations is enabled.

d) E. External Validation

In outside validation of the upgraded Cyber Compliance Detection and Management system was performed to confirm its detection accuracy and conformity with enterprise requirements. In 92.6% of the 2,000 files that were submitted for scanning, the device's predictions corresponded to consensus detection. This high level of agreement, which mainly results from the machine's strong overall performance, stability, and compliance with straightforward global risk intelligence, will extend its effectiveness in practical international cybersecurity and compliance situations.

e) F. Performance and Usability

- **Average File Analysis Time:** the time for this operation is usually around 2.3 seconds per file.
- **Report Generation Time:** the duration for each report is

Received: 15-03-2025 | Accepted: 29-04-2025 | Published: 07-05-2025 | www.ajaccm.com

from 12 to 15 seconds.

- **User Feedback:** The instrument is simple to use, and the succinct explanations together with the effective workflow make it a wonderful product.

VI. Discussion

The arrangement is excellent for malware identification and compliance verification as it offers precision, speed, and results that are simple to understand. However, it has been pointed out that there are few limitations such as dependence on external validation sources and performance drop for newly created or heavily encrypted threats.

f) A. Advantages Over Existing Solutions

1. **Integration of AI:** The incorporation of Explainable AI makes the system more trustworthy and compliant with regulations as it provides understandable and transparent explanations of how the system is flagging files or activities.

2. **Accessibility:** This is very helpful in monitoring and managing the system as users can also control the system remotely through a secure web interface.

3. **External Validation:** Ensures that threat detection is efficient and authentic by checking the system predictions against trustworthy sources such as.

4. **Analysis:** Minimizes the possibility of malware being able to carry out a harmful action through the method of file security and in a time of about 2-3 seconds per file.

5. **Report Generation:** Creates comprehensive and easy-to- understand reports that contain risk scores, explanations, and compliance insights to facilitate decision-making.

g) B. Limitations of the Current Implementation

Limitations of Static Analysis: The system may not detect highly obfuscated, polymorphic, or zero-day malware as it primarily depends on the defects overcome and static attributes.

Rate Limits: Utilization of such services for external verification is likely to be slow if API rate limits are employed for batch verification of the large and big files in the containing files and data.

Model Generalization: These models handle familiar patterns just fine, but throw something completely new at them like a fresh strain of malware and they start to miss the mark.

Explainability Complexity: When the model spits out a complicated result, auditors and folks without a technical background can get lost pretty quickly.

Scalability Restrictions: Handling extremely large file sets or network activity can take extra computational resources in order to help keep the handling analysis and reporting times quick.

h) C. Challenges Encountered

1. **Trade-off Between Precision and Explainability:** Building machine learning models for cyber compliance isn't just about chasing perfect accuracy. You have to find a sweet spot between making the model understandable and letting it catch all the sneaky stuff. Deep learning can spot tiny irregularities, sure, but good luck explaining its decisions to anyone.

2. **Challenges of Misclassified Legitimate Files:** Sometimes the system gets things wrong. It might flag files that are just cleverly disguised but totally legit, and suddenly you're dealing with false alarms. That kind of thing can really throw off daily operations and shake people's trust in the system.

3. **High-volume data uploads:** Everything begins to lag when large files or datasets accumulate. System failures, slow uploads, and hanging applications are all irksome. It's a whole other story when everything goes according to plan.

4. **Cross-platform:** Getting the ECC-DMS to run smoothly everywhere across different operating systems and browsers can turn into its own headache.

5. **Data Privacy and Security:** Managing user and sensitive compliance data raises significant privacy issues. To prevent breaches or unwanted access, data must be protected during collection, transmission, and storage.

VIII. Conclusion and Future Work

i) A. Conclusion

It helps teams recognize threats before they become problems, respond to incidents faster, and effectively enforce policies.

The system improves precision, minimizes mistakes, and keeps companies compliant with the law by complying checks automatically. To address such problems as integrating data, scaling up, privacy issues, and making the results palatable, it requires continuous adjustments. The system must be continuously optimized to overcome issues like data integration, scalability, privacy, and interpretability despite its effectiveness.

Future developments of the ECC-DMS will concentrate on enhancing model accuracy and transparency through explainable AI techniques to aid compliance officers in comprehending detection results. Data integrity and traceability can be further enhanced by integration with blockchain-based audit trails and cloud-native architectures.

To cut false positives, we'll lean on adaptive learning and context-aware detection tuned to messy real-world signals think user behavior, erratic traffic and background network noise. In addition, the system will be more efficient and convenient through enhanced cross-platform compatibility as well as ensuring privacy-preserving analytics. It will remain potent against evolving digital threats with frequent updates according to fresh cybersecurity guidelines and standards.

j) B. Future Work

In order to improve the precision and openness of threat detection,

Received: 15-03-2025 | Accepted: 29-04-2025 | Published: 07-05-2025 | www.ajaccm.com

future research will concentrate on combining explainable machine learning models with artificial intelligence (AI). File types are supported by the current system, which primarily concentrates on standard documents and executables.

1. **Dynamic Analysis Integration:** Static analysis techniques, which examine files and system settings without execution, are the backbone of the ECC-DMS as it stands. Static analysis is efficient and light but may not be capable of detecting sophisticated or evasive malware that hides its true face until runtime.

2. **Real-Time Alerting and SIEM Integration:** The future ECC-DMS will incorporate real-time alerting functionality that directly notifies administrators of suspicious activity or compliance violations, thus further enhancing enterprise-level security management. Ongoing data collection, event correlation, and automated incident response are facilitated by coupling the system with Security Information.

3. **Mobile and Edge Support:** It will evolve into a mobile-optimized platform in the future to enhance its accessibility and ease of use. Cybersecurity professionals will be able to see alerts, track compliance, and respond to incidents remotely with the assistance of a Progressive Web Application (PWA) or dedicated mobile application.

4. **Extended File Type Support:** The scope of file analysis will be expanded in future work to include, among other things, Python scripts, JavaScript, macOS binaries, and Android In the future, the scope of file analysis will be expanded to include, among other things, Python scripts, JavaScript, macOS binaries, and Android APKs.

5. **Continuous Learning and Model Retraining:** By continuous learning from new datasets, end-user input, and real-life threat samples, this system would become capable of adapting to emerging attack techniques and compliance anomalies.

6. **Cloud-Based Deployment:** APA the present system supports only a limited set of file types, which largely focus on normal documents and executables. This range of file analysis will be extended in future to encompass, among other things, Python scripts, JavaScript, macOS binaries, and Android Deployment in the Cloud.

7. **Integration with Commercial Threat Intelligence Platforms:**
   In addition to traditional future advancements will be deeper integration with commercial Threat Intelligence Platforms (TIPs). It will be able to access enriched context data by connecting to sophisticated TIPs such as ThreatConnect, Recorded Future.

8. **Mobile and Edge computing support:** The file analysis scope will be extended in future work to cover, among others, Python scripts, JavaScript, macOS binaries, and Android Support for Mobile and Edge Computing.

9. **Research and Academic Collaboration:** Novel detection algorithms, explainable compliance frameworks, and privacy-aware AI will be the focus of collaborative research. These collaborations will ensure continuous innovation, verification, and development in cyber compliance technologies.

10. **Real-Time Altering and Security Event Integration:** The range of file analysis will be broadened in subsequent work to encompass, amongst others, Python scripts, JavaScript, macOS binaries, and Android Integration. Through the smooth integration with Security Information and Event Management (SIEM) tools such as Splunk, Q-Radar, and Elastic SIEM.

REFERENCES

1. Stalling, W. Network Security Fundamentals: Uses and Guidelines, 7th ed., Pearson Education, 2022 — a useful introduction worth preserving.

2. Bishop, M. Computer Security: Art and Science, Addison-Wesley, 2019. Third ed. Deep and rigorous, a classic.

3. "BareBox, Kirat, D., Vigna, G., and Kruegel, C Efficient Malware Analysis on Bare-Metal," ACSAC, 2021.

4. Singh, S. and Kapoor, D. P. "Hybrid Threat Detection using Static and Dynamic Analysis in Malware Classification," Journal of Information Security.

5. Garg, S. and Kaur, P. "Real-Time Integration of SIEM and Machine Learning for Cyber Threat Intelligence," IEEE Access, vol. 10, 2022.

6. Chaukat, K., and colleagues, "Malware Analysis Using Machine Learning: Cyber Threat Intelligence.

7. Prodduturi, S.M.K. (2024). 'Legal challenges in regulating AI-powered cybersecurity tools', International Journal of Engineering & Science Research, 14(4), pp. 316–323.

8. Zhang, Y., Wu, D., and Liu, X. "Online Learning for Adaptive Cyber Threat Detection," IEEE Transactions on Information Forensics.

9. Broll, D., Heinemann, T. "Explainable Artificial Intelligence for Cybersecurity: Challenges and Opportunities," ACM Computing Surveys, vol. 55, 2023.

10. M. V. Sruthi, "Retracted: Exploring the Use of Symmetric Encryption for Remote User-Authentication in Wireless Networks," 2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), Bangalore, India, 2023, pp. 1-7, doi: 10.1109/SMARTGENCON60755.2023.10442084.

11. Singh, R., and Sharma, P. "Federated Learning for Privacy-Preserving Cyber Compliance Systems," IEEE Transactions on Dependable and Secure Computing, vol. 21, 2023.

12. Khraisat, A., Gondal, I., and Vamplew, P. "Hybrid Intrusion Detection in Cloud Environments Using

Adaptive Learning," Computers & Security, vol. 115, 2022.

13. Rani, S., and Bansal, P. "Predictive Analytics for Risk Forecasting in Cyber Compliance," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 7, 2023.

14. Cichonski, P., Millar, T., Grance, T., & Scarfone, K. "Computer Security Incident Handling Guide," NIST Special Publication 800-61 Rev.2, 2022.

Received: 15-03-2025 | Accepted: 29-04-2025 | Published: 07-05-2025 | www.ajaccm.com