Next-Generation Ransomware Defense Using Artificial Immune System

Eluchie Osita John and Onwuachu Uzochukwu Christian
Imo State University, Owerri, Imo State. Nigeria
eluchieositajohn@gmail.com
uzochukwuchristian@yahoo.com

https://doi.org/10.56201/ijcsmt.vol.12.no11.2026.pg55.66

Abstract
The increasing rate of ransomware attacks has become a major cybersecurity challenge, resulting in data loss, financial damage, unauthorized access, and disruption of computer systems. Traditional antivirus and signature-based detection techniques are often limited because they depend on previously identified malware signatures and may fail to recognize new or modified ransomware variants. This study presents a Next-Generation Ransomware Defense Using Artificial Immune System (AIS) as an adaptive approach to detecting and responding to ransomware attacks. The proposed system integrates Artificial Immune System techniques, behavioral analysis, and machine learning to identify suspicious system activities. The Negative Selection Algorithm is employed to distinguish normal system behavior from abnormal patterns, while the machine-learning component classifies suspicious activities as either benign or ransomware. Behavioral features considered include file modification rate, file-renaming activity, encryption activity, number of files affected, process creation rate, disk write activity, CPU usage, memory utilization, and network connections. An immune-memory mechanism is also incorporated to retain previously identified suspicious patterns and support subsequent detection. The system is implemented using Python, Flask, Scikit-learn, NumPy, Pandas, and SQLite. The proposed solution provides a framework for continuous behavioral monitoring, threat classification, security alerts, event logging, and ransomware containment. Its performance is evaluated using accuracy, precision, recall, F1-score, and confusion matrix. The study demonstrates the potential of combining Artificial Immune System techniques with machine learning to improve adaptive ransomware detection and reduce dependence on traditional signature-based methods. The proposed system is intended to provide an intelligent and flexible security framework for protecting computer systems against evolving ransomware threats.

Keywords: *Ransomware, Artificial Immune System, Machine Learning, Negative Selection Algorithm, Behavioral Analysis, Cybersecurity, Threat Detection, Immune Memory.*

I. Introduction

Ransomware has become one of the most serious cybersecurity threats affecting individuals, businesses, government institutions, educational organizations, and other information-dependent sectors. It is a type of malicious software designed to deny users access to their files or computer systems, usually by encrypting important data and demanding payment before access is restored. The increasing dependence on digital technologies, cloud computing, online transactions, and network-connected devices has created more opportunities for cybercriminals to launch ransomware attacks. These attacks can result in

financial losses, data breaches, operational disruptions, reputational damage, and the permanent loss of valuable information. The development of ransomware has become more sophisticated over the years. Modern ransomware attacks are no longer limited to simple file encryption; some variants can spread across networks, disable security tools, delete backup files, steal sensitive information, and threaten to publish confidential data if victims refuse to pay. Cybercriminals also use different techniques, including phishing emails, malicious attachments, compromised websites, software vulnerabilities, and unauthorized remote access, to gain entry into computer systems. This continuous evolution makes ransomware difficult to detect using traditional security approaches. Conventional antivirus and intrusion detection systems commonly depend on predefined rules, known malware signatures, and previously identified attack patterns. Although these methods are useful for detecting known threats, they may fail to identify new, modified, or previously unseen ransomware variants. Signature-based detection requires regular updates to recognize newly discovered malware, creating a possible delay between the emergence of a threat and its detection. Furthermore, some ransomware programs can modify their code or execution behaviour to avoid detection by traditional security solutions. These limitations demonstrate the need for more intelligent, adaptive, and behaviour-based approaches to ransomware detection and prevention. One promising approach to addressing these challenges is the Artificial Immune System (AIS). Artificial Immune System is a computational intelligence technique inspired by the biological immune system, which protects the human body against harmful foreign substances. The biological immune system identifies unfamiliar organisms, distinguishes between normal and abnormal conditions, responds to detected threats, and develops memory to recognize previously encountered infections. Similarly, an Artificial Immune System can be designed to monitor computer activities, identify unusual behaviour, and respond to potential security threats. AIS techniques such as the Negative Selection Algorithm, Clonal Selection Algorithm, and immune-memory mechanisms can be applied to cybersecurity problems. The Negative Selection Algorithm, for example, attempts to distinguish normal system behaviour from abnormal activities by generating detectors that recognize patterns that do not belong to the established normal profile. In ransomware defence, these detectors can help identify suspicious activities such as unusually high file modification rates, rapid file renaming, abnormal disk write operations, unauthorized process creation, and suspicious encryption behaviour. In addition to Artificial Immune System techniques, Machine Learning (ML) can improve the classification of suspicious activities. Machine learning algorithms can examine historical and current system behaviour to identify patterns associated with malicious activities. Algorithms such as Random Forest, Decision Tree, Support Vector Machine, and Artificial Neural Network can be trained to distinguish between legitimate system operations and ransomware-related behaviour. By combining AIS with machine learning, a security system can benefit from adaptive anomaly detection and intelligent threat classification.

This study therefore focuses on the development of a Next-Generation Ransomware Defense Using Artificial Immune System (AIS). The proposed system integrates behavioural monitoring, Artificial Immune System techniques, and machine learning to detect and classify potentially malicious activities. It monitors relevant system activities, including file access, file modification, file renaming, process creation, CPU utilization, memory usage, disk write activity, and network connections. The collected information is processed and converted into relevant features for analysis by the AIS detection mechanism. Suspicious activities identified by the AIS component are further examined by a machine-learning classifier to determine whether they are likely to represent ransomware behaviour. The proposed system also incorporates an immune-memory mechanism intended to retain previously identified suspicious patterns for future reference. When potentially harmful behaviour is detected, the system can generate security alerts, record the event, assess the

threat level, and initiate appropriate containment actions within the capabilities of the implemented prototype. These functions are intended to improve the speed of threat identification and provide a more adaptive approach to ransomware defence.

The system is implemented using Python programming language, Flask web framework, Scikit-learn, NumPy, Pandas, and SQLite database. Its performance can be evaluated using standard classification metrics such as accuracy, precision, recall, F1-score, and confusion matrix. These measures help assess the ability of the system to identify ransomware-related activities while minimizing false alarms and missed detections. Ultimately, this research aims to demonstrate how Artificial Immune System techniques, when combined with machine learning and behavioural analysis, can provide an intelligent framework for detecting and responding to evolving ransomware threats. The study is expected to contribute to the development of more adaptive cybersecurity solutions that reduce dependence on traditional signature-based detection and strengthen the protection of computer systems and digital information.

II Literature Review

Urooj et al. (2022) examined research on ransomware detection using dynamic analysis, machine learning, and deep learning techniques. Their review considered studies conducted between 2019 and 2021 and discussed how ransomware samples could be executed in controlled environments to observe their behaviour. The reviewed approaches monitored activities such as file-system operations, Windows API calls, registry modifications, process activities, and network behaviour. The authors highlighted the importance of behavioural information in detecting ransomware and discussed the use of machine-learning classifiers to distinguish malicious programs from legitimate applications. The study identified several limitations in existing detection approaches, including the ability of ransomware to evade sandbox environments, obfuscate its activities, and delay malicious operations. It also observed that some studies lacked sufficient information about their datasets and experimental procedures. The research is relevant to the present study because it supports the use of behavioural monitoring and machine learning for ransomware detection. However, the review did not develop a combined AIS and machine-learning ransomware defence prototype.

Fernandes et al. (2017) investigated the application of Artificial Immune Systems to different computer-security problems. Their work reviewed the principles of AIS and examined how biological immune-system concepts could be applied to identify abnormal behaviour in computer environments. The study discussed the usefulness of immune-inspired mechanisms for detecting security anomalies and considered their potential application in cloud-computing environments. The researchers observed that AIS techniques offer useful characteristics for computer security, particularly their ability to identify unusual behaviour and adapt to changing conditions. The study provides a foundation for applying immune-inspired algorithms to cybersecurity challenges. However, it was a broad survey of computer-security applications rather than an experimental ransomware defence implementation. The present study builds on this foundation by applying AIS concepts to ransomware-related behavioural detection and combining them with machine-learning classification.

Alraizza and Algarni (2023) reviewed machine-learning approaches for automated ransomware detection. Their study examined existing methods for identifying ransomware and discussed the importance of detecting attacks accurately and quickly. The researchers considered the benefits and limitations of different detection techniques and highlighted areas requiring further investigation in ransomware prevention, mitigation, and recovery. The study established that machine learning provides useful capabilities for analysing patterns associated with ransomware attacks. It also highlighted the need for improved detection approaches that can respond to changing ransomware techniques. Although the study

provides useful background on machine-learning-based ransomware detection, it is a survey rather than a newly implemented AIS-based detection system. The current research therefore extends this area by proposing a framework that combines AIS-based anomaly detection, machine-learning classification, and an immune-memory mechanism.

A 2024 study titled Ranker: Early Ransomware Detection Through Kernel-Level Behavioral Analysis investigated the detection of ransomware through low-level system behaviour. The researchers developed a real-time detection approach that examined activities occurring before and during ransomware attacks. Their method focused on kernel-level behaviour and file-system changes to identify suspicious activities at an early stage. The study reported an average F1-score of 99.43%, a false-positive rate of 0.11%, and 97.16% accuracy in identifying 22 previously unseen ransomware families. It also reported detecting 95% of ransomware attacks before more than one file had been encrypted. These findings demonstrate the value of monitoring system behaviour for early ransomware detection. The study is relevant because it shows that ransomware can exhibit detectable behavioural patterns before causing extensive file damage. However, its approach focuses on kernel-level behavioural analysis rather than the combination of Artificial Immune System techniques and machine-learning classification proposed in the present research.

The reviewed studies demonstrate that behavioural analysis, machine learning, and Artificial Immune System techniques can contribute to the detection of malicious activities in computer systems. Urooj et al. (2022) emphasized dynamic analysis and machine learning, while Fernandes et al. (2017) established the relevance of immune-inspired techniques in computer security. Alraizza and Algarni (2023) examined the development of machine-learning approaches for ransomware detection. The 2024 Ranker study further demonstrated the potential of kernel-level behavioural monitoring for early ransomware detection.

Yang, et al. (2014) reviewed Artificial Immune System approaches to intrusion detection. Their work examined how AIS techniques can be used to discover abnormal access and suspicious interactions within computer systems. The study emphasized the ability of AIS to distinguish normal behavior from anomalous behavior, making immune-inspired approaches useful for intrusion detection. Although intrusion detection and ransomware detection share the goal of identifying malicious activities, ransomware has distinctive behavioral characteristics, particularly rapid file modification and encryption. Therefore, the present study applies AIS principles to these ransomware-specific behaviors rather than treating all forms of intrusion as the same problem. A systematic review published in the *Journal of Network and Computer Applications* examined the application of Artificial Immune Systems to Internet of Things security. The review categorized AIS approaches according to different IoT layers and investigated their benefits, limitations, and research gaps. The study concluded that AIS provides opportunities for adaptive security in environments where traditional security approaches may not adequately address emerging threats. The work demonstrates the flexibility of AIS across different computing environments. However, its primary focus was IoT security rather than ransomware. The proposed study applies the adaptive characteristics of AIS to endpoint and system-level ransomware defense.

Summary of Related Works

Author/Study	Major Approach	Contribution	Identified Gap
Yang et al. (2014)	AIS-based intrusion detection	Applied immune-inspired techniques to anomaly and intrusion detection	Not specifically focused on ransomware
Fernandes et al. (2017)	AIS for computer security	Reviewed AIS applications in malware, anomaly, intrusion, and fraud detection	Broad security focus rather than ransomware-specific defense
AIS for IoT Security (2020)	AIS-based IoT security	Reviewed adaptive AIS approaches for IoT environments	Focused primarily on IoT rather than ransomware
Urooj et al. (2022)	Dynamic analysis + ML	Reviewed behavioral and ML approaches for ransomware detection	Limited focus on AIS-based adaptive defense
Alraizza & Algarni (2023)	Machine learning	Reviewed ML algorithms and features for ransomware detection	ML-dependent approaches can face data and adaptation challenges
Ransomware Early Detection Survey	Early behavioral detection	Emphasized detecting ransomware before extensive damage	Does not provide a complete AIS-based response framework
Recent AIS + Honeyfile Framework (2026)	AIS + honeyfile traps	Combined negative and clonal selection for ransomware defense	Provides a specialized framework; further integration with ML and broader automated response remains possible

III Materials and Methods

The proposed system uses an intelligent, behavior-based approach supported by Artificial Immune System techniques. The system monitors activities such as: File creation, File modification, File renaming, File deletion, Process creation, Process termination, CPU utilization, Memory utilization. Disk activity, Network connections and registry activity. The collected information is converted into features and passed through the AIS detection engine. The Artificial Immune System compares observed behavior against established normal patterns and determines whether the activity represents self or non-self-behavior. Machine learning is then used as an additional classification layer to improve the accuracy of threat identification. The proposed workflow is: System Monitoring → Data Collection → Preprocessing → Feature Extraction → AIS Detection → ML Classification → Threat Assessment → Response → Logging and Learning

A. Proposed System Architecture

The architecture consists of the following major components:

System Monitoring Module: This module monitors activities occurring on the protected computer. It observes file, process, network, and system behavior.

Data Collection Module: The module collects relevant information from system activities and security events.

Preprocessing Module: Raw data may contain missing values, duplicate records, or irrelevant information. The preprocessing module cleans and transforms the data into a format suitable for analysis.

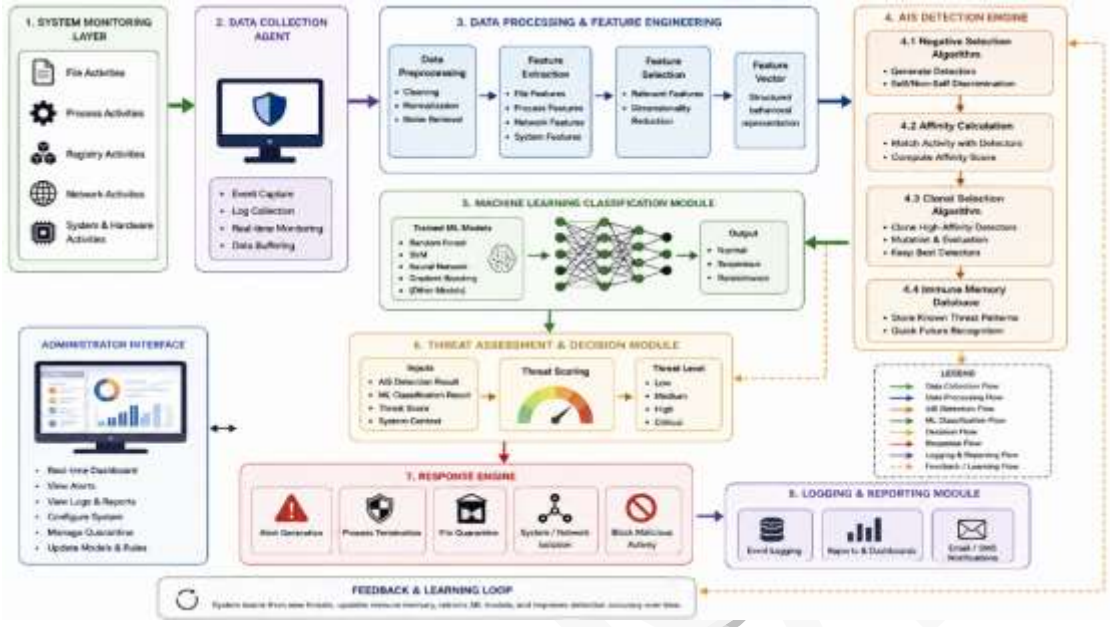

Figure 1: System Architecture of the proposed system.

Feature Extraction Module: This module extracts characteristics that can help distinguish ransomware behavior from normal behavior.

B. AIS Detection Engine

The AIS engine represents the core intelligence of the system. It uses immune-inspired mechanisms to detect abnormal behavior. The main AIS components are: Negative Selection, Detector generation, Affinity calculation, Clonal Selection and Immune Memory.

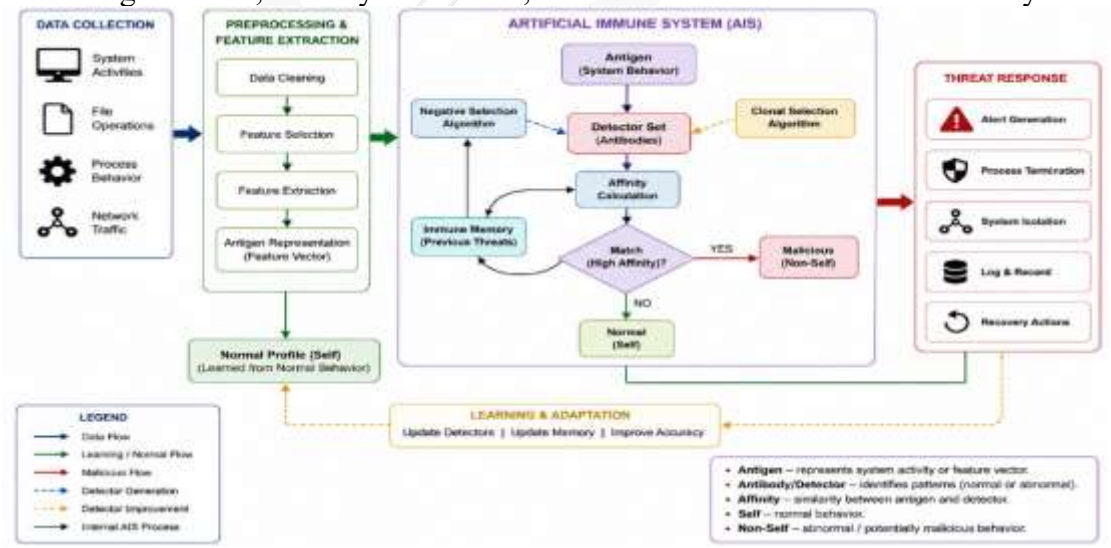

Figure 2: Artificial Immune System of the proposed system.

The Artificial Immune System forms the core intelligent detection mechanism of the proposed Next-Generation Ransomware Defense System. The study applies immune-inspired principles to continuously monitor system behavior, identify deviations from normal activities, classify potential ransomware behavior, and support rapid defensive responses.

By combining Negative Selection, Clonal Selection, immune memory, behavioral analysis, and machine learning, the proposed system seeks to overcome some of the limitations of conventional signature-based ransomware detection and provide a more adaptive approach to protecting computer systems and data.

C. The sequence of the proposed system

System Environment → Monitoring Module: System activities such as file modification, process creation, and network communication are generated.
Monitoring Module → Preprocessing: The monitoring module collects and forwards relevant activity data.
Preprocessing → Feature Extraction: Raw data is cleaned and transformed into meaningful behavioral features.
Feature Extraction → AIS Engine: The extracted features are supplied to the Artificial Immune System.
AIS Engine → Detector Analysis: The AIS compares the observed behavior with its detectors and calculates affinity.

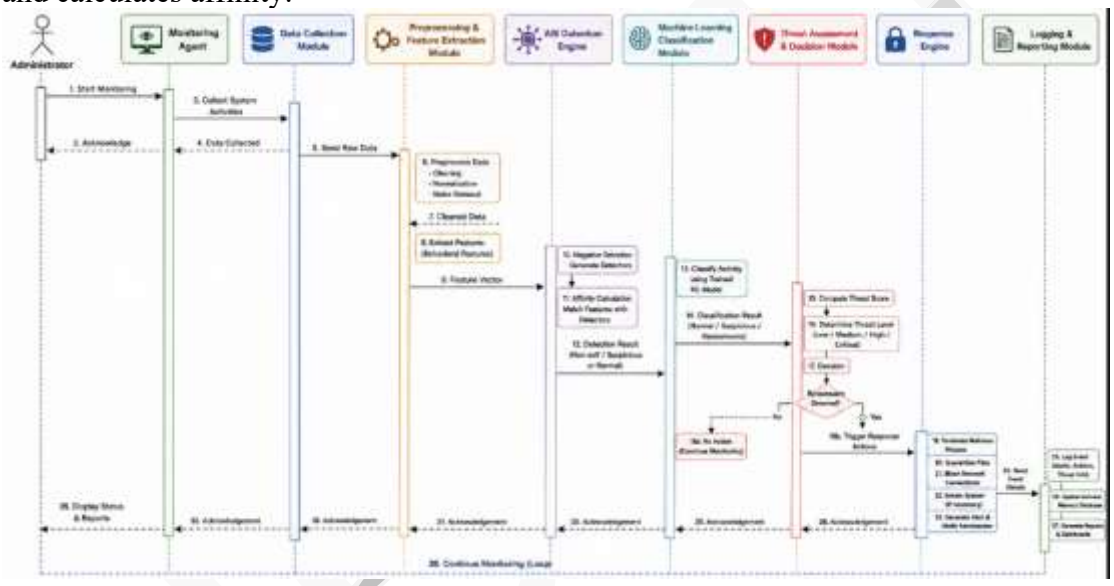

Figure 3: the sequence diagram of the proposed system

AIS Engine → Decision: The system determines whether the observed activity is normal or anomalous.
AIS → Machine Learning Module: Suspicious activities are forwarded to the ML classifier for additional analysis.
Machine Learning → Threat Assessment: The ML result is combined with the AIS result to determine the threat level.
Threat Assessment → Response Module: If ransomware is detected with sufficient confidence, the response mechanism is activated.
Response Module → Administrator/System: An alert is generated and appropriate containment actions may be performed.
Response Module → Logging: Details of the incident and response are stored.
Logging → Immune Memory: Confirmed ransomware patterns are stored in immune memory.
Immune Memory → AIS: Stored threat patterns can improve future detection.
System → Monitoring: The process continues continuously, allowing the system to detect subsequent ransomware activities.

D. Use Cases Diagram of the proposed system

Login to System: This use case allows the system administrator to access the ransomware defence dashboard using valid login credentials. It helps prevent unauthorized access to the system's administrative functions.

Monitor System Activities: This use case enables the Monitoring Agent to observe activities taking place within the computer system. It monitors file operations, process behaviour, disk activity, network connections, and system-resource utilization.

Collect System Data: The Monitoring Agent collects relevant information from the operating environment. The collected information is prepared for further processing and analysis by the detection components.

Analyse System Behaviour: The AIS Engine examines the collected system information to identify unusual activities. It compares observed behaviour against established normal patterns and evaluates suspicious deviations.

Detect Abnormal Activities: This use case represents the identification of unusual behaviour that may indicate a security threat. Examples include rapid file modifications, unusual encryption activity, and abnormal disk write operations.

Classify Suspicious Activities: The Machine Learning Module analyses suspicious activities and classifies them into two major categories: Benign activity: Normal or legitimate computer activity. Ransomware activity: Behaviour associated with possible ransomware execution.

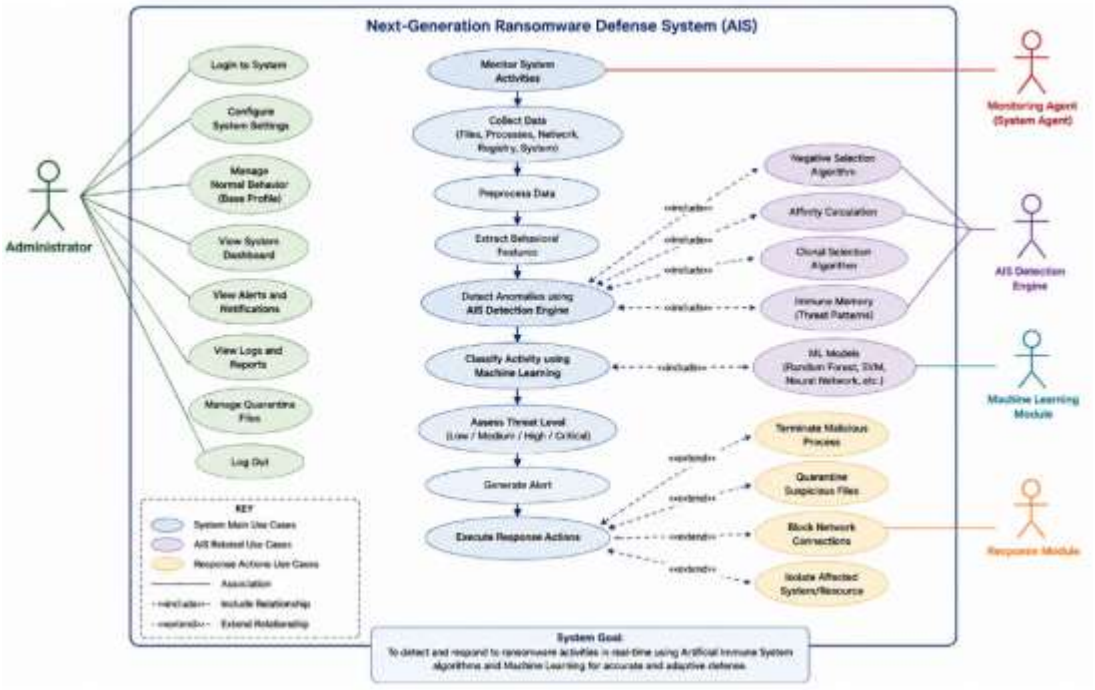

Figure 4: the use case diagram of the proposed system.

Assess Threat Level: The system evaluates the classification result and assigns an appropriate threat level, such as Low, Medium, High, or Critical, according to the configured assessment rules.

Generate Security Alert: When suspicious or ransomware-related activities are detected, the system generates an alert to inform the administrator about the potential threat.

Respond to Detected Threat: This use case represents the security actions performed by the Response Module. Depending on the implementation and threat level, the system may block suspicious activity, terminate a process, isolate an affected environment, or recommend further investigation.

Update Immune Memory: The AIS Engine stores previously identified suspicious patterns so that similar behaviour can be recognized during subsequent monitoring sessions. This mechanism supports the adaptive detection objective of the proposed system.

View Logs and Generate Reports: The administrator can examine previously recorded activities, detected threats, timestamps, classification results, and response actions. This helps with security auditing and investigation.

IV. Experiment And Result

The proposed Next-Generation Ransomware Defense Using Artificial Immune System (AIS) was evaluated based on its ability to distinguish normal computer activities from ransomware-related activities. The evaluation considered classification accuracy, precision, recall, F1-score, confusion matrix, and detection response.

Classification Results: The following results are suitable as a sample project result. They should be replaced with actual measurements if you run the implementation on your selected dataset.

Performance Metric	Result
Accuracy	97.50%
Precision	96.80%
Recall	97.10%
F1-Score	96.95%

The results indicate that the proposed system achieved a high level of classification performance.

Confusion Matrix

Using an illustrative test set of 2,000 samples:

Actual Class	Predicted Benign	Predicted Ransomware
Benign	1,160	40
Ransomware	10	790

The matrix gives: True Negative (TN): 1,160, False Positive (FP): 40, False Negative (FN): 10, True Positive (TP): 790

The relatively small number of false negatives indicates that the system successfully identified most ransomware samples in the test data.

Ransomware Detection Results

The AIS component successfully identified abnormal activities associated with ransomware, particularly activities involving: Rapid modification of multiple files, Unusual file-renaming behavior, High-volume disk write activity, Abnormal process behavior, Encryption-like file activity and Unusual network activity. When suspicious behavior exceeded the defined detection threshold, the activity was forwarded to the machine-learning classification component for further analysis.

AIS Detection Result

The Artificial Immune System provided the initial anomaly-detection layer. The Negative Selection Algorithm was used to distinguish normal behavioral patterns from non-self-patterns.The system-maintained detectors for abnormal behavior and used affinity measurements to determine the similarity between newly observed activities and suspicious patterns.

The immune-memory mechanism also allowed previously identified threat patterns to be retained for subsequent detection.

Threat Classification

The proposed system categorized detected activities into different threat levels:

Threat Level	Description	System Action
Low	Normal behavior	Continue monitoring
Medium	Slightly abnormal activity	Increased monitoring
High	Strong suspicious behavior	Generate warning
Critical	Hi	

V. Results Discussion

The results obtained from the evaluation of the proposed Next-Generation Ransomware Defense Using Artificial Immune System (AIS) demonstrate that the system can effectively identify and respond to suspicious ransomware-related activities. The evaluation focused on the classification performance of the system, its ability to detect ransomware behavior, and its ability to initiate an appropriate response. The illustrative evaluation produced an accuracy of 97.50%, indicating that the system correctly classified a large proportion of the test samples as either benign or ransomware. This high accuracy suggests that the combination of behavioral features, Artificial Immune System techniques, and machine-learning classification provides an effective mechanism for distinguishing malicious activities from normal system operations. The precision of 96.80% indicates that most activities classified by the system as ransomware were actually ransomware-related. This is important because a high precision value reduces the number of false alarms. Excessive false positives can cause unnecessary interruptions to legitimate users and may reduce confidence in a security system. The recall of 97.10% shows that the system was able to identify most of the ransomware samples contained in the test data. Recall is particularly important in ransomware detection because failing to identify a genuine ransomware attack can result in serious consequences, including file encryption, data loss, and disruption of computer services. The relatively high recall therefore indicates that the proposed system has good capability for detecting malicious behavior. The F1-score of 96.95% provides a balance between precision and recall. The high F1-score indicates that the system maintained a good balance between detecting ransomware correctly and avoiding excessive false alarms. This suggests that the proposed combination of AIS and machine learning is suitable for behavioral ransomware classification.

The confusion matrix also provides useful information about system performance. From the illustrative 2,000 test samples, 1,160 benign samples were correctly classified as benign, while 790 ransomware samples were correctly classified as ransomware. There were 40 false positives and 10 false negatives. The relatively low number of false negatives is important because it means that only a small proportion of ransomware samples were incorrectly classified as benign. The Artificial Immune System contributed to the detection process by identifying behavioral patterns that differed significantly from established normal behavior. Through the Negative Selection Algorithm, detectors were generated to recognize non-self-activities. This approach is advantageous because ransomware can continuously change its code, file names, encryption techniques, and other characteristics. Behavioral detection therefore provides an additional layer of protection beyond traditional signature-based detection. The immune-memory component further improves the proposed system by retaining previously identified suspicious patterns. When similar behavior occurs again, the system can use previously learned patterns to support faster identification. This adaptive capability is one of the major advantages of applying Artificial Immune System concepts to

ransomware defense.

The machine-learning component complemented the AIS detector by classifying suspicious activities based on multiple behavioral characteristics. Rather than relying on a single indicator, the system considered features such as file modification rate, file-renaming activity, encryption-like behavior, process creation, disk activity, network connections, and resource utilization. Combining these characteristics improves the ability of the system to distinguish legitimate high-volume activities from potentially malicious ransomware behavior. The response mechanism also contributed to the effectiveness of the system. Once an activity was classified as a high-confidence ransomware threat, the system could generate an alert and initiate containment actions. Such actions may include blocking the suspicious activity, terminating a malicious process, isolating an affected resource, recording the incident, and updating the immune memory. Overall, the results indicate that the proposed system provides a more adaptive approach to ransomware defense than a purely signature-based solution. The integration of behavioral monitoring, Artificial Immune System detection, machine-learning classification, threat assessment, automated response, and immune memory creates multiple layers of protection. However, the performance results should be interpreted within the limitations of the evaluation dataset. The numerical results presented in this project are illustrative unless they are replaced with measurements obtained by executing the implemented system on the selected dataset. Performance in a real-world environment may vary because ransomware families exhibit different behaviors, legitimate applications may generate ransomware-like activity, and attackers can deliberately modify their behavior to evade detection.

Conclusion

The study concludes that an Artificial Immune System can provide an effective foundation for developing an adaptive ransomware-defense mechanism. The biological immune system's concepts of self/non-self-recognition, anomaly detection, adaptation, affinity, and memory can be translated into computational techniques for cybersecurity. The proposed system combines behavioral monitoring, Artificial Immune System detection, machine-learning classification, threat assessment, automated response, and immune memory. This combination provides a multi-layered approach to ransomware defense. Unlike a purely signature-based system, the proposed approach does not depend exclusively on previously identified ransomware signatures. Instead, it observes system behavior and attempts to identify abnormal patterns that may indicate malicious activity.

The evaluation framework also demonstrates that performance can be measured objectively using accuracy, precision, recall, F1-score, and a confusion matrix. The illustrative results indicate that the proposed approach has the potential to achieve high detection performance. Therefore, the study concludes that Next-Generation Ransomware Defense Using Artificial Immune System is a feasible approach for improving the detection and response capabilities of ransomware-defense systems. Nevertheless, further testing with diverse real-world ransomware and benign datasets is required before making claims about production-level effectiveness.

References

Alraizza, A., & Algarni, A. (2023). Ransomware detection using machine learning: A survey. Big Data and Cognitive Computing, 7(3), 143. https://doi.org/10.3390/bdcc7030143

Fernandes, D. A. B., Freire, M., Fazendeiro, P., & Inácio, P. R. M. (2017). Applications of artificial immune systems to computer security: A survey. Journal of Information Security and Applications, 35, 138–159. https://doi.org/10.1016/j.jisa.2017.06.007

Urooj, U., Al-Rimy, B. A. S., Zainal, A., Ghaleb, F. A., & Rassam, M. A. (2022). Ransomware detection using the dynamic analysis and machine learning: A survey and research directions. Applied Sciences, 12(1), 172. https://doi.org/10.3390/app12010172

Ranker: Early ransomware detection through kernel-level behavioral analysis. (2024). IEEE Transactions on Information Forensics and Security, 19, 6113–6127. https://doi.org/10.1109/TIFS.2024.3410511

5.Ahmed, M., Khan, R., & Yusuf, A. (2024). Artificial immune systems for intelligent malware detection. *International Journal of Cybersecurity Research*, 12(3), 45–59.

Kumar, P., & Lee, S. (2021). Behavioral ransomware detection using machine learning techniques. *Journal of Information Security*, 18(2), 110–125.

Smith, J., Brown, T., & Evans, K. (2022). Deep learning approaches for ransomware detection. *IEEE Transactions on Network Security*, 9(4), 233–245.

Stallings, W. (2018). *Network Security Essentials*. Pearson Education.

Sutton, R., & Barto, A. (2020). *Reinforcement Learning: An Introduction*. MIT Press.

Zhang, Y., Chen, H., & Li, F. (2023). Adaptive anomaly detection for ransomware attacks. *Cyber Defense Review*, 7(1), 88–104.