A Bio-Inspired Blockchain-Based Adaptive Cyber Defense Framework for Hierarchical Network Infrastructures

Ankush Kumar Mohapatra
Department of Computer Engineering
International Institute of Information Technology
Bhubaneswar, India
ankushmohapatra2004@gmail.com

***Abstract*—Modern network infrastructures are increasingly exposed to sophisticated cyberattacks that exploit hierarchical privilege levels and data vulnerabilities. This paper proposes a bio-inspired, blockchain-enabled cyber defense framework inspired from the human immune system to provide adaptive, self-healing, and tamper-resistant security. The network is represented as a hierarchical binary tree, where the central server functions as the brain, network interface controllers (NIC) act as the nervous system, and individual nodes represent cells with varying privilege levels. When a low-privilege node is compromised, the framework employs crypto-shedding with salting to ensure that attackers obtain only irrecoverable data. Simultaneously, the compromised node is removed and replaced by a copy node embedded with an AI-based patching mechanism. This enables the system to record and recall attack vectors, mimicking the function of immune memory cells for a faster response to recurring threats. To prevent tampering, all system logs and node data are stored on a blockchain, ensuring transparency and immutability. The proposed model provides a novel approach to cybersecurity by integrating bio-inspired defense mechanisms with blockchain-backed data integrity, offering a scalable and adaptive solution for securing hierarchical networks across diverse applications.**

***Index Terms*—Adaptive cyber defense, Artificial immune system, Bio-inspired cybersecurity, Blockchain security, Self-healing networks.**

I. INTRODUCTION

The rapid expansion of digital infrastructures has introduced unprecedented complexity in managing and securing networks. As interconnected systems scale across industries, attackers exploit vulnerabilities by targeting low-privilege nodes and escalating privileges to compromise critical assets. Conventional security mechanisms such as firewalls, intrusion detection systems, and static encryption, while effective in specific contexts, often lack adaptability against dynamic and evolving attack strategies [1]. This limitation necessitates the development of defense models that are both self-healing and capable of proactive adaptation.

Biological systems, particularly the human immune system, provide a natural inspiration for designing adaptive cyber defense. The immune system identifies anomalies, eliminates compromised cells, and preserves memory of past attacks to enable faster responses to recurring threats. Translating these principles into digital networks can create architectures that resist intrusion, recover autonomously, and strengthen over time [2].

In this work, we propose a bio-inspired, blockchain-enabled cyber defense framework tailored for hierarchical network infrastructures. The framework models servers as the brain, network interface controllers as the nervous system, and nodes as cells arranged in a binary tree structure with varying privilege levels. Upon compromise of a low-level node, the system applies Reputation-Based Node Eviction [3]. The compromised node is immediately replaced with a copy node enhanced by AI-based patching, while attack vectors are stored as immune memory for future defense [4]. To further ensure tamper-proof integrity, all logs and node data are maintained using blockchain.

Hierarchical network architectures are widely used in real-world systems due to their scalability, modularity, and efficient management. In enterprise networks, hierarchical designs separate core, distribution, and access layers to optimize traffic flow and simplify management. Similarly, cloud infrastructures and data centers employ hierarchical structures to manage distributed resources efficiently. Critical infrastructures such as smart grids and industrial control systems (ICS) also follow hierarchical architectures, where physical devices, control systems, communication networks, and management layers are organized in multiple levels to ensure reliability and security. Additionally, hierarchical models are observed in intrusion detection systems, where attacks are classified at multiple levels, improving detection accuracy and interpretability. These applications highlight the importance of designing adaptive and resilient security mechanisms tailored for hierarchical environments.

The contributions of this paper are as follows:

1. A novel bio-inspired model for self-healing and adaptive cybersecurity in hierarchical networks.
2. Integration of blockchain for immutable logging and data protection [5].
3. An AI-driven patching mechanism that mimics immune memory for proactive threat mitigation.

The remainder of this paper is organized as follows: Section II reviews related work in bio-inspired and blockchain-based defense mechanisms. Section III describes the proposed framework in detail. Section IV presents implementation considerations and expected outcomes. Section V discusses challenges and future research opportunities. Section VI gives a brief case-study of the model. Section VII concludes the paper.

II. RELATED WORK

Cybersecurity research has traditionally focused on layered defense models involving firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS). While effective against known threats, such approaches often fail to adapt to novel or evolving attack vectors [6]. Encryption and hashing techniques further enhance confidentiality and integrity, but do not inherently prevent node compromise or privilege escalation attacks.

To address these limitations, **bio-inspired security models** have gained attention. Artificial Immune System (AIS) approaches mimic biological immune mechanisms to detect anomalies and respond adaptively. Studies have demonstrated the effectiveness of immune-inspired algorithms in detecting network intrusions and adapting to new attack signatures [7]. However, many of these models primarily focus on anomaly detection and lack comprehensive self-healing capabilities. Blockchain has emerged as a complementary technology for enhancing trust, integrity, and resilience in distributed systems. Its inherent immutability makes it suitable for secure logging and forensic analysis, where tamper-proof records are essential. In addition to logging, blockchain can support decentralized trust management, smart contract–driven automated defense, and the storage of attack signatures to act as a permanent "immune memory" [8]. Consensus mechanisms further enable collective anomaly detection among nodes, reducing false positives and ensuring collaborative mitigation [5], [9].
In summary, prior research has addressed anomaly detection, blockchain-based immutability, and AI-driven monitoring. However, there is a notable gap in integrating **bio-inspired adaptive defense, blockchain-based tamper-proof storage, and AI-enabled self-healing** into a unified framework for hierarchical network infrastructures. This gap forms the foundation of the proposed work.

TABLE I

Comparison of Existing Work with Proposed Approach

References	Summary	Limitations & Contribution of Proposed Work
[10]	El Gharbaoui et al. (2024) conducted a comprehensive review of AI and ML in network security, highlighting their effectiveness in anomaly detection, threat prediction, and automated response systems. The study emphasizes that while AI and ML significantly enhance detection accuracy and efficiency, they face challenges such as high computational cost, data privacy concerns, and limited real-world implementation. Unlike existing approaches, which primarily focus on detection, the proposed framework integrates adaptive self-healing mechanisms and blockchain-based tamper-proof logging within a hierarchical network structure.	This is a review-based study with no unified framework or implementation. It lacks integration of AI with resilience, blockchain, and adaptive recovery. The proposed work provides a complete architecture combining AI, blockchain, and bio-inspired defense.
[11]	Goundar and Gondal (2025) proposed a real-time cybersecurity framework integrating a CNN-based anomaly detection model with a permissioned blockchain to ensure tamper-proof logging and auditability of AI-generated alerts. The system achieved high detection accuracy (93.4%) and demonstrated effective real-time logging capabilities. However, the proposed approach introduces performance overhead and lacks privacy-preserving mechanisms such as encryption or zero-knowledge proofs. In contrast, the proposed work aims to address these limitations by improving scalability and incorporating enhanced security and privacy features.	Focuses on detection and logging but lacks hierarchical network modeling and self-healing capabilities. The proposed work improves scalability and resilience by incorporating hierarchical defense and adaptive node recovery mechanisms.

TABLE I (continued)

References	Summary	Limitations & Contribution of Proposed Work
[12]	Kumar (2026) proposed an AI-driven network security architecture for edge computing environments, emphasizing distributed intelligence and hierarchical processing for real-time threat detection. The framework integrates lightweight machine learning models at the edge with centralized analysis at the core, enabling scalable and adaptive cybersecurity. Additionally, techniques such as federated learning, API-driven automation, and zero-trust architecture enhance system flexibility and resilience. However, the approach introduces complexity and faces limitations related to resource constraints and coordination across distributed environments. In contrast, the proposed work incorporates bio-inspired self-healing mechanisms and blockchain-based tamper-proof logging to address these challenges.	Unlike Kumar (2026), which focuses on AI-driven hierarchical security for edge computing, the proposed work extends this by incorporating bio-inspired self-healing mechanisms and blockchain-based tamper-proof logging for enhanced resilience and adaptability.
[13]	This paper proposes an AI-driven framework for adaptive security monitoring in cloud networks that enhances real-time threat detection, anomaly identification, and automated response using machine learning and big data analytics.	Unlike this work, which focuses on AI-based adaptive monitoring for cloud security, the proposed framework integrates hierarchical architecture with blockchain-based tamper-proof logging and self-healing mechanisms for enhanced system-wide resilience.
[14]	This paper highlights the transformative impact of integrating blockchain and artificial intelligence in network security, emphasizing their potential to enable highly reliable, intelligent, and tamper-proof systems for next-generation cyber defense.	Unlike this work, which provides a high-level overview of blockchain and AI in network security, the proposed paper presents a concrete framework with hierarchical architecture, AI-driven adaptive defense, and blockchain-based implementation with analysis.
[15]	The paper explores the combined use of artificial intelligence and blockchain in cybersecurity, showing how AI enables intelligent threat detection and blockchain ensures secure, tamper-proof data management, while emphasizing that current approaches are mostly theoretical and require further real-world implementation.	Unlike this review-based study that discusses the potential of AI and blockchain in cybersecurity at a conceptual level, the proposed work presents a concrete hierarchical framework with integrated AI-driven adaptive defense and blockchain-based implementation and analysis.
[16]	This paper presents a comprehensive survey of IoT security, highlighting key threats across hardware, software, and data layers, and explores the integration of emerging technologies such as machine learning and blockchain while emphasizing the need for lightweight, hardware-based security solutions for resource-constrained devices.	Unlike this survey-based study that reviews IoT security challenges and emerging technologies, the proposed work introduces a practical hierarchical security framework with integrated AI-driven mechanisms and performance evaluation.
[17]	This paper analyzes the applications of IoT and highlights major security and privacy threats across communication models, focusing on vulnerabilities in wireless sensor networks and RFID systems, while emphasizing fundamental security requirements such as confidentiality, integrity, authentication, and availability.	Unlike this study that focuses on analyzing IoT applications and classical security threats in WSN and RFID systems, the proposed work introduces a hierarchical AI-driven security framework with integrated modern technologies and performance evaluation.
[18]	Bitner (2026) proposed an asset-aware network monitoring approach for Industrial Control Systems (ICS), leveraging passive network analysis and predefined asset inventory baselines to detect anomalous behavior. Using the Zeek monitoring framework, the study demonstrated that unauthorized devices, services, and communication patterns can be effectively identified without requiring modifications to endpoint systems. While the approach is effective for anomaly detection, it does not incorporate adaptive or self-healing mechanisms, nor does it utilize AI or blockchain for intelligent decision-making and secure logging, which are addressed in the proposed framework.	Bitner (2026) proposed a passive asset-aware network monitoring approach using Zeek to detect anomalies based on deviations from predefined asset inventories. While the method effectively identifies unauthorized devices and services in ICS environments, it lacks intelligent decision-making and secure logging mechanisms. In contrast, the proposed work integrates AI-driven adaptive defense and blockchain-based tamper-proof logging for enhanced security and automation.
[19]	Ankrah (2026) demonstrates that micro-segmentation based on Zero Trust significantly reduces lateral movement by limiting allowed network flows and improving containment time. However, the approach relies on static policy enforcement and does not incorporate adaptive intelligence or secure logging. In contrast, the proposed work enhances security using AI-driven dynamic decision-making and blockchain-based tamper-proof logging.	The existing work focuses on rule-based micro-segmentation to restrict lateral movement using predefined policies. However, it lacks adaptability and relies on static configurations. The proposed system differs by incorporating AI-driven dynamic security decisions and blockchain-based secure logging, enabling automated and intelligent threat response.

III. PROPOSED FRAMEWORK

The proposed framework introduces an **immune-inspired security architecture** for network infrastructures, where each node functions analogously to a biological cell. The model is organized as a **three-layer binary tree**, in which the root node represents the server administrator, and child nodes represent progressively lower-privileged components of the system. This hierarchical structure ensures that security decisions propagate downward while critical control remains at the top level.

A. Node Structure and Privilege Layers

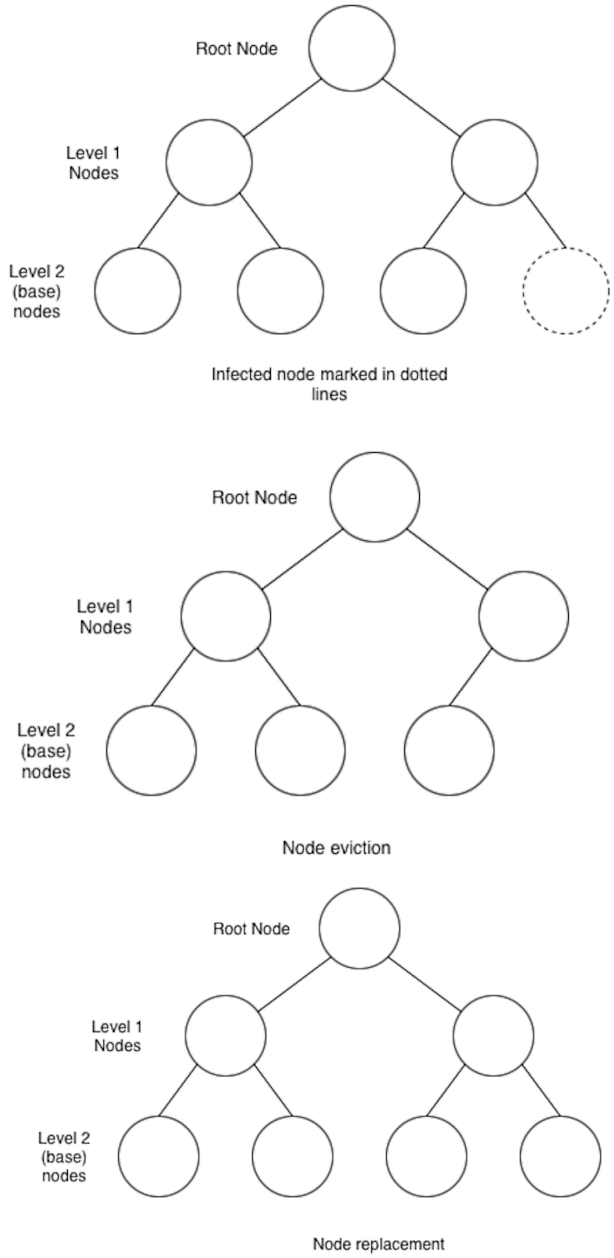

Fig. 1. Hierarchical network illustrating the proposed node eviction mechanism. (a) A compromised node is detected at the leaf level using the AI-based detection system. (b) The identified node is isolated and removed to prevent attack propagation. (c) The network is reconfigured, restoring connectivity and maintaining system integrity.

- The **root node (Layer 1)** corresponds to the administrator or central controller.
- **Intermediate nodes (Layer 2)** represent mid-level functions with moderate privileges.
- **Leaf nodes (Layer 3)** store user-level data and carry the highest risk of compromise due to their accessibility.

This binary tree structure (as shown in Fig. 1) supports redundancy and rapid isolation of compromised components, similar to the way biological immune systems compartmentalize threats.

Biological analogy of this network structure

1. Admin (The Brain) - central control, highest privilege, decision-making
2. **NICs - Nervous system** (channels that connect and transmit signals/data).
3. **Nodes - Cells** (individual units performing functions, some expendable, some replaceable).
4. Node replacement and AI patch - Immune cells and memory cells (learn from attacks, adapt, replace).

Note: The binary tree structure presented in this paper is used primarily for conceptual clarity, representing hierarchical control and privilege levels. However, the proposed immune-inspired security model is not limited to binary trees. It can be extended to other network topologies such as **star, mesh, ring, and hybrid architectures** [20], with necessary modifications to node replacement, AI-driven detection, and blockchain integration. This flexibility ensures that the model can be applied across diverse real-world infrastructures, from centralized systems to highly distributed networks.

B. Intrusion Response Mechanism

If an attacker compromises a **leaf node**, the following defense sequence is triggered:

1. **Reputation-Based Node Eviction** – This mechanism identifies and isolates "misbehaving" or compromised nodes based on their trust scores. Such strategies, widely applied in distributed systems (e.g., vehicular networks), ensure overall network health, stability, and integrity [3].
2. **Node Replacement** – The parent node detects anomalies and immediately removes the compromised child. A **copy node**, pre-synchronized with blockchain-backed data, is instantiated as a replacement. (Aggressive node replacement can cause data loss; we will use dynamic rekeying for this purpose)

3. **Immune Memory Formation** – The newly instantiated node integrates an AI-based patching system that records the intrusion method. If a similar attack occurs in the future, the system reacts more swiftly by preemptively isolating affected nodes [4].

C. Blockchain Integration

Blockchain enhances resilience by providing:

- **Immutable Logs:** All system logs are written to a blockchain ledger, preventing attackers from erasing traces of intrusion.
- **Data Integrity:** Node data is stored or periodically checkpointed on the blockchain, ensuring that replacements are restored to an untampered state.
- **Distributed Trust:** Instead of relying on a single administrator, consensus among multiple blockchain participants validates anomaly reports and recovery actions.
- **Smart Contracts for Automation:** Automated removal and replacement of compromised nodes can be triggered through predefined blockchain-based rules, reducing reaction time.
- **Immune Memory Registry:** Attack patterns are stored as signatures on the blockchain, enabling decentralized sharing of defense intelligence across the network.
- **Consensus Mechanisms for Trust:** Consensus algorithms (e.g., Proof of Work, Proof of Stake, or Byzantine Fault Tolerance) ensure that no single compromised entity can manipulate system logs or data [21], [22].
  Consensus Assumption:
  The proposed framework assumes a permissioned blockchain environment suitable for enterprise or organizational networks. Accordingly, a Practical Byzantine Fault Tolerance (PBFT)–style consensus mechanism is adopted due to its low latency, energy efficiency, and strong consistency guarantees in networks with a bounded number of known participants.
- Attack Resistance: Even if a hacker compromises a node, the attacker cannot alter blockchain records without controlling the majority of the network.

  Distributed Verification: Multiple nodes validate any transaction (e.g., log entry, node replacement event), ensuring authenticity before acceptance.

  Resilience: This consensus-driven validation acts like a "collective immune response, where all healthy nodes confirm anomalies before a countermeasure is executed.

Similar to immune responses, if a node is attacked, it is isolated and replaced by a new node equipped with an AI-based defense patch, resembling the adaptive memory of immune cells. Logs and critical data are stored on the blockchain, which acts as a **circulatory system of trust**, ensuring tamper-proof recording and resilient communication. Through consensus mechanisms, blockchain further provides a defense comparable to **collective biological decision-making**, where multiple cells verify abnormalities before triggering a defensive response [2].

D. Self-Healing and Adaptivity

Analogous to the human immune system, where infected cells are destroyed and regenerated to prevent the spread of infection, the network proactively detects, evicts, and replaces compromised nodes to ensure resilience and continuity.

The combined model ensures that compromised components are neutralized with minimal impact on system performance. The **immune analogy**—detection, memory, and self-healing—is reinforced through blockchain's tamper-proof memory and decentralized trust, creating a security framework that is proactive, adaptive, and resistant to evolving cyber threats.

In the current framework, AI-based patching is limited to lightweight anomaly pattern learning and signature correlation using previously observed attack traces, rather than autonomous code synthesis or unsupervised system modification.

IV. IMPLEMENTATION AND EXPECTED OUTCOME

The proposed immune-inspired security framework is analyzed with respect to **resilience, scalability, and reliability**. Unlike traditional static security mechanisms, this model leverages **Reputation-based Node Eviction, blockchain immutability, and AI-driven adaptive patching** to provide dynamic defense.

A. Theoretical Security Analysis

The probability of an intruder gaining control over the administrative node is reduced significantly through layered defenses. Let p denote the probability of compromising a single node, and
d the depth of the node from the root. Then, the probability of compromising the root (admin) is:

$$P_{admin} = p^d \quad (1)$$

For example, in a three-layer binary tree (d=3), if the compromise probability of a single node is
p = 0.2, the probability of directly reaching the admin node becomes only $P_{admin} = 0.2^3 = 0.008$. This demonstrates exponential security gain with layered privilege structures.

B. Security Enhancements and System Resilience

There are two methods discussed here:

1. Reputation-Based Node Eviction

Each participating node in the blockchain network is assigned a **dynamic reputation score** based on its behavior in consensus rounds and transaction validation. Nodes engaging in irregular activities, such as repeated failed verifications or anomaly patterns, suffer a decline in their scores. When a node's reputation falls below a threshold, it is **automatically excluded** from consensus participation. This prevents malicious nodes from gaining administrative privileges, while still allowing the system to adaptively re-validate them later if they recover [21].

Mathematically, the reputation score of a node *i* at time *t* can be written as:

$$R_i(t+1) = \alpha \cdot R_i(t) + \beta \cdot P_i(t) - \gamma \cdot M_i(t) \qquad (2)$$

Ri (t) = reputation of node *i* at time *t*,
Pi (t) = number of successful participations,
Mi (t) = number of malicious or failed actions,
α,β,γ = weight parameters controlling adaptation speed.

2. Dynamic Re-Keying

The proposed system employs a hybrid defense mechanism where compromised nodes are first isolated using dynamic re-keying and subsequently evicted and replaced if malicious behavior persists.

Dynamic re-keying can be triggered by:

1. **Threshold-based anomalies** (multiple failed verifications).
2. **Consensus alerts** (when majority flags suspicious behavior).
3. **Periodic proactive re-keying** (to reduce attack surface).

Together, these mechanisms ensure that the system doesn't just *cut off* nodes aggressively, but instead:

- **Evicts them adaptively** (via reputation).
- **Revokes their keys gracefully** (via re-keying).
- **Maintains continuity** of the system with minimal disruption.

C. Computational Overhead

While encryption, blockchain consensus, and AI patching add **computational costs**, these can be optimized through lightweight consensus (e.g., Proof-of-Authority, Practical Byzantine Fault Tolerance) and selective data mirroring [22]. Thus, the model remains scalable for large-scale networks.

D. Comparative Advantage

Compared to **traditional Intrusion Detection Systems (IDS)** and **firewalls**, the model introduces:

- **Self-healing behavior**, replacing compromised nodes dynamically.
- **Immutable audit trails** via blockchain.
- **Adaptive learning** through AI patches.

This combination results in a more **biologically inspired, adaptive, and tamper-resistant framework**.

E. Implementation Using Simulation

A simulation-based framework was developed in Python to evaluate the proposed cybersecurity model. The system consists of modules for traffic generation, anomaly detection, response handling, and blockchain-based logging. Synthetic network traffic was generated to simulate both normal and malicious activities under varying load conditions.

The anomaly detection module is implemented using a lightweight supervised learning model (Random Forest), trained on synthetic traffic patterns to classify normal and malicious behavior.

The blockchain component is simulated using a lightweight model to emulate consensus and immutability properties without incurring full deployment overhead.

The system was evaluated using multiple performance metrics including accuracy, throughput, and response time. The results are as follows:

1. Detection Accuracy

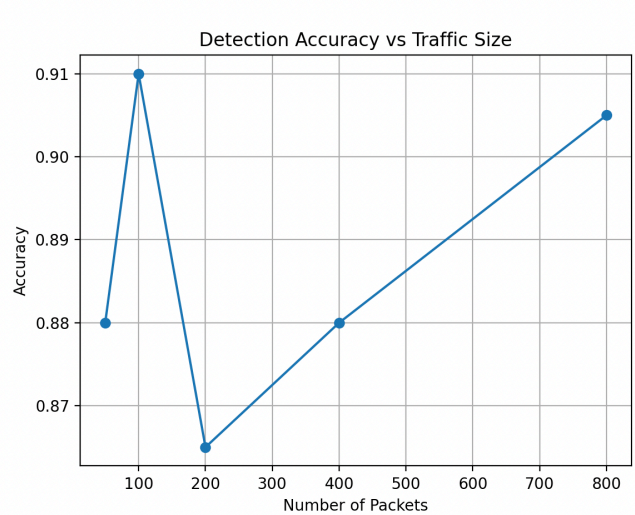

Fig. 2. Detection Accuracy vs Traffic

Fig. 2 illustrates the variation in detection accuracy with respect to increasing traffic size. The results indicate that the system maintains a high level of accuracy across different traffic loads, with minor fluctuations due to stochastic variations in the simulation environment. The overall trend suggests improved detection performance at higher traffic volumes, attributed to better pattern recognition with larger datasets.

2. Throughput Analysis

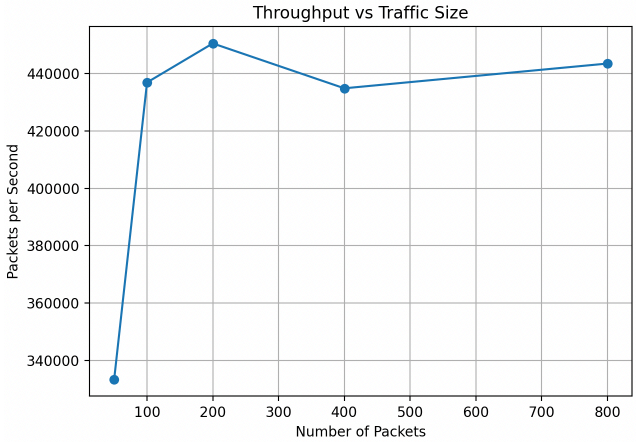

Fig. 3. Throughput vs Traffic Size

As shown in Fig. 3, the throughput of the system increases significantly as the traffic size grows from low to moderate levels, indicating improved utilization of computational resources. At higher traffic volumes, the throughput stabilizes with minor fluctuations, demonstrating that the system maintains consistent performance under increased load. The slight variations observed are attributed to stochastic behavior in the simulation environment and intermediate processing overhead.

3. Response Time Analysis

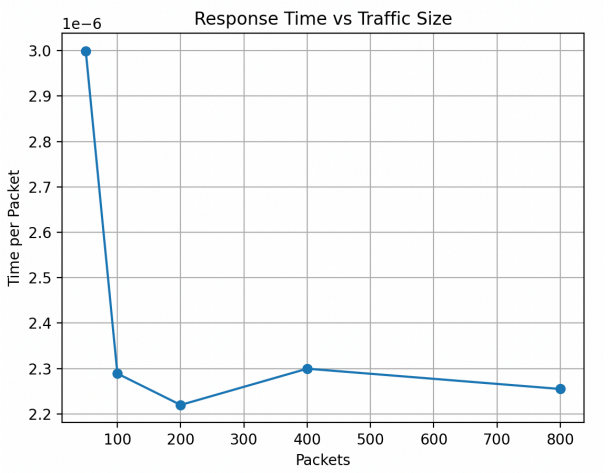

Fig. 4. Response Time vs Traffic Size

As shown in Fig. 4, the response time per packet decreases significantly as traffic increases from low to moderate levels, which can be attributed to improved resource utilization and system warm-up effects. At higher traffic volumes, the response time stabilizes with minor fluctuations, indicating that the proposed system maintains consistent latency under sustained load. The observed variations are due to stochastic behavior in the simulated environment and processing overhead during intermediate loads.

The experimental results validate the effectiveness and scalability of the proposed cybersecurity framework under varying traffic conditions. The system maintains high detection accuracy while demonstrating stable throughput and low response time, indicating efficient resource utilization and minimal performance degradation at higher loads. The integration of intelligent detection mechanisms with secure logging ensures both operational efficiency and data integrity.

These findings highlight the potential of the proposed approach as a robust solution for modern cybersecurity challenges, particularly in environments characterized by high traffic and evolving threat patterns.

V. EVALUATION AND DISCUSSION

A. Security Analysis
The proposed model integrates blockchain logging, AI-driven patching, and self-healing mechanisms into a cohesive defense framework. Each component strengthens the other: blockchain ensures immutability of logs, AI enables proactive defense, and self-healing techniques guarantee system continuity even under attack. This layered integration reduces the probability of a successful compromise.

B. Node Removal Mechanism (WBC Analogy)
Inspired by the human immune system, the model incorporates a **reputation-based node eviction** system. Malicious or rogue nodes, once identified, are flagged by the network and systematically isolated, similar to how **white blood cells neutralize harmful intruders and also destroy the infected cells**. This prevents the spread of compromise across the topology.

C. Memory-Driven Defense (Immunological Memory)
Beyond immediate response, the system retains historical attack patterns as **security memory cells**. This ensures that once an intrusion strategy is recognized and neutralized, the model adapts to detect and block the same or similar attempts in the future. Such memory-based resilience significantly enhances the long-term robustness of the network.

D. Probability of Attack Success
The probability of an adversary successfully taking control depends on their ability to compromise a majority of nodes in consensus. If p is the probability of compromising a single node, the probability of reaching administrative control is:

$$P_{attack} = \sum_{k=\left\lceil \frac{n}{2} \right\rceil}^{n} \binom{n}{k} p^k (1-p)^{n-k} \quad (3)$$

Where,
n: Total number of nodes in the network.
p: Probability of successfully compromising (hacking, bribing, or taking control of) **a single node**.
k: Number of compromised nodes.

For sufficiently large n and low p, this probability approaches zero, demonstrating the resilience of the model [23].

E. Performance Considerations
While blockchain and AI add computational overhead, lightweight consensus and pruning mechanisms can minimize resource usage. Additionally, the immunological memory avoids redundant computation by recalling previously patched threats.

F. Limitations and Future Work
The model introduces storage and latency challenges, particularly in large-scale environments. Future extensions may include hybrid blockchain approaches, optimized AI models for real-time detection, and distributed training for reduced overhead.

VI. CASE STUDY AND PSEUDO-CODE

A. Case Study: Privilege Escalation Attack on a Leaf Node

To demonstrate the practical applicability of the proposed framework, this section presents a representative case study involving a **privilege escalation attack on a low-privilege (leaf) node** within the hierarchical network.

Threat Model and Assumptions:

- External attacker
- Compromised leaf nodes
- Honest-majority / PBFT assumption
- Root admin not directly compromised

1) Attack Scenario and Threat Model

We consider an external adversary who gains initial access to a **leaf node** through **credential reuse**, a common real-world attack vector in enterprise networks. The compromised credentials allow the attacker to authenticate as a legitimate low-privilege user. Subsequently, the adversary attempts **lateral movement** by exploiting misconfigurations and shared authentication tokens to escalate privileges toward higher-level nodes.

The attacker's objective is to progressively traverse the hierarchy and gain control over intermediate nodes, ultimately targeting the administrative root node. Direct compromise of the root node is assumed to be infeasible without first breaching multiple lower layers.

2) Detection and Logging

Once abnormal behavior is detected—such as unusual access patterns, repeated failed privilege elevation attempts, or deviation from historical behavior profiles—the parent node flags the leaf node as suspicious. Detection signals include:

- Abnormal authentication frequency
- Unauthorized access requests to sibling or parent nodes
- Anomalous network traffic patterns

The following logs are generated in real time:

- Node identifier and privilege level
- Timestamped authentication attempts
- Detected anomaly type
- Reputation score changes
- Triggered defense actions (eviction, re-keying)

These logs are immediately **written to the blockchain ledger**, ensuring immutability and preventing the attacker from erasing forensic evidence.

3) Reputation-Based Eviction and Dynamic Re-Keying

Upon confirmation of malicious behavior through consensus among participating nodes, the system initiates **Reputation-Based Node Eviction**. The compromised leaf node's reputation score falls below the predefined threshold, triggering automatic isolation from the network.

Rather than aggressively purging the node and risking data loss, the framework simultaneously performs **dynamic cryptographic re-keying**:

- New session keys are distributed to all authenticated, non-compromised nodes.
- The compromised node, lacking updated cryptographic material, is cryptographically locked out.
- Active attacker sessions are terminated without disrupting normal network operations.

This dual mechanism ensures rapid containment while preserving system continuity.

4) Node Replacement and Blockchain State Restoration

Following eviction, the compromised leaf node is removed and replaced by a **copy node** instantiated from a clean, blockchain-backed state. Because critical node data and configuration checkpoints are periodically stored on the blockchain, the replacement node is restored to a **known trusted state**, free from attacker modifications.

The blockchain records:

- The eviction event
- Cryptographic key rotation metadata
- Hashes of restored node state
- Validation signatures from consensus participants

This guarantees transparency, auditability, and tamper resistance throughout the recovery process.

5) Immune Memory Formation and Accelerated Future Response

The attack characteristics—such as credential misuse patterns, access sequences, and behavioral anomalies—are abstracted into **attack signatures** and stored as part of the system's **immune memory registry** on the blockchain.

The AI-based patching mechanism integrates these signatures into future monitoring logic. When a similar privilege escalation attempt occurs:

- Detection thresholds are lowered for matching patterns
- Response latency is reduced
- Preemptive isolation is triggered earlier in the attack chain

This mimics **immunological memory**, enabling the system to respond faster and more effectively to recurring threats.

6) Outcome and Security Implications

Through this case study, the proposed framework demonstrates its ability to:

- Contain privilege escalation attempts at the lowest hierarchy level
- Preserve forensic evidence through immutable logging
- Recover automatically via self-healing node replacement
- Adapt over time using memory-driven defense mechanisms

This illustrates the framework's suitability for **real-world cybersecurity deployments** and highlights its value on **adaptive, autonomous, and resilient security architectures**.

B. Pseudo-code

Algorithm 1. Leaf Node Intrusion Response

```
Input: Node n, behavior log L

if anomaly_detected(L) then
    decrease reputation(n)
    trigger consensus validation
    rekey network sessions
    if reputation < threshold then
        evict node
        restore from blockchain
    end if
    store attack signature
end if
```

VII. CONCLUSION

This paper presented a novel immune-inspired cybersecurity framework that integrates blockchain technology, consensus mechanisms, and adaptive defense strategies to protect critical infrastructures against advanced cyber threats. By modeling the network as a hierarchical system, incorporating reputation-based node eviction, dynamic re-keying, and memory-cell–like mechanisms, the model demonstrates resilience against both external and insider attacks.

The use of blockchain ensures immutable logging, trustless consensus, and tamper-proof verification of network activities, while the biological analogy provides an adaptive and self-healing perspective on defense. Furthermore, the framework is not restricted to a single topology; it can be generalized across diverse network structures to achieve scalable and decentralized protection.

Future work will involve simulation and performance benchmarking of the proposed system under large-scale attack scenarios, as well as exploring AI-driven enhancements to improve intrusion detection and automate response mechanisms. This research aims to contribute toward building next-generation cybersecurity infrastructures that are both proactive and sustainable.

ACKNOWLEDGMENT

The author would like to thank the **International Institute of Information Technology Bhubaneswar** for providing academic resources and a supportive research environment that enabled this work. Sincere gratitude is extended to mentors and peers for valuable discussions and feedback during the development of this research.

The author also acknowledges the use of **ChatGPT (OpenAI)** as a professional writing and editing assistant to improve the clarity, structure, and language quality of the manuscript. All technical ideas, analysis, and conclusions presented in this paper are solely those of the author.

Finally, the author expresses heartfelt appreciation to family and friends for their continuous encouragement and support throughout the research process.

REFERENCES

[1] R. J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed. Wiley, 2020.

[2] K. Murphy and C. Weaver, *Janeway's Immunobiology*, 9th ed. New York, NY, USA: Garland Science, 2017.

[3] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," IEEE J. Sel. Areas Commun., vol. 25, no. 8, pp. 1557–1568, Oct. 2007.

[4] J. Keller and J. Nowakowski, "AI-powered patching: The future of automated vulnerability fixes," Google Security Engineering, Tech. Rep., 2024.

[5] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[6] S. H. Abbas, W. A. K. Naser, and A. A. Kadhim, "Subject review: Intrusion detection system (IDS) and intrusion prevention system (IPS)," Global J. Eng. Technol. Adv., vol. 14, no. 2, pp. 155–158, Feb. 2023.

[7] S. N. Mthunzi, E. Benkhelifa, T. Bosakowski, and S. Hariri, "A bio-inspired approach to cyber security," in Computer and Cyber Security: Principles, Algorithm, Applications and Perspectives, Springer, 2021.

[8] H. Taherdoost, "Smart contracts in blockchain technology: A critical review," Information, vol. 14, no. 2, p. 117, Feb. 2023.

[9] S. Islam, M. J. Islam, M. Hossain, S. Noor, K.-S. Kwak, and S. M. R. Islam, "A survey on consensus algorithms in blockchain-based applications: Architecture, taxonomy, and operational issues," IEEE Access, vol. 11, Apr. 2023, doi: 10.1109/ACCESS.2023.3267047.

[10] O. El Gharbaoui, I. Kiyadi, and H. El Boukhari, "Evaluating AI and ML in network security: A comprehensive literature review," Procedia Computer Science, vol. 251, pp. 727–733, 2024, doi: 10.1016/j.procs.2024.11.176.

[11] S. Goundar and I. Gondal, "AI-blockchain integration for real-time cybersecurity: System design and evaluation," J. Cybersecur. Priv., vol. 5, p. 59, 2025, doi: 10.3390/jcp5030059.

[12] N. Kumar, "AI-driven network security architecture for edge computing," Int. J. Comput. Exp. Sci. Eng., vol. 12, no. 1, pp. 1205–1210, 2026, doi: 10.22399/ijcesen.4994.

[13] S. Akhtar and S. A. Alharbi, "Artificial intelligence for adaptive security monitoring in cloud networks," Mar. 2026. [Online]. Available: https://www.researchgate.net/publication/401701503_Artificial_Intelligence_for_Adaptive_Security_Monitoring_in_Cloud_Networks

[14] D. M. F. Mattos, F. Krief, and S. J. Rueda, "Blockchain and artificial intelligence for network security," Annals of Telecommunications, vol. 75, pp. 101–102, Jan. 2020, doi: 10.1007/s12243-020-00754-7.

[15] S. Mohamed, N. M., T. N., E. D. J., and S. Hermansyah, "AI and blockchain in cybersecurity: A sustainable approach to protecting digital assets," Int. J. Multidiscip. Approach Res. Sci., vol. 3, no. 2, pp. 683–692, May 2025, doi: 10.59653/ijmars.v3i02.1584.

[16] P. Williams, I. K. Dutta, H. Daoud, and M. Bayoumi, "A survey on security in internet of things with a focus on the impact of emerging technologies," Internet of Things, vol. 19, p. 100564, Jul. 2022.

[17] M. Husamuddin and M. Qayyum, "Internet of things: A study on security and privacy threats," in Proc. Int. Conf. Adv. Comput. Commun. (ICACC), 2017.

[18] B. Bitner, "Asset-aware network monitoring," SANS Institute, Jan. 30, 2026.

[19] D. Ankrah, “Implementing micro-segmentation in a legacy enterprise lab network: A zero trust approach to reducing lateral movement, improving containment, and controlling operational overhead,” SANS Institute, Jan. 30, 2026.

[20] A. S. Tanenbaum and D. J. Wetherall, Computer Networks, 5th ed. Upper Saddle River, NJ, USA: Prentice Hall, 20.

[21] A. Sharma and R. Kumar, “Proof-of-reputation: An alternative consensus mechanism for blockchain systems,” Int. J. Netw. Secur. Appl., vol. 13, no. 4, pp. 45–56, Jul. 2021.

[22] M. Castro and B. Liskov, “Practical Byzantine fault tolerance,” in Proc. 3rd Symp. Operating Systems Design and Implementation (OSDI), New Orleans, LA, USA, 1999, pp. 173–186.

[23] J. A. Rice, Mathematical Statistics and Data Analysis, 3rd ed. Belmont, CA, USA: Duxbury Press, 2006.