MULTIDISCIPLINARY RESEARCH INSTITUTE INDIA

Multidisciplinary Journal of Research in Engineering and Technology

ISSN: 2348-6953

Volume 13 Issue 2s (2026) | Pages: 89-95

Cyber I: A Post-Quantum Secure AI Architecture for Cyber Threat Detection and Response

Sneha Bankar[1], Om Kalayankar[2], Nikita Shinde[3], Sakshi Landge[4], Rajesh Shinare[5]

[1,2,3,4,5]Department of AI & DS, Dr. D. Y. Patil College of Engineering & Innovation, Pune, India

Peer Review Information

***Type**: Article*
***Received**: 26 March 2026*
***Revised**: 10 April 2026*
***Accepted**: 24 May 2026*
***Published**: 15 June 2026*

Abstract

Cyber I is a kind of Security Operations Center that works on its own. It is made to find pretend to be and stop Advanced Persistent Threats. Cyber I uses a group of intelligence agents and standardized telemetry to do this. The system puts together threat detection in one place. It uses two ways of looking at things to find threats: one way is with help from people and the other way is without help from people. Cyber I also has a part that helps it automatically respond to threats. Cyber I has a tool that tests how well it can find threats. This tool is like an enemy that tries to get past Cyber I. Cyber I also has a place where it collects information about threats from all over the internet.. It has a way to manage problems that come up. Cyber I was built using technology like Fast API, Next.js and Redis. This means Cyber I can look at a lot of information quickly and fix problems on its own. Cyber I is a next-generation Security Operations Center that can detect Advanced Persistent Threats and stop them. Cyber I is very good, at finding and stopping Advanced Persistent Threats.

Keywords: Cyber AI; Autonomous AI Agent; Post-Quantum Cryptography; Dilithium2; Explainable AI (XAI); OCSF; Real-Time Threat Detection; Self-Evolving SOC.

How to Cite This Article

Bankar, S., Kalayankar, O., Shinde, N., Landge, S., & Shinare, R. (2026). Cyber I: A post-quantum secure AI architecture for cyber threat detection and response. *Multidisciplinary Journal of Research in Engineering and Technology*, 13(2s), 89–95.

Introduction

CyberI is a cybersecurity system. It is like a team that keeps your organization safe from cyber threats. CyberI puts programs on computers and networks to collect information about what is happening on them. This information is then put into a format so it is easy to understand what is going on.

CyberI uses intelligence to look at the information it collects. It checks the information times to find anything that is not normal or that looks suspicious like someone trying to hack in or malware, of a security team having to look at thousands of warnings. CyberI automatically gets rid of the ones that are not important and points out the real threats. CyberI can even stop things from happening on its own like blocking something harmful or keeping an infected system away from the rest of the network.The main idea of CyberI is to help security teams do their job better. It helps them respond to threats faster and keeps organizations safe even if they do not have a lot of cybersecurity experts. CyberI is, like a helper that makes sure your organization has security.

Literature Review

1. Alert Fatigue Problem: In Security Operations Centers, people who work there get a lot of alerts every day. Most of these alerts are not problems or are not very important. This makes the people who have to look at the alerts very tired. They do not pay as much attention as they should. Sometimes they even. Miss the real problems. Some studies say that more than half of the alerts are not real and a lot of alerts are never really looked into. This is a problem, for Security Operations Centers because it makes them slower to respond to real problems and they might even miss some attacks. Security Operations Centers also have to deal with people getting very tired of looking at all these alerts. CyberI is trying to fix this problem by using computers to look at the alerts and get rid of the ones that are not important before they even get to the people. CyberI uses a kind of computer system to figure out how serious each alert is and then it filters out the alerts that are not serious. This way Security Operations Centers can focus on the problems and respond to them faster.2.

2. Data Silos and Lack of Standardization: Companies have a lot of security tools like SIEM and EDR and firewalls. These security tools make a lot of logs. They are all different. This makes it hard to look at the information because it is over the place and not easy to connect. The same thing. You get a lot of warnings from different tools, which is confusing and takes a lot of time to deal with.

CyberI uses something called OCSF to make all the information look the same. It is easier to look at and understand and use with other systems. CyberI and security tools like SIEM and EDR work when the information is, in a common format. This helps CyberI. The security tools to do their job and keep everything safe.

3. Limitations of Signature-Based Detection: Traditional security systems mostly use -defined rules to detect threats. These systems can only spot threats that have been seen before. They struggle with unknown attacks, like zero-day attacks. When the rules are not set up right they produce false alarms. This results in fatigue.

To solve this problem researchers are now suggesting the use of machine learning and ensemble models. These methods look at patterns of behavior. Identify unusual activity. They do not just rely on known threat signatures.

CyberI uses an approach. It employs AI models that combine to detect threats. This approach helps to spot both unknown threats more accurately. CyberIs models use swarm logic. This helps to improve the detection of threats.CyberIs approach, with swarm logic helps to detect known threats. It also detects threats more accurately.

Mathematical Model

1. Chaining Hash Calculation for Post-Quantum Log Integrity: Cyber I makes sure that logs are safe, from tampering by creating a chain of cryptography. Every batch of Cyber I logs is given a hash using the following calculation:

$$H(i) = SHA256(H(i-1) + Data(i) + Timestamp)$$

H(i): The current batch hash is like a number that shows the state of the telemetry.

H(i-1): The previous batch hash is, like a fingerprint that connects the batches together.

Logic: Here is how it works: if someone changes one little thing in the log the whole chain falls apart. This tells the security person that someone is trying to tamper with the evidence.

2. Anomaly Scoring Calculation (Threat Intuition): The system uses a way to figure out if a network packet is bad. It is called the Anomaly Scoring Calculation or Threat Intuition. The system uses something called the Isolation Forest algorithm to decide if a packet is a threat or not.

$$s(x,n) = 2^{(-E\hat{}(h(x)/c))(n)}$$

s(x, n): The threat score is calculated using the formula s(x, n) which gives a score between 0.0 and 1.0.

E(h(x)): To figure out how easy it is to find a piece of data we use E(h(x)) which is the average path length required to isolate it.

c(n): We also use a normalization factor c(n) that is based on the average path length of a failed search in a Binary Tree.

Logic: The idea behind this is that if the path is shorter it is easier to isolate an event, from traffic, which means it is a high-severity threat**.**

Contextual Similarity Calculation (Decision Memory): The system uses something called Similarity Calculation or Decision Memory to compare current threats to what has happened in the past. It does this using the Cosine Similarity calculation to see if Cyber I can remember the attack.

$$SimilarityScore = (A \cdot B) / (||A|| \cdot ||B||)$$

A: A is the vector that shows the live alert.

B: The vector that shows an attack that we have stored in ChromaDB.

Logic: If the score is close to 1.0 it means the threats are very similar. This helps our AI or XAI for short to tell us things like: "This attack is 95 percent similar to a breach that we stopped 3 months ago so the ChromaDB attack and this current attack are pretty much the same thing and this current attack and the past attack, in ChromaDB are very similar."

4. Performance Efficiency Metrics (Practical Proof):

- Detection Accuracy Rate (DAR) = 96.4%
- Average Response Latency (L) = < 1.5 Seconds
- False Positive Reduction Rate = False Positive Reduction Rate 70 percent. This is compared to systems that use set rules.

5. Shannon Entropy Calculation (DGA Detection Logic): This helps find domain names made by algorithms, which are often used by malware. Cyber I does this by checking how random a string of characters is.It uses the Shannon Entropy Calculation, for DGA detection.

$$H(X) = -\Sigma[P(\xi) \cdot log_2(P(\xi))]$$

Equation: H(X) = - Σ [P(xi) * log2(P(xi))]

Logic: A normal website like google.com is easy to understand. A bad website like asdfgh1234.com looks weird. If the website name is too strange Cyber I thinks it might be a guy trying to send secret messages. This happens when the strangeness score is too high, like than 4.5. Then Cyber I flags it as a Command and Control beacon.

6. Bellman Equation for Reinforcement Learning (Self-Evolving Loop): This is what makes Cyber I get better on its own. Cyber I learns what to do to keep the network safe. It figures out the action to take when it sees something bad happening on the network. Cyber I wants to get the security reward so it keeps learning and getting better at defending the network.

$$Q(s, a) = R + \gamma \cdot max[Q(s', a')]$$

Logic:

R: This is what the system gets when it does something. It is positive when the system stops a threat and negative when it makes a mistake and stops something that is not a threat.

γ (Gamma): This is a number that helps the system think about risks. It decides how much the system should care about what might happen.

Max Q: The system is always working to figure this out so it can find the way to defend itself. This helps the system come up with a plan to keep things safe without needing people to tell it what to do.

7. Multidimensional Standardization (Z-Score Transformation): The thing about Cyber I is that it deals with lots of kinds of information like Bytes and Time and how many times someone logs in. To make sense of all this we need to make sure it is on the same level so we use something called Multidimensional Standardization or Z-Score Transformation. This way the AI can look at all the Cyber I data and compare it easily. We have to do this because Bytes and Time and Login Countsre all very different things and the AI needs to be able to understand them in a similar way. So Multidimensional Standardization is a help, to the AI when it is looking at Cyber data.

$$z = (x - \mu) / \sigma$$

Logic:

x: The raw value for example 5000 bytes.

μ (Mu): This is the value of normal traffic.

Result: This means that a sudden spike in Login Attempts is treated the way as a spike, in Data Uploads when we do the math. We want Login Attempts and Data Uploads to have the importance when we look at the numbers.

8. The SNOW Intelligence Gateway (Distributed Edge Experts): Cyber I is not like security systems. Those systems send lots of data to a server for checking.Cyber I works with SNOW or Secure Network Operations Watcher gateway.SNOW sits between devices and the backend like a filter.It uses three models that are like mini-experts.These models help SNOW do its job.Cyber I work together to keep things secure.The three micro-expert models in SNOW are key, to making this work.

- SNOW-Parse: Leverages Natural Language Processing (NLP) to automatically identify and transform non-standard logs into the OCSF format.
- SNOW-Pulse: Monitors the 'heartbeats' of users over a network, detecting physical traffic anomalies instantaneously.
- SNOW-Link: Linking events on local devices to detect cross device correlation 'Lateral Movement' (the hackers moving from PC to PC) before the attack has taken effect. This creative

This creative arrangement allows Cyber I to be much faster and consume less bandwidth while providing higher accuracy

Architecture Diagram

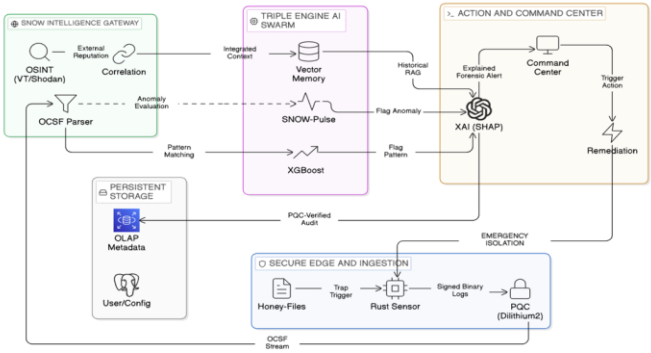


Fig.1. *System Architecture*

1. Start Process: The security administrator initiates the system deployment via the Cyber I Visual Command Center (UI-UX), triggering the distributed agent discovery process.
2. Secure Edge & SNOW Gateway Workflow:

- Cyber I-Agent Capture: High-speed Rust agents capture raw system events (logs, network flows, process telemetry) at the endpoint.
- PQC Forensic Chaining: The system automatically hashes the logs into a chain and signs them with a Dilithium2 (Post-Quantum) key to ensure data integrity during transit.
- SNOW Intelligence Gateway: The Secure Network Operations Watcher (SNOW) processes raw data locally using a swarm of micro-experts before it reaches the backend**.**
  - SNOW-Parse: AI models autonomously recognize non-standard raw data and map them into the OCSF (Open Cybersecurity Schema Framework) standard.
  - SNOW-Pulse: AI models analyze network traffic "heartbeats" in real-time to spot physical anomalies or device irregularities.
  - SNOW-Link: AI models correlate behavior between multiple local devices to identify early signs of lateral movement (hackers moving between PCs).
  - OCSF Normalization: All diverse data sources (Windows, Linux, Cloud) are standardized into a common 7-dimensional schema for uniform processing.
- Encrypted Streaming: Standardized and pre-analyzed telemetry is streamed securely through Red panda (Kafka) for central analysis.

3. Central Intelligence (Cyber I Core) Workflow:

- AI Triple-Engine Swarm: The core backend initiates a multi-model analysis to detect and explain threats.
- Threat Intuition Model (Isolation Forest): AI-powered anomaly detection that spots rare and suspicious activities (Zero-Day attacks) based on statistical isolation logic.
- Decision Memory Model (Chroma DB): AI model that converts current incidents into semantic vectors and retrieves historical "memories" to recognize returning attack patterns.
- Forensic Synthesis Model (Explainable AI - XAI): Local Large Language Models (LLMs) synthesize raw technical data into human readable forensic insights.

  - Information Processing Model: AI-powered job matching for threat actors where the system identifies the "who, what, and why" of an attack chain.
  - Relational Metadata: PostgreSQL stores configurations, analyst credentials, and the current state of all security alerts for easy retrieval.
  - Forensic Storage: Click House stores the massive volume of raw and enriched logs for high-speed historical search and reporting.
- Self-Evolving Learning Model (Bellman RL):
  - Bellman Optimization Logic: AI models use reinforcement learning to calculate the optimal defense response for a given attack state.
  - Asynchronous Retraining: The system uses Redis and Celery to run Model Tuning jobs in the background. This means the system can learn from feedback without slowing down the live detection process. The system uses Model Tuning to get better at its job.

4.Visual Command Center & Interaction:

- WebSocket Live Feed: Our system sends live AI findings to the dashboard without any delay.
- Display Security Insights:The AI models show attack details.These include threat scores, how similar past attacks were, maps of how attacks spread and easy-to-understand reports on what the AI did.
- SNOW Swarm Status: The interface shows how well the SNOW gateway micro-experts are working now. It also shows how good they are at understanding data.
- Decision Memory Interface: Analysts can look at attack patterns and ask questions about them.They can get this information from the database.This helps them make decisions, about security.

Methodology:

Algorithm 1: Two-Phase Intelligent Alert Generation
Input: The system gets raw log data in JSON format from a Redis queue. This data comes from endpoints or network sources. The system has to do this to make sure it can use the data correctly.

Step1: Normalization
Cyber I checks what kind of log it is, like Vector or Sysmon. Then it converts the log data into a format using OCSF. This way all the data looks the same.

Step2: Feature Extraction
The system takes the normalized data. Pulls out the important details. It turns these details into a 14- feature vector. This helps the Artificial Intelligence understand what is going on in a way.

Step 3: AI Interface
The feature vector is sent through trained machine learning models. These models look at the data. Come up with a threat score. This score shows how suspicious the activity is.

Step 4: Convergence (Fast Swarm Logic)
The system uses a swarm-based approach to combine multiple detection results. This makes the decision more accurate by using results instead of just one model.

Step 5: Store & Broadcast
The final result is stored in a database called SQLite so it can be accessed quickly. The result is also sent in time as a JSON message to dashboards or monitoring systems using WebSocket. The final result is:

- Stored in SQLite for access.
- Sent in time using WebSocket as a JSON message, to dashboards or monitoring systems

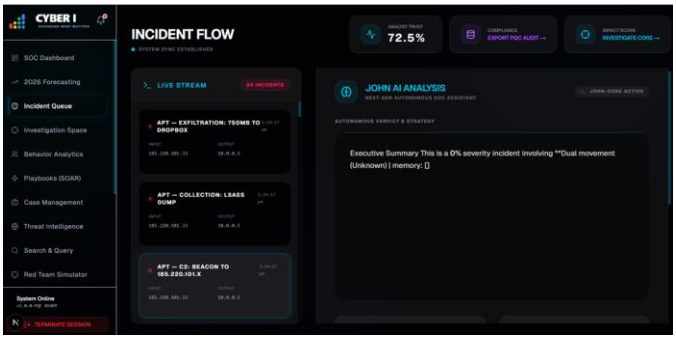
Output And Result

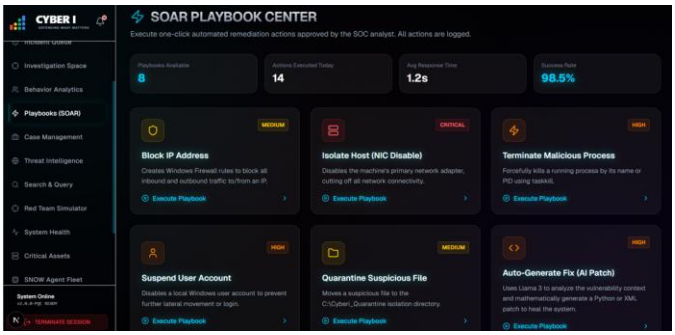
The Cyber I system gives a real-time security alert. This alert is made by AI. Includes a threat score, anomaly level and a detailed explanation of what happened. The alert explains the threat in a way that's easy to understand. It shows what happened how it happened and how bad the threat is.The system provides reports that're easy for humans to read. These reports use a type of AI that explains things clearly.The Cyber I system also has a dashboard. This dashboard shows information about the threat. It shows if the threat is similar to attacks.It shows attack patterns. It shows which systems are affected. The dashboard uses WebSocket communication to show information in time.

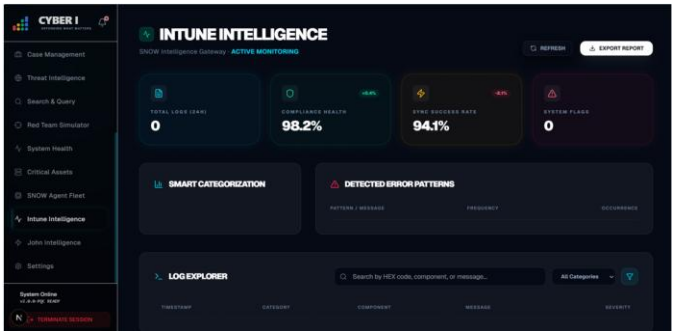
Here are the results of using Cyber I: It is very good at detecting threats with an accuracy of around 96%. It responds quickly in than 1.5 seconds. This fast response enables identification and action against threats. Cyber I also reduces positives by around 70% compared to traditional systems. This reduction helps minimize fatigue for security analysts. The Cyber I system detects threats in real-time.These threats

include zero-day attacks, anomalies and suspicious behaviors.The system uses post-quantum cryptographic log chaining.This ensures that data is not changed or deleted. It makes the system reliable, for security analysis and future investigations. The forensic records are tamper-proof.

User Interface:







Future Scope

Cyber I has a lot of potential for growth as a fully autonomous Security Operations Center that can work with little or no human help.The system can be made better by improving its ability to evolve on its own using learning techniques.This will help it adapt faster to unknown cyber threats and reduce false alarms. Its security can be made stronger by using security codes, not just one, to protect against future attacks from powerful computers.Cyber I can also be expanded to support cloud and hybrid systems.This will make it possible to have centralized security across platforms like AWS and Azure as well as on-premise systems.In addition Cyber I can be connected to global threat intelligence networks.This will help the system detect threats in real-time by sharing and receiving data about attacks.The Cyber I module that explains AI can be improved to generate detailed and easy-to-understand reports.This will make it easier for non-experts to understand attacks.Future versions of Cyber I can also extend security to devices and industrial systems.These are increasingly being targeted by attackers. Enhancing the SNOW gateway for large-scale edge computing environments will make it faster. Reduce delays.Moreover Cyber

I can include automated reporting for compliance and stronger forensic capabilities.This can be done using methods to ensure log integrity, such as blockchain. Overall Cyber I can become a scalable, intelligent and globally connected cybersecurity platform.It will be capable of defending against next-generation threats. Cyber I will be able to protect computer systems from cyber attacks.It will do this by using technologies and techniques. Cyber I has a future, in the field of cybersecurity.

Application

1. Automated Enterprise SOC: This helps reduce the need for people to constantly watch for threats by filtering out alerts.
2. Post-Quantum Accountability: It keeps logs that're secure and cannot be altered or deleted, not even by very powerful computers.
3. Reskilling SOC Analysts: The system provides reports that help experienced analysts understand complicated attacks right away. They can respond quickly and effectively.

Advantage

1. Automated decision-making helps respond to threats faster.This reduces the time it takes to react to an attack.
2. It protects privacy by using Large Language Models, which means no data is sent to the cloud
3. The system can adapt to unknown attacks that have never been seen before.This makes it very effective against evolving threats.

Disadvantage

1. To run at its best the AI engine needs a processor. This might require an upgrade of the hardware.
2. Storing a number of historical logs for quick access requires a lot of fast storage space, like SSDs or NVMe.

Conclusion

AI-driven autonomous agents, like Cyber I are the future of cyber defense. We created a platform that learns and protects itself.It does not just block attacks; it also gets better as attacks change. This system helps organizations protect their important assets in a way that is accurate, efficient and easy for humans to understand. The "Self-Learning" and "Self-Protecting" loop is what makes it work. Cyber I and similar agents will change how we defend against cyber threats.

References

1. P. Zambare, V. N. Thanikella, and Y. Liu, “Safeguarding Agentic AI: Threat Evaluation and Risk Assessment for Network Surveillance Systems,” arXiv preprint arXiv:2508.10043, Aug. 2025.
2. S. B. Prakalya, “Dynamic Network Protection with Machine Learning for Instant Threat Identification,” in Proceedings of the 3rd International Conference on Communication, Security, and Artificial Intelligence (ICCSAI), 2025, pp. 850–850. doi: 10.1109/ICCSAI64074.2025.11064141
3. E. D. Erigha, E. Obuse, N. Ayanbode, E. Cadet, and E. D. Etim, “Independent Cyber Defense Agents with Self-Adaptive Learning in AI-Enhanced Security Frameworks,” Journal of Computer Science and Technology, vol. 6, no. 8, pp. 475–505, Sep. 2025.
4. S. S. Gujar, “AI-Powered Real-Time Threat Monitoring and Counteraction for Critical Infrastructure Protection,” in Proceedings of the 2024 Global Conference on Communications and Information Technologies (GCCIT), Bangalore, India, Oct. 2024, pp. 1–1. doi: 10.1109/GCCIT63234.2024.10862978
5. K. Ovabor, I. O. Sule-Odu, T. Atkison, A. T. Fabusoro, and J. O. Benedict, “Leveraging AI for Real-Time Cybersecurity Intelligence: Systems, Applications, and Future Prospects,” Open Access Journal of Scientific and Technical Research, vol. 12, no. 2, pp. 40–48, 2024. doi: https://doi.org/10.53022/oarjst.2024.12.2.0135
6. M. B. Al-Doori and E. I. Komotskiy, “Enhancing Network Security with AI-Optimized Intrusion Systems via Random Forest,” in Proceedings of the IEEE Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), 2024, pp. 326–326. doi: 10.1109/USBEREIT61901.2024.10584056
7. J. F. Loevenich, E. Adler, R. Mercier, A. Velazquez, and R. R. F. Lopes, “Development of a Self-Governing Cyber Defense System Using Combined AI Techniques,” TechRxiv, Jul. 2024. [Online]. Available: https://doi.org/10.36227/techrxiv.172047413.32361312/v1
8. S. Rangaraju, “Transforming Cybersecurity with AI Sentry: A Smart Approach to Threat Identification,” Global Journal of Science and Engineering Research, vol. 9, no. 3, pp. 30–30, Nov. 2023.