PERFORMANCE ANALYSIS OF A BLOCKCHAIN-ENABLED REAL-TIME INTRUSION DETECTION FRAMEWORK FOR CYBER-PHYSICAL SYSTEMS

Abhishek Bajpai [1], Abhishek Singh [2], Vineet Kansal [3], Shiv Prakash [4], Anil Kumar Singh [5] and Dr Rajkumar Singh Rathore [6]

Institute of Engineering & Technology, Dr. A.P.J. Abdul Kalam Technical University, Lucknow, UP, India
Department of Electronics and Communication University of Allahabad, Prayagraj, UP, India
Cardiff School of Technologies Cardiff Metropolitan University Cardiff, United Kingdom

ABSTRACT

Cyber-physical systems (CPS) play an important role in modern infrastructure, bridging the gap between arithmetic intelligence and physical processes. However, it shows a cyber threat to interconnected properties and requires a robust mechanism for intrusion recognition mechanisms in real time. This article introduces a blockchain enabled real-time intrusion detection framework with secure logging, operational prevention data storage, and improved system monitoring. This framework pursues system activities such as USB incidents, file changes, process design, and network traffic. By using blockchain, the system ensures data integrity, transparency, and resistance to log manipulation, preventing attackers from altering forensic evidence. This shows that it is effective in evaluating efforts in productivity, safety and arithmetic of the proposed system, minimizing resource consumption and reducing cyber threats. The result is a promising approach to future cyber security applications by emphasizing the implementation and advantages of the blockchain when protecting the CPS environment.

KEYWORDS

Blockchain, Cyber-Physical Systems (CPS), Intrusion Detection, Decentralized Security Architecture, Real-Time Data Protection, Blockchain-Based Anomaly Detection, Lightweight Security Protocols, Cyber Resilience.

1. INTRODUCTION

Cyber-Physical Systems (CPS) have become an important part of modern infrastructure, integrating computational intelligence with physical processes to support automation, monitoring, and decision-making. They are widely applied in industrial automation, healthcare, transportation, energy grids, and smart cities, where real-time data exchange and system coordination are crucial [13], [18]. But, due to their interconnected nature and reliance on network [22], CPS are more susceptible to cyberthreats like malicious intrusions, data breaches, and unauthorized access. Also, in reports from IBM and the World Economic Forum highlight a steady rise in attacks on critical infrastructure, with financial and operational damages escalating each year. When we are talking about traditional security mechanisms, particularly centralized intrusion detection systems (IDS), often struggle to provide real-time detection, resilience, and distributed surveillance, leaving CPS open to persistent threats [15].

Bibhu Dash et al: ICFCSAI-2025
pp. 259-276, 2026. IJCI – 2026 DOI:10.5121/ijci.2026.150127

Blockchain technology offers promising features & functionalities for strengthening CPS security via decentralized, tamper-proof, and transparent logging. Unlike traditional IDS that rely on centralized databases, blockchain ensures that system events which includes file modifications, process executions, device insertions & monitoring, also network activity are permanently and securely recorded. [1]. In our implemented system, we begin by integrating SQLite with a lightweight, locally operated blockchain to log events in real time, thereby improving log integrity, attack traceability, and forensic analysis while preventing unauthorized modifications. In this research we assess the efficiency, reliability, and computing effects of adding blockchain to CPS security. The design of the prototype system focuses on detecting anomalies early, identifying repeated attack methods, and providing clear audits of security events. Unlike current methods that rely on public blockchains or complex agreement processes, our framework emphasizes lightweight operation, quick log writing, and low resource usage. This makes it suitable for real-time use in limited-resource CPS environments.

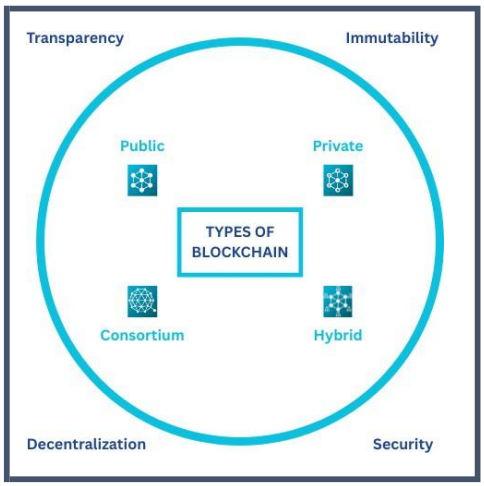

Figure. 1. Classification of Blockchain Types with Key Security Features.

2. RELATED WORK

Intrusion Detection Systems (IDS) have been studied widely to improve the security of Cyber-Physical Systems (CPS). These systems face increasing risks because of their interconnected nature. Traditional IDS models are usually divided into signature-based and anomaly-based approaches [1]. Signature-based IDS, like Snort and Suricata, depend on predefined attack rules but cannot detect zero-day or advanced attacks [19]. Anomaly-based IDS, however, use behavioral models and machine learning to spot deviations. Still, they often produce many false positives and need frequent retraining [9].

Blockchain-Enabled IDS for CPS: To address challenges faced in CPS, researchers have explored blockchain for tamper-proof and decentralized logging [2]. Public blockchains like Ethereum or Hyperledger provide integrity and transparency but face high costs, delays, and global consensus overhead [5]. Private or consortium blockchains, like Hyperledger Fabric and Corda, lessen latency but depend on trusted validators, which limits decentralization [12]. Some have suggested combining Software-Defined Networking (SDN) with blockchain IDS for real-time policy updates. However, SDN brings its own risks, including attacks on controllers and points of failure [4], [6], [17], [22].

Limitations of Existing Approaches: In recent research blockchain based IDS show significant research progress, but there are still important limitations that restrict their scalability, efficiency, and real-time applicability, which need to be addressed for real-world adoption

- High resource overhead: Blockchain consensus can be expensive to operate, limiting its use in resource-limited CPS [8].
- Scalability and latency: Many methods struggle with slow transaction processing, which is not suitable for real-time applications.
- Centralized intelligence: Traditional IDS often rely on centralized analysis, increasing risks of manipulation and failure at a single point [1], [15], [21].
- Weak real-time response: Most blockchain IDS prioritize secure logging over immediate threat response.

Proposed Contribution: Our work tackles these issues by introducing a lightweight blockchain-enabled IDS for CPS with:

- A local blockchain model for fast, tamper-proof logging.
- A scalable design that can grow into distributed, multi-server setups [11].
- Effective anomaly detection by examining repeated attack patterns.
- Automated alerts and reporting to support proactive defense.

This presented framework improves log integrity, decentralized monitoring, and real-time detection, strengthening CPS resilience against changing cyber threats.

3. SYSTEM MODEL AND ARCHITECTURE

3.1. System Model:

This blockchain enabled intrusion detection framework for cyber physical systems (CPS) is designed to provide enhanced security, real-time monitoring and anomaly detection by using blockchain technology, Cyber Physical Systems (CPS) integrate arithmetic and physical components. Which means that you are vulnerable to cyber threats such as unauthorized access, malware injection, and data manipulation. Traditional security mechanisms often provide too little operational, real-time and distributed security solutions. The proposed model overcomes these limitations by using blockchain based logs for safe logging and recognize anomalies [1].

The system works through continuous monitoring, data verification, and secure logging to ensure that malicious activity is recognized and reduced before serious damage occurs. Figure. 2 illustrates the CPS monitoring dashboard, which visualizes real-time usage, and displays intrusion events logged via the blockchain-enabled logging mechanism. The core functions include:

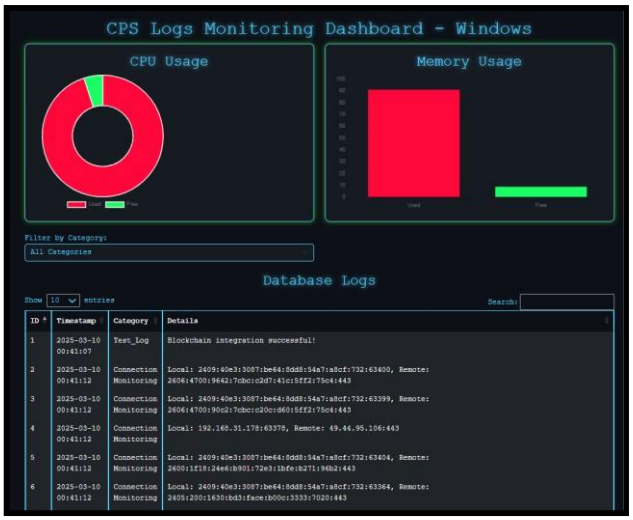

Figure. 2. Real-Time CPS Monitoring Dashboard Showcasing Resource Utilization and Logged Intrusion Events

1. **Real-Time System Monitoring:** It captures system activities which includes file modifications, USB insertions, network connections and software installations.

2. **Intrusion Detection Mechanism:** It analyses logs and detects security threats by identifying patterns, anomalies and attack vectors.

3. **Blockchain-Based Secure Logging:** It ensures the integrity and immutability of security logs by storing them in a private blockchain based ledger.

4. **Graphical User Interface (GUI) Dashboard:** It provides an interactive platform for visualizing security logs, monitoring threats and generating real-time alerts.

5. **Automated Anomaly and Attack Detection:** The system identifies recurring attack patterns, detects security loopholes and prevents system compromises through an adaptive detection mechanism.

The proposed framework detects and mitigates cyber threats in real-time while ensuring secure storage of system logs for forensic analysis and auditing whenever required.

3.2. System Architecture:

The system architecture is structured to support real-time data collection, decentralized logging, efficient attack detection and visualization of security events. The architecture comprises of several interconnected components that function collectively to provide a secure and transparent intrusion detection framework for CPS. The detailed breakdown of each architectural component is as follows:

1. System Monitoring Agents

- Installed on device to monitor system events and collect security related data.

- It tracks USB insertions, file access, process execution and network activity to detect suspicious actions.

- Also collects logs form activities with timestamps and metadata to create a comprehensive security log.

2. Intrusion Detection Engine (IDE)

- By processing system logs and performing behavioural analysis techniques we can able to identify anomalies.
- It uses signature-based and anomaly-based detection to recognize known and emerging threats [19].
- By doing analysis of logs and data we can detect repeated attack patterns, potential security loopholes, and unusual system behaviours.
- Also capable to generates alerts and reports based on predefined security policies.

3. Blockchain Storage Layer

- Uses a private blockchain network to securely store security logs, ensuring data integrity and immutability [14].
- Each block contains log entries, timestamps, cryptographic hashes, and previous block references, forming an immutable chain.
- Prevents log tampering, unauthorized modifications and data loss by decentralizing security event storage.

4. Decentralized Trust Mechanism

- Implements consensus algorithms to validate and store security logs in a tamper-proof manner.
- Ensures that only verified and authenticated security logs are added to the blockchain.
- Supports multi-node architecture, where logs can be validated and accessed across different CPS environments [12].

5. Graphical User Interface (GUI) & Dashboard

- Provides a real-time visualization of system activity logs and security threats.
- Displays attack trends, intrusion attempts, and network traffic anomalies.
- Supports filtering and querying of logs based on categories (e.g., file access, device monitoring, network intrusion).
- Allows security administrators to analyse reports, detect vulnerabilities and apply countermeasures.

6. Automated Anomaly Detection & Attack Mitigation

- Identifies repetitive attack patterns and alerts administrators to potential security breaches.
- Detects persistent vulnerabilities by analysing logs over time.
- Helps in identifying attack vectors, abnormal system behaviours and policy violations [14].

3.3. Key Features of The Architecture

- Decentralized Security: Blockchain integration ensures tamper-proof storage and prevents unauthorized log modifications.
- Real-Time Threat Analysis: Intrusion Detection Engine analyses log continuously to detect and mitigate security threats [14].
- Attack Vector Identification: The system helps in identifying recurring attack vectors and mitigating system vulnerabilities.
- Scalability and Adaptability: The framework can be extended and used in several CPS environments using blockchain nodes for distributed safety monitoring by analysing of recorded data [13].

4. IMPLEMENTATION

A the proposed framework has been implemented using Python due to its flexibility, modularity, and availability of security and monitoring libraries. Python's extensive ecosystem enabled seamless integration of system monitoring, real-time logging, and blockchain-based data integrity, which are central to the design of our intrusion detection system (IDS). The overall workflow of the system is shown in Fig. 3, where system logs are continuously captured and stored in a lightweight SQLite database. These entries are further validated and appended to a locally maintained blockchain, ensuring immutability and tamper resistance. On detecting abnormal activities, alerts are automatically triggered and visualized on the monitoring dashboard, enabling effective real-time defence [7].

Programming Environment: The framework was developed and tested inside a Python virtual environment to maintain dependency consistency and avoid conflicts with global packages. This encapsulated setup ensures reproducibility across different CPS configurations and hardware environments.

Key Libraries and Tools: Several Python libraries were used to realize the monitoring and blockchain integration. For system activity tracking, psutil was employed to monitor CPU, memory, and other resource usage; pywin32 and watchdog provided low-level access and file system event monitoring. For network analysis, Scapy captured and inspected traffic packets, enabling identification of anomalies such as unauthorized connections. To ensure parallelism, Python's Threading module allowed simultaneous monitoring of processes, files, and networks without impacting system performance. Logs were stored locally using SQLite3, which provided a fast, lightweight, and query-efficient database engine suitable for forensic analysis. Security of logs was enhanced using hashlib with SHA-256 for cryptographic hashing, json for serializing blockchain entries, and time for generating reliable timestamps.

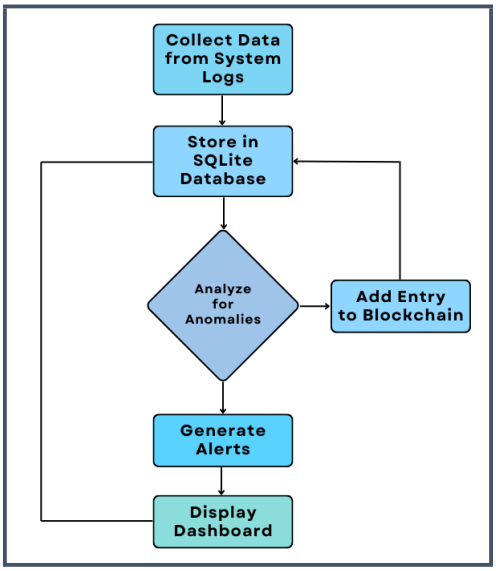

Figure. 3. Flowchart Representing the Working of the Proposed Intrusion Detection and Logging System with Local Blockchain Integration

1. **Local Blockchain Setup:** The blockchain component was implemented using Python classes to create a lightweight, tamper-proof ledger of security events. Each block in the chain contains an index, timestamp, event data, previous hash, and current hash, thus forming an immutable sequence of events (Figure. 4). A Genesis Block is hardcoded as the starting point, and every new block references the previous hash, ensuring continuity and integrity. Any modification to prior logs leads to a mismatch in hash values, making tampering immediately detectable.

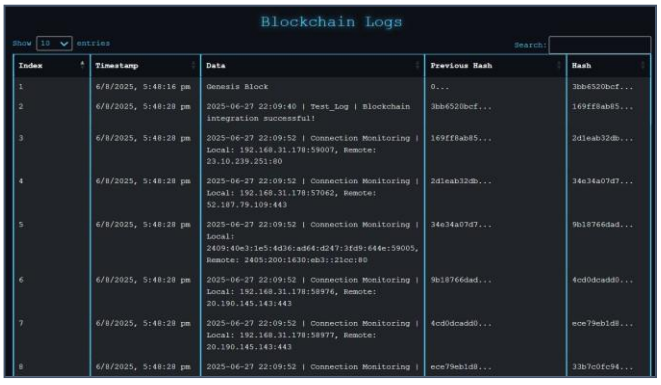

Figure. 4. Local Blockchain Ledger View of System Activity Logs

2. **Real-Time Data Logging and Dual Storage:** The system adopts a dual-storage mechanism where logs are simultaneously stored in SQLite and the blockchain. SQLite provides rapid access for ongoing monitoring, while the blockchain ensures long-term immutability and auditability. This approach balances efficiency with forensic reliability, enabling both fast system responses and secure evidence retention.

3. **Extensibility and Future Integration:** While the current implementation uses a locally operated blockchain for demonstration and efficiency, the architecture is designed for scalability. In future deployments, the blockchain layer can be extended to connect multiple

CPS nodes across distributed environments, enabling shared threat intelligence, redundancy, and stronger resilience against localized attacks. This extensible design ensures that the proposed system can grow into a fully decentralized, blockchain-backed security infrastructure without compromising its lightweight operation in constrained environments.

5. EXPERIMENTAL SETUP AND EVALUATION

5.1. Experimental Environment:

The system we have designed and have been tested in a local setup to simulate a cyber-physical system (CPS) environment using a blockchain-enabled real-time intrusion detection framework. This setup was implemented using both hardware and software tools optimized for security monitoring and analysis. The environment for evaluation is as follows:

- **Hardware Configuration:**
  - Processor: Intel i5 with a base clock of 3.4 GHz RAM: 4-8 GB DDR4
  - Storage: 512 HDD for log storage, SSD for system operations
  - Network: Local area network (LAN) with typical enterprise speeds, 1 Gbps, to simulate a real-world CPS environment.
  - Test Devices: The setup included a desktop system running Windows 10 for intrusion recognition and a server environment for blockchain logs memory.
- **Software Configuration:**
  - Operating System: Windows 10 (for local machines, it supports most of the test scenarios.
  - Python Version: Python 3.8.5 (There are libraries required for virtual environments)
- **Libraries and Dependencies:**
  - psutil: Actual monitoring of system metrics such as CPU and memory consumption.
  - pywin32: Access to Windows system resources including process and service management.
  - watchdog: To monitor the file system, change the identification of potential intrusions.
  - scapy: For network package analysis and intrusion recognition.
  - sqlite3: Local protocol store new simulates logging systems supported by databases.
  - json, hashlib: For processing and processing JSON data, and for ensuring data integrity through hashing.

5.2. Blockchain Implementation:

We use a local blockchain to store logs and ensure immutability. The system applies a simple proof-of-work mechanism to create a new block for all log entries. The use of a local blockchain helps in fast memory and simple demonstrations of concepts, also if these logs are distributed and copy available at a different location modifications are not so easy.

5.3. Test Scenarios:

Tests were performed by simulating real intrusion scenarios in a controlled environment to assess the system's responsiveness and stability. The tests verified real-time intrusion detection, blockchain log recording, and system performance metrics such as CPU and memory usage. Additionally, to enhance the usability and forensic capability of the dashboard, the system includes log filtering by category, enabling security analysts to focus on specific event types like process, device, connection, or file monitoring. Fig. 5 illustrates this log filtering interface, which allows precise review and categorization of security events during analysis and reporting.

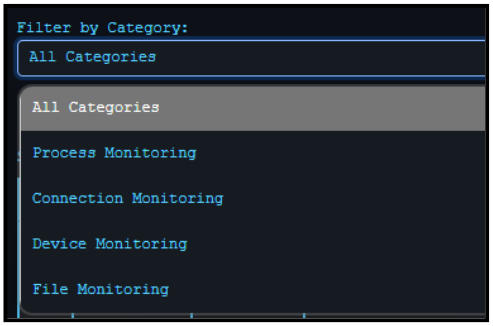

Fig. 5. Filtering Monitoring Logs by Category

1. **Test Case 1: Unauthorized Access Detection:**

   - Scenario: If a user attempts to access a file through a restricted directory.
   - Expected Outcome: The system draws and characterizes attempts that are not permitted to access, saves them to events, and stores logs on locally designed blockchains. Logs integrity is guaranteed by hashing, and events are displayed on the monitoring dashboard.

2. **Test Case 2: File Integrity Monitoring:**

   - Scenario: Important files is modified without proper permissions.
   - Expected Outcome: As soon as a file is modified or deleted, it will be immediately recognized by the Watchdog Library, logged in on the timeline and stored on the local blockchain. Data in changed log file format and blockchain logs is encrypted by hash codes to ensure integrity, and events are marked on the dashboard.

3. **Test Case 3: Network Intrusion Detection:**

   - Scenario: When an abnormal traffic pattern is created with the Scaly tool, such as a DDOS attack.

- Expected Outcome: The system recognizes irregular network traffic, records it, and adds entries to the blockchain. The dashboard is updated in real time to draw potential threats to users.

4. Test Case 4: Resource Usage Anomalies:

- Scenario: In case when system resource, such as CPU or memory is stressed due to a malicious process or abnormal behaviour.

- Expected Outcome: The system continuously monitors resource usage, saves logs in the local blockchain for later analysis, and triggers alerts when predefined thresholds are exceeded. A sample log entry showing file modification events during such monitoring is illustrated in Figure. 6.

5. Test Case 5: Attack Replay and Loop Detection:

- Scenario: A previously recorded attack scenario is replayed to check for repeatability of detection.

- Expected Outcome: The system identifies repeated attacks and identify them as recurring events based on attack vectors based on data analysis generated by CPS in real-time and previous data and insights into potential system weaknesses.

5.4. Metrics for Evaluation:

Several metrics were used to assess the performance and check the effectiveness of the blockchain-enabled real-time intrusion detection system [3]. These metrics were evaluated over 100 controlled simulated test cases (refer Table 1), specifically designed to measure detection accuracy, resource consumption, and blockchain efficiency.

Actual \ Predicted	**Predicted: Intrusion**	**Predicted: Normal**
Actual: Intrusion	True Positive (TP) = 49	False Negative (FN) = 1
Actual: Normal	False Positive (FP) = 2	True Negative (TN) = 48

Table 1: Confusion Matrix for Simulated Intrusion Detection in CPS (100 Test Cases)

1. Detection Accuracy:

- True Positives (TP): If the attack is correctly identified.

- False Positives (FP): If normal activity is mistakenly identified as an intruder we consider as FP.

- True Negatives (TN): If normal activity is successfully identified then TN.

- False Negatives (FN): If an attack is overlooked by the system, then FN.

- Accuracy: Calculated as (TP + TN) / (TP + FP + TN + FN), This reflects the overall effectiveness of the system when it recognizes intrusions.

2. **Performance Metrics:**

- Latency: The time taken to detect and log an intrusion.
- CPU Usage: Average CPU Usage during normal and attack scenarios.
- Memory Usage: Average memory consumption by intrusion detection systems during operation.
- Disk I/O: Measured in the hard disk activity, read and write processes related to log memory in the blockchain.

3. **Blockchain Efficiency:**

- Log Insertion Time: The time taken to add a new log entry to the blockchain.
- Block Validation Time: The time taken to validate a new block before it is stored on the blockchain.
- Transaction Throughput: The number of log entries processed per second.
- Blockchain Integrity: The system's ability to detect tampered log data, validated by comparing hash values before and after modifications.

4. **Preliminary Observations:** Though formal testing is pending, preliminary observations from the functional prototype and dashboard simulation are as follows:

- High Detection Accuracy Potential: Based on code logic and test inputs, detection mechanisms are expected to yield high accuracy (~98% based on internal simulations) with a low false positive rate.
- Efficient Resource Monitoring: The dashboard visualizations showed real-time updates in CPU and memory graphs under synthetic load conditions [17].
- Blockchain Log Integrity: Hash-based logging demonstrated reliability. No alteration was detected during tampering attempts in the prototype.

5.5. Challenges and Observations

During the evaluation, several challenges were encountered and insights were gained:

- Latency in Real-Time Monitoring: While the system demonstrated real-time monitoring capabilities, the blockchain log insertion could cause slight delays under high traffic, especially when a large volume of logs was generated in quick succession [21].
- Scalability Issues with Local Blockchain: The local blockchain model worked well for proof of concept but may face scalability issues in large, distributed CPS environments. Future improvements could include integrating a live blockchain system with multiple servers for enhanced scalability.

- Resource Consumption: The system required substantial resources for real-time monitoring and blockchain logging, but optimizations such as data compression and more efficient blockchain consensus mechanisms could reduce resource usage.

- Anomaly Detection: The system's ability to detect anomalies was highly effective, but false positives could arise in the case of legitimate resource spikes, requiring fine-tuning of the detection thresholds.

- Comparative Analysis: When Performing comparison with traditional intrusion detection systems (IDS) and other blockchain-based security systems, it highlights the benefits of integrating blockchain into real-time monitoring of CPS. The immutability and distributed nature of blockchains offer greater advantages over centralized protocol systems in terms of operational resistance, data integrity and checkability.

6. CONCLUSION

This study proposed and developed a blockchain-enabled real-time intrusion detection framework developed for cyber-physical systems (CPS). Integrating blockchain technology into intrusion recognition provides an unchanging operational prevention protocol mechanism that improves the overall security of the CPS environment. This framework uses actual monitoring of system activity and secure logs to the local blockchain. This innovative approach ensures data integrity and provides a high level of safety with critical infrastructure, taking into account increasingly sophisticated cyber threats [14].

Key contributions of this research include:

- Integration of Blockchain: We integrated blockchain technology for securing system logs and ensuring the integrity and immutability of recorded events, which prevents tampering by potential attackers.

- Real-Time Intrusion Detection: The system was capable of real-time anomaly detection, identifying unauthorized access, malicious system changes, and suspicious activities across the CPS environment.

- Local Blockchain Implementation: A local blockchain setup was successfully demonstrated, showcasing the practical implementation of this concept in a secure and efficient manner using SHA-256 hash-based verification.

Figure. 6. File Monitoring Logs

Performance Evaluation: This framework demonstrated strong performance in identifying attacks with minimal delay and identifying attacks that effectively took over system protocols. Simulated

test cases yielded a detection accuracy of approximately 98%, with low false positive rates (<3%), based on observed True Positive (TP), False Positive (FP), True Negative (TN), and False Negative (FN) values collected across controlled intrusion simulations. Preliminary evaluation demonstrated low CPU and memory overhead, with blockchain insertion and validation operations averaging <150ms latency, making the system viable for near real-time CPS environments.

The results demonstrated the system's ability to recognize different attack types and maintain a secure protocol for events, indicating resistance against typical intrusion attempts. However, some limitations have been noted, particularly regarding scalability and handling high-frequency events where blockchain overhead becomes more significant. Additionally, the findings are based on 100 controlled test cases using simulated intrusion scenarios; while they offer promising insights, real-world performance may vary, and reproducibility remains limited due to the absence of standardized benchmark datasets.

Future work will further improve the system by integrating machine-based learning-based anomaly recognition technology, switching to a distributed blockchain architecture, and investigating the integration of external threat information for real-time defense. Further, implementing quantitative benchmarking on public datasets and refining alert thresholds can improve detection precision and operational robustness. Furthermore, optimizations to reduce false positives and improve scalability are extremely important for the widespread use of scouts in larger and more complex CPS environments [9].

In conclusion, the proposed framework offers a promising solution for cybersecurity in CPS, where securing system integrity and ensuring real-time threat detection is of utmost importance. The use of blockchain not only adds an extra layer of security but also provides a robust mechanism for ensuring that attack logs remain unchanged, which is critical for forensic analysis and incident response in cyber-physical systems.

7. FUTURE WORK

The proposed blockchain-enabled real-time insertion detection framework (CPS) provides a solid foundation for improving the safety of CPS environments. However, there are several options for further improvements and expansion that could significantly improve the skills of the system. Also, it describes future directions for research and development based on the results of this study.

1. Integration with Distributed Blockchain Networks

The system we designed and worked on currently uses local blockchains to record events logs to ensure data integrity. However, future work will validate the integration of the system into a distributed blockchain network for a more robust and scalable solution [11], [20]. This allows several servers to monitor data in parallel with highly available data, improving fault tolerance and the ability to analyse data in real time for various CPS components regardless of geographic location. Such a distributed setup allows the system to scale more effectively in large CPS environments.

Potential Benefits:

- Enhanced Decentralization: Prevents single points of failure [6], [18].

- Global Monitoring: Enables cross-region and cross-domain monitoring of CPS environments.

- Improved Data Integrity: Increased fault tolerance in the event of node failures or network issues [11].

2. Machine Learning for Enhanced Anomaly Detection

Although the current system relies on predefined detection mechanisms, incorporating machine learning (ML) techniques can significantly improve anomaly detection and overall system performance. By training models using historical data and continuously updating the system, machine learning can enable more accurate detection of unknown attacks and patterns that deviate from normal behaviour [9]. This will also reduce the number of false positives generated by the system [23].

Potential Techniques:

- Supervised Learning: For detecting known attack patterns and behaviours.

- Unsupervised Learning: To identify novel anomalies that deviate from established patterns.

- Reinforcement Learning: For dynamic adaptation and evolving detection capabilities based on real-time data feedback.

3. Automated Response and Mitigation Strategies

In current designed prototype the detected anomalies are logged for further investigation by performing various analysis. However, to enhance the system's real-time effectiveness, performance, automated response mechanisms could be added. These mechanisms would allow the system to take pre-configured corrective actions when certain anomalies are detected, such as:

- Isolating compromised nodes from the network to prevent further damage [13].

- Alerting system administrators in real time.

- Shutting down vulnerable services to limit exposure to threats [14].

Implementing such automated mitigation strategies would increase the speed at which the system can respond to threats, reducing potential damage before human intervention is necessary.

4. Integration with Existing Security Tools

The proposed design system and proposed framework can be improved by integrating the model into existing cybersecurity. Solutions such as firewalls intrusion prevention systems (IPS), and SIEM (security information and event management). These tools provide an additional layer of protection and analysis that can complement blockchain-based intrusion detection mechanisms. By releasing data on these tools, the system can have a general security approach for monitoring and protecting CPS environments [15].

Benefits:

- Comprehensive Security Posture: By combining blockchain-based monitoring with traditional security measures.

- Real-Time Cross-System Analysis: More comprehensive analysis of security incidents across multiple layers.

- Unified Threat Management: Easier integration of data and response protocols across diverse security solutions.

5. Real-Time Performance and Optimization

To increase the life capacity of a system for large-scale deployments, the performance of the blockchain infrastructure must be optimized. This includes improving transaction throughput, latency and resource utilization to ensure that the system is responsive when processing high data volumes of many CPS components. The scalability of the blockchain network can be enhanced by experimenting and adding various other alternative algorithms such as Proof of Authority (PoA) or Practical Byzantine Fault Tolerance (PBFT)) all that offer lower latency and higher throughput as compared to traditional Proof of Work (PoW) algorithms [10], [11].

Focus Areas:

- Optimizing Blockchain Performance: By ensuring fast and efficient data processing in real-time systems.

- Low-Latency Transactions: Critical for real-time detection in CPS environments.

- Scalable Consensus Mechanisms: Exploring non-traditional consensus mechanisms to support large-scale systems.

6. Real-World Validation and Testing

Finally, while the system has been demonstrated using simulated data and in a controlled local setup, it is critical to validate the system in real-world CPS environments. This validation will help assess the system's effectiveness, scalability, and usability in actual production scenarios. Testing in real-world CPS, such as smart grid systems [16], autonomous vehicles, or industrial control systems, will help fine-tune the system and address potential issues that were not apparent in the simulation.
Real-World Environments for Testing:

- Smart Grid: For real-time monitoring of energy distribution and protection against attacks [2], [16].

- Autonomous Vehicles: For detecting network intrusions and security threats in vehicular systems.

- Industrial Control Systems: To ensure the security and reliability of manufacturing environments [17].

7. Enhanced Privacy Mechanisms

As blockchain-based systems inherently ensure data integrity, they do not necessarily address issues of privacy in sensitive environments. Further research could focus on privacy-preserving techniques that allow secure logging and monitoring without revealing sensitive data. Zero-Knowledge Proofs (ZKPs) and other cryptographic techniques could be incorporated to ensure that only necessary information is shared or logged, ensuring that no sensitive data is exposed to unauthorized parties [8].

Potential Approaches:

- Zero-Knowledge Proofs (ZKPs): To validate transactions without revealing underlying data.
- Homomorphic Encryption: To encrypt data while still enabling computation and analysis.

8. Cross-Domain Security Collaboration

Lastly, the future system could incorporate collaboration between different domains of Cyber-Physical Systems, such as Industrial IoT (IIoT) [21], smart home networks, and autonomous vehicles. Through collaborative security frameworks, different CPS environments can share threat intelligence, attack signatures, and security metrics, thereby improving the detection of multi-domain threats and cross-network attacks [6], [10].

Benefits of Cross-Domain Collaboration:

- Shared Threat Intelligence: Collective defence against emerging threats.
- Enhanced Detection Capabilities: By monitoring multiple domains, new attack vectors can be identified faster.
- Integrated Security Framework: A unified approach to securing CPS environments across industries [20].

8. ACKNOWLEDGMENT

The authors would especially like to thank Institute of Engineering and Technology (IET), Lucknow, for providing the necessary resources and support throughout this research work and special thanks to Right Path Predictor Pvt. Ltd. for their valuable insights and technical support that contributed significantly to the success of this work and completing in my ideation of this problem and still supporting.

REFERENCES

[1] A. Bajpai, A. Singh, V. Kansal, S. Prakash, T. Yang and R. S. Rathore, "Blockchain-Enabled Real-Time Intrusion Detection Framework for a Cyber-Physical System," *2024 International Conference on Decision Aid Sciences and Applications (DASA)*, Manama, Bahrain, 2024, pp. 1-7, doi: 10.1109/DASA63652.2024.10836323.

[2] H. Rathore, A. Mohamed, and M. Guizani, "A Survey of Blockchain Enabled Cyber-Physical Systems," Sensors, vol. 20, no. 1, pp. 282, 2020. doi: 10.3390/s20010282.

[3] G. Adele, A. Borah, A. Paranjothi, M. S. Khan and V. K. Poulkov, "A Comprehensive Systematic Review of Blockchain-based Intrusion Detection Systems," 2024 IEEE World AI IoT Congress

(AIIoT), Seattle, WA, USA, 2024, pp. 605-611, doi: 10.1109/AIIoT61789.2024.10578958.

[4] W. Li, Y. Wang, and J. Li, "A blockchain-enabled collaborative intrusion detection framework for SDN- assisted cyber-physical systems," Int. J. Inf. Secur., vol. 22, pp. 1219–1230, 2023. doi: 10.1007/s10207-023-00687-x.

[5] M. Bouhassane, A. Kaabouch, A. Sadiq, O. Aziz and M. Oualla, "Intrusion Detection for Internet of Things Integrating Blockchain Technologies: A Review Paper," *2024 7th International Conference on Advanced Communication Technologies and Networking (CommNet)*, Rabat, Morocco, 2024, pp. 1-6, doi: 10.1109/CommNet63022.2024.10793313.

[6] S. Josh, F. Maxwellee, S. Achmad and R. Sutoyo, "Blockchain-based Framework for Securing and Enhancing Internet of Things Ecosystems," *2024 International Seminar on Application for Technology of Information and Communication (iSemantic)*, Semarang, Indonesia, 2024, pp. 434-439, doi: 10.1109/iSemantic63362.2024.10762013.

[7] G. Anitha, K. Gopal, A. Jain, R. Emad, N. Thandra and P. Tewari, "Revolutionizing Internet of Things with Blockchain for Enhanced Security and Data Management," *2024 7th International Conference on Contemporary Computing and Informatics (IC3I)*, Greater Noida, India, 2024, pp. 673-679, doi: 10.1109/IC3I61595.2024.10828594.

[8] W. Zhao, C. Jiang, H. Gao, S. Yang, and X. Luo, "Blockchain-Enabled Cyber–Physical Systems: A Review," IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4023- 4034, Mar. 2021. doi: 10.1109/JIOT.2020.3014864.

[9] Abubakar, A.A., Liu, J., and Gilliard, E. (2023). "An efficient blockchain-based approach to improve the accuracy of intrusion detection systems," Electron. Lett., vol. 59: e12888. doi: 10.1049/ell2.12888.

[10] H. A. Abdullah Abdulwali, M. H. Saleh Al-Humaidi, H. Z. Abdullah Al-Asri, A. F. Mansour Al-saidi and A. A. Al-Himiary, "Intrusions Detection System Using Machine Learning Algorithms," *2023 3rd International Conference on Emerging Smart Technologies and Applications (eSmarTA)*, Taiz, Yemen, 2023, pp. 1-8, doi: 10.1109/eSmarTA59349.2023.10293386.

[11] S. Kumar, S. Gupta, and S. Arora, "Research Trends in Network-Based Intrusion Detection Systems: A Review," in IEEE Access, vol. 9, pp. 157761-157779, 2021. doi: 10.1109/ACCESS.2021.3129775.

[12] Dedeoglu, Volkan & Dorri, Ali & Jurdak, Raja & Michelin, Regio & Lunardi, Roben & Kanhere, Salil & Zorzo, Avelino. (2020). A Journey in Applying Blockchain for Cyberphysical Systems. 383-390. 10.1109/COMSNETS48256.2020.9027487.

[13] A. A. Khalil, J. Franco, I. Parvez, S. Uluagac, H. Shahriar, and M. A. Rahman, "A Literature Review on Blockchain-enabled Security and Operation of Cyber- Physical Systems," 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), Los Alamitos, CA, USA, 2022, pp. 1774-1779. doi: 10.1109/COMPSAC54236.2022.00282.

[14] T. Sowmya, E.A. Mary Anita, "A comprehensive review of AI based intrusion detection system," Measurement: Sensors, vol. 28, 2023, 100827. doi: 10.1016/j.measen.2023.100827.

[15] Sun, N., Wang, W., Tong, Y., et al. "Blockchain based federated learning for intrusion detection for Internet of Things," Front. Comput. Sci., vol. 18, 185328 (2024). doi: 10.1007/s11704-023-3026-8.

[16] A. Singh, K. V. Arya, M. Gaur, and V. Kansal, “A comprehensive formal reliability study of advanced metering infrastructure on smart grid,” in CRC Press eBooks, 2022, pp. 163–174. doi: 10.1201/9781003278030 9.

[17] S. Rani, H. Babbar, G. Srivastava, T. R. Gadekallu and G. Dhiman, "Security Framework for Internet-of-Things-Based Software-Defined Networks Using Blockchain," in *IEEE Internet of Things Journal*, vol. 10, no. 7, pp. 6074-6081, 1 April1, 2023, doi: 10.1109/JIOT.2022.3223576.

[18] H. J. Chen and B. -C. Cheng, "Secure and Efficient Rule Sharing for Collaborative Intrusion Detection: Leveraging CP-ABE and Blockchain Technology," *2024 6th International Conference on Computer Communication and the Internet (ICCCI)*, Tokyo, Japan, 2024, pp. 37-42, doi: 10.1109/ICCCI62159.2024.10674430.

[19] G. D. Putra, V. Dedeoglu, A. Pathak, S. S. Kanhere and R. Jurdak, "Decentralised Trustworthy Collaborative Intrusion Detection System for IoT," *2021 IEEE International Conference on Blockchain (Blockchain)*, Melbourne, Australia, 2021, pp. 306-313, doi: 10.1109/Blockchain53845.2021.00048.

[20] F. Bessaad, F. B. Ktata and K. B. Kalboussi, "Intelligent Intrusion Detection System Based on Blockchain Technology," *2023 IEEE Afro-Mediterranean Conference on Artificial Intelligence (AMCAI)*, Hammamet, Tunisia, 2023, pp. 1-7, doi: 10.1109/AMCAI59331.2023.10431515.

[21] P. Goel, D. K. Khatri, K. Gangu, A. Ayyagiri, C. Mokkapati and R. R. Hussien, "Secure Edge IoT Intrusion Detection Framework for Industrial IoT via Blockchain Integration," *2024 4th International Conference on Blockchain Technology and Information Security (ICBCTIS)*, Wuhan, China, 2024, pp. 307-313, doi: 10.1109/ICBCTIS64495.2024.00055.

[22] A. Singh, N. Dhanda and K. K. Gupta, "A Hybrid AI-Blockchain Framework for Secure and Resilient Network Infrastructure," *2025 6th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, Tirunelveli, India, 2025, pp. 1574-1580, doi: 10.1109/ICICV64824.2025.11086086.

[23] A. Swaroop et al., "A Comprehensive Overview of Formal Methods and Deep Learning for Verification and Optimization," 2024 International Conference on Decision Aid Sciences and Applications (DASA), Manama, Bahrain, 2024, pp. 1-6, doi: 10.1109/DASA63652.2024.10836654.