www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 1116-1123

e-ISSN : 2583-1062
Impact Factor : 7.001

# THE ROLE OF AI, ML, AND BLOCKCHAIN IN THE EVOLUTION OF NETWORK INTRUSION DETECTION SYSTEMS

**Akkaladevi Nandini[1], Mr. G. S. Udaya Kiran Babu[2], Dr. D William Albert[3]**

[1]M. Tech Student, Dept. of CSE, Bheema Institute of Technology & Science, Adoni, A.P, India.
[2]Associate Professor, Dept. of CSE, Bheema Institute of Technology & Science, Adoni, A.P, India.
[3]Professor & Head, Dept. of CSE, Bheema Institute of Technology & Science, Adoni, A.P, India.

DOI: https://www.doi.org/10.58257/IJPREMS39764

## ABSTRACT

As cyber threats grow in scale and sophistication, traditional Network Intrusion Detection Systems (NIDS) often struggle to detect and respond to emerging and unknown attacks effectively. This paper examines the transformative role of Artificial Intelligence (AI), Machine Learning (ML), and Blockchain technologies in the evolution of NIDS. By integrating intelligent analysis, adaptive threat recognition, and decentralized trust mechanisms, these technologies collectively address the inherent limitations of conventional systems. The result is a new generation of NIDS that are more robust, responsive, and capable of securing modern digital infrastructures against dynamic and persistent threats.

**Keywords:** Network Intrusion Detection Systems (NIDS), Artificial Intelligence (AI), Machine Learning (ML), Blockchain, Cybersecurity, Data Integrity, Signature-Based, Secure Logging.

## 1. INTRODUCTION

In today's hyper-connected digital ecosystem, cyberattacks have become more frequent, sophisticated, and targeted, posing serious threats to organizational assets and critical infrastructure[1]. Traditional Network Intrusion Detection Systems (NIDS) largely depend on static rule sets and predefined signatures to identify malicious activity[2]. While effective against known threats, these systems often fail to detect zero-day attacks and advanced persistent threats (APTs), which continue to evolve in complexity and evasiveness.

To address these limitations, the integration of Artificial Intelligence (AI), Machine Learning (ML), and Blockchain technologies into NIDS has emerged as a promising direction. These innovations collectively enable the development of intelligent, adaptive, and tamper-proof intrusion detection mechanisms[3-4]. AI and ML empower systems with dynamic learning capabilities, allowing them to identify novel attack patterns and reduce false positives. Blockchain, on the other hand, introduces decentralized trust and immutable logging, enhancing system transparency and resilience.

This paper explores the individual and combined roles of AI, ML, and blockchain in transforming traditional NIDS into next-generation, intelligent security frameworks. It also provides a comprehensive overview of current implementations, challenges, and potential future directions for this evolving field.

## 2. TRADITIONAL NIDS: FOUNDATIONS AND LIMITATIONS

### 2.1 Types of Network Intrusion Detection Systems

Network Intrusion Detection Systems (NIDS) are traditionally categorized based on their detection methodologies[4-5]. The two primary types are:

- **Signature-Based Detection**: This method relies on a database of known attack signatures or patterns. When network traffic matches one of these predefined signatures, an alert is generated. While this technique is effective for detecting previously encountered threats, it is limited in its ability to recognize new or unknown attacks.
- **Anomaly-Based Detection**: This approach involves establishing a baseline of normal network behavior and identifying deviations from that norm. Any significant anomaly in the traffic pattern may indicate a potential intrusion. Although anomaly-based systems can detect zero-day attacks, they often suffer from high false positive rates due to the dynamic nature of network environments.

### 2.2 Key Limitations of Traditional NIDS

Despite their widespread use, traditional NIDS face several critical limitations:

- **Inability to Detect Novel Threats**: Signature-based systems are inherently reactive, failing to identify zero-day exploits or previously unseen attack vectors.
- **High False Positive/Negative Rates**: Anomaly detection systems can generate excessive false alarms, overwhelming security analysts and leading to alert fatigue, while also potentially missing subtle but genuine threats.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 1116-1123

e-ISSN : 2583-1062
Impact Factor : 7.001

- **Centralized Logging Prone to Tampering**: Most traditional NIDS rely on centralized logging mechanisms, which can become single points of failure and are susceptible to manipulation by attackers who gain access to the system.
- **Poor Adaptability in Dynamic Environments**: As network environments grow more complex and heterogeneous, static detection rules become increasingly inadequate, resulting in reduced effectiveness and slower response times.

These challenges underscore the need for more advanced and intelligent approaches to intrusion detection—prompting the integration of AI, ML, and blockchain technologies to enhance the effectiveness, scalability, and trustworthiness of NIDS.

## 3. ARTIFICIAL INTELLIGENCE IN NIDS

3.1 Role of Artificial Intelligence

Artificial Intelligence (AI) plays a pivotal role in modernizing Network Intrusion Detection Systems by introducing cognitive-like capabilities to analyze, interpret, and respond to cyber threats[6]. Unlike traditional rule-based systems, AI-powered NIDS can process vast amounts of network data in real time and adapt to evolving attack patterns.

Key contributions of AI include:

- **Enhanced Decision-Making**: AI simulates human-like reasoning, enabling systems to make context-aware decisions based on a variety of inputs and scenarios.
- **Real-Time Threat Assessment and Response**: AI algorithms can quickly detect anomalies or malicious behavior and trigger immediate responses, reducing the time between threat detection and mitigation.

3.2 Use Cases of AI in NIDS

The application of AI within NIDS has led to several innovative use cases that significantly improve detection accuracy and operational efficiency:

- **Intelligent Correlation of Alert Data**: AI systems can correlate data from multiple sources (e.g., logs, traffic flows, historical events) to identify patterns that may indicate a coordinated or multi-stage attack.
- **Threat Prioritization and Risk Assessment**: By evaluating the potential impact and likelihood of a detected threat, AI can assign risk scores and prioritize alerts, allowing security teams to focus on the most critical issues.
- **Self-Healing and Autonomous Response**: Through reinforcement learning, AI-enabled systems can learn from past responses and adapt their strategies, eventually leading to autonomous threat mitigation without human intervention.

These capabilities demonstrate how AI transforms NIDS from passive monitoring tools into proactive, intelligent defense mechanisms. When integrated with machine learning and blockchain technologies, AI becomes part of a larger ecosystem for advanced, resilient cybersecurity.

## 4. MACHINE LEARNING IN NIDS

Machine Learning (ML) has emerged as a key enabler in enhancing the performance and intelligence of Network Intrusion Detection Systems[7]. By leveraging data-driven models, ML allows NIDS to recognize complex patterns in network traffic, detect previously unseen threats, and improve detection accuracy over time without explicit reprogramming.

### 4.1 ML Techniques and Models

Various ML techniques have been adopted in NIDS to address different types of security threats. These can be broadly categorized as follows:

- **Supervised Learning**: Involves training models on labeled datasets. Common algorithms include:
  - Support Vector Machines (SVM) – Effective in binary classification tasks.
  - Random Forest – A robust ensemble method that improves accuracy and reduces overfitting.
  - Naïve Bayes – A probabilistic model known for its simplicity and speed.
- **Unsupervised Learning**: Used for detecting anomalies in unlabeled data. Common approaches include:
  - Clustering Algorithms (e.g., K-Means) – Group similar data points to identify outliers.
  - Autoencoders – Neural networks that learn efficient representations and can detect deviations from normal behavior.
- **Deep Learning**: Advanced neural network models capable of extracting complex features from raw data:

- Convolutional Neural Networks (CNNs) – Effective for identifying spatial patterns in traffic features.
- Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) – Well-suited for sequential data such as time-series network logs.

### 4.2 Contributions to NIDS

Machine learning introduces several key enhancements to traditional NIDS:

- **Real-Time Pattern Recognition**: ML models can analyze high-dimensional network traffic data in real time to detect malicious activity with improved speed and accuracy.
- **Adaptation to Evolving Threats**: Unlike static rule-based systems, ML models can be retrained on new data to adapt to emerging attack vectors, making them more resilient against zero-day threats.
- **Reduction of False Alarms**: Through improved classification and anomaly detection, ML helps reduce false positives and negatives, enabling more reliable alerts for security teams.

### 4.3 Challenges

Despite its advantages, integrating ML into NIDS presents several challenges:

- **Training Data Quality and Quantity**: ML models require large, diverse, and labeled datasets to perform effectively. However, obtaining such data—especially for rare or zero-day attacks—can be difficult.
- **Model Interpretability**: Complex models like deep neural networks often function as "black boxes," making it hard for security analysts to understand or justify their decisions.
- **Computational Overhead**: Training and deploying ML models, particularly deep learning architectures, can be resource-intensive and may not be feasible for all network environments, especially those with real-time or edge-based constraints.

These challenges highlight the need for careful model selection, ongoing data management, and optimization strategies to fully leverage ML in intrusion detection systems.

## 5. BLOCKCHAIN IN NIDS

Blockchain technology, widely known for its role in decentralized finance, has recently gained attention in the field of cybersecurity[19-10]. Its inherent features—immutability, decentralization, and transparency—make it particularly valuable for enhancing the trustworthiness and resilience of Network Intrusion Detection Systems (NIDS). When integrated with NIDS, blockchain provides a secure, distributed framework for recording and verifying intrusion-related data without the need for centralized control.

### 5.1 Core Advantages

- **Immutability**: Once data is recorded on the blockchain, it cannot be altered or deleted. This ensures that intrusion logs and alert records remain tamper-proof, enabling reliable forensic investigations and accountability.
- **Decentralization**: Blockchain operates on a peer-to-peer network, eliminating single points of failure. This decentralized nature increases system robustness, especially in distributed security environments or across enterprise networks.
- **Transparency**: All transactions on a blockchain are timestamped and verifiable by network participants, promoting transparency. This is especially useful for auditing intrusion events and validating alert histories in a trustworthy manner.

### 5.2 Applications in NIDS

- **Secure Logging of Intrusion Events**: Blockchain can serve as a distributed ledger for logging detected threats, ensuring that records cannot be erased or manipulated—even by insiders or attackers.
- **Sharing Threat Intelligence Across Distributed Networks**: Blockchain enables real-time and secure sharing of threat intelligence among different NIDS nodes or organizations, facilitating collaborative defense mechanisms.
- **Smart Contracts for Automated Response and Mitigation**: Predefined conditions coded into smart contracts can trigger automatic responses to detected threats, such as isolating infected nodes or alerting administrators—enhancing response speed and consistency.

### 5.3 Implementation Challenges

Despite its advantages, applying blockchain in NIDS also presents several technical and operational challenges:

- **Latency and Scalability**: Blockchain consensus mechanisms can introduce delays that are problematic for real-time intrusion detection. High-frequency transaction loads may also affect network throughput.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 1116-1123

e-ISSN : 2583-1062
Impact Factor : 7.001

- **Privacy and Regulatory Concerns**: Storing intrusion data on a public or even semi-public blockchain can raise concerns about user privacy, data exposure, and compliance with regulations like GDPR.
- **Integration with Traditional NIDS Architecture**: Incorporating blockchain into existing NIDS infrastructures may require significant architectural changes, resource investments, and specialized expertise.

While these challenges are non-trivial, ongoing research and the evolution of lightweight, permissioned blockchain platforms offer promising solutions for integrating blockchain into next-generation intrusion detection frameworks.

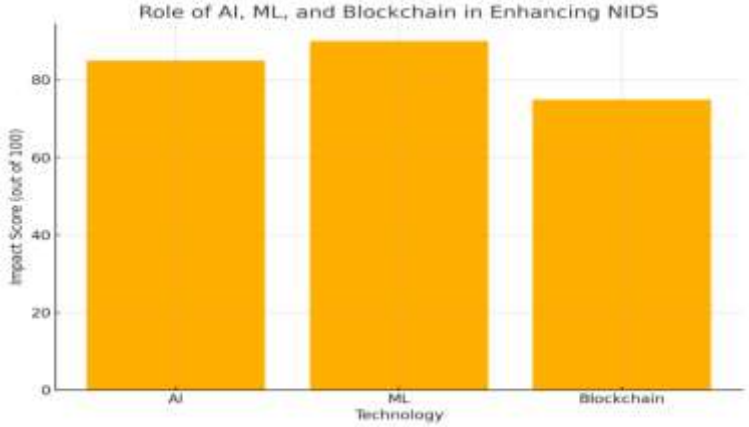


**Figure 1:** Impact Scores of AI, ML and Blockchain

Here is a figure 1 illustrating the **role of AI, ML, and Blockchain in enhancing Network Intrusion Detection Systems (NIDS)**. The impact scores are, representing each technology's contribution to improving detection accuracy, adaptability, and data integrity.

## 6. INTEGRATED SMART NIDS ARCHITECTURE

The integration of Artificial Intelligence (AI), Machine Learning (ML), and Blockchain within a unified Network Intrusion Detection System forms what is referred to as a **Smart NIDS**. This architecture is designed to deliver intelligent detection, adaptive learning, and tamper-proof logging in a seamless, end-to-end intrusion detection framework. Each component in this system plays a crucial role in transforming raw network traffic into actionable, trustworthy security intelligence.

**Key Components of the Architecture**

- **Traffic Monitor**: The traffic monitor is responsible for capturing packet-level network data from various sources, such as routers, switches, or endpoint devices. It collects real-time traffic flows and forwards them to the processing modules. Tools like Wireshark, Tcpdump, or custom packet sniffers are often employed at this layer.
- **Machine Learning (ML) Engine**: The ML engine serves as the core analytical module. It receives network traffic features, performs preprocessing (e.g., normalization, feature extraction), and applies trained models to classify traffic as either normal or potentially malicious. The ML engine may include multiple classifiers (e.g., Random Forest, CNN, LSTM) to enhance detection reliability across various attack types.
- **Blockchain Layer**: Once an intrusion is detected, the relevant alert information—such as time, source IP, destination, threat classification, and severity—is logged onto a blockchain ledger. This layer ensures that event records are immutable, traceable, and resistant to tampering. It may also include smart contracts that define automated rules for threat response and threat intelligence sharing.
- **AI Orchestrator**: Acting as the decision-making hub, the AI orchestrator coordinates system responses based on ML outputs and context-aware rules. It can prioritize alerts, initiate mitigation actions (e.g., traffic blocking, user notification), and refine system policies through reinforcement learning. The orchestrator also communicates with the blockchain layer to enforce logging and contractual responses.

**System Workflow Overview**

- Traffic Capture: Network packets are monitored in real time.
- Feature Extraction: Raw data is converted into structured inputs for analysis.
- ML-Based Classification: Traffic is classified as normal or suspicious.
- AI Decision Making: The AI orchestrator evaluates the context and defines appropriate responses.
- Immutable Logging: Alerts and actions are recorded on the blockchain for audit and future reference.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 1116-1123

e-ISSN : 2583-1062
Impact Factor : 7.001

## 7. REAL-WORLD APPLICATIONS AND CASE STUDIES

The integration of Artificial Intelligence, Machine Learning, and Blockchain into Network Intrusion Detection Systems has moved beyond theoretical exploration into practical implementations. Both academia and industry are actively developing and testing Smart NIDS frameworks, demonstrating their potential to enhance cybersecurity across various environments. This section highlights notable real-world applications and case studies that showcase the effectiveness of such integrations.

### 7.1 Academic Research: ML-Enhanced NIDS with CICIDS2017 Dataset

One of the most widely cited academic contributions in this domain involves the use of the Canadian Institute for Cybersecurity Intrusion Detection System 2017 (CICIDS2017**)** dataset to evaluate machine learning models in NIDS. Researchers have employed supervised learning techniques such as Random Forest, Support Vector Machines (SVM), and deep learning models like Convolutional Neural Networks (CNNs) to detect a range of modern attacks including DDoS, brute force, and infiltration attacks.

Key findings from these studies indicate that ML models can significantly outperform traditional rule-based detection systems, particularly in terms of:

- **Detection accuracy**
- **False positive reduction**
- **Adaptability to dynamic threats**

Such research continues to drive the development of intelligent intrusion detection frameworks capable of handling large-scale and complex network traffic.

### 7.2 Industry Implementation: Blockchain-Based Logging in Enterprise Security

Several cybersecurity vendors and enterprises have begun integrating **blockchain technology into their security logging infrastructures** to enhance auditability and trust. In practice, blockchain is used to store cryptographically signed intrusion alerts and incident logs in an immutable ledger.

For example, companies in the **finance and healthcare sectors**, where compliance and data integrity are critical, use **permissioned blockchain platforms like Hyperledger** to maintain secure audit trails of security events. This prevents attackers or insiders from tampering with logs post-breach and ensures that forensic investigations are based on trustworthy data.

Benefits observed in these implementations include:

- Tamper-proof logging
- Improved regulatory compliance
- Enhanced transparency in security operations

### 7.3 Collaborative NIDS: Federated Learning and Blockchain

Emerging research has also demonstrated the potential of **collaborative intrusion detection systems** that use **federated learning** to share threat detection models across distributed nodes without exposing raw data. In such systems:

- Each node trains a local model on its own traffic data.
- Only model parameters are shared across the network.
- Blockchain ensures secure synchronization and trust among participants.

This approach preserves data privacy while enhancing the global detection capabilities of the NIDS network. It is especially promising in large-scale environments such as cloud infrastructure, smart cities, and industrial IoT ecosystems, where centralized data sharing is impractical or non-compliant with privacy regulations.

These case studies demonstrate that Smart NIDS—powered by AI, ML, and blockchain—are not only feasible but already making tangible impacts in both research and commercial sectors. Their continued refinement and deployment hold strong promise for the future of proactive cybersecurity.

## 8. FUTURE DIRECTIONS

As cyber threats continue to evolve in complexity and volume, the development of intelligent and resilient Network Intrusion Detection Systems must also advance[11-15]. While current integrations of AI, ML, and blockchain have shown significant promise, several emerging technologies and research directions have the potential to further enhance the effectiveness, scalability, and trustworthiness of Smart NIDS. The following subsections highlight key areas for future exploration.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 1116-1123

e-ISSN : 2583-1062
Impact Factor : 7.001

8.1 Explainable AI (XAI) in NIDS

One of the primary limitations of current AI and ML models is their "black-box" nature—security analysts often struggle to understand how decisions are made. **Explainable AI (XAI)** aims to bridge this gap by providing transparent, interpretable insights into model behavior.

In the context of NIDS, XAI can:

- Increase trust in AI-driven decisions by justifying why a certain traffic pattern was flagged as malicious.
- Help analysts identify false positives and improve system tuning.
- Facilitate compliance with regulations that require explainability in automated decision-making.

Integrating XAI into Smart NIDS will make them more user-friendly, auditable, and accessible to non-expert operators.

8.2 Federated Machine Learning for Privacy-Preserving Collaboration

**Federated Learning (FL)** offers a decentralized approach to training machine learning models by allowing multiple entities to collaborate without sharing raw data. This technique is particularly relevant for intrusion detection systems in distributed environments such as multi-branch organizations, cross-border networks, or IoT ecosystems.

Benefits of FL in NIDS include:

- Enhanced privacy and data sovereignty
- Collaborative learning from diverse attack profiles
- Reduced central processing and storage demands

Combined with blockchain, FL can ensure secure model updates and consensus on learned patterns across distributed nodes.

8.3 Quantum-Resistant Blockchain in Cybersecurity

With the advent of quantum computing, traditional cryptographic algorithms used in blockchain systems may become vulnerable. The future of Smart NIDS must therefore consider **quantum-resistant cryptography** to maintain the integrity and security of decentralized intrusion logging.

Future blockchain platforms integrated into NIDS may adopt:

- Lattice-based encryption
- Hash-based signature schemes
- Post-quantum key exchange protocols

These advancements will ensure that blockchain-enhanced NIDS remain secure in a post-quantum threat landscape.

8.4 Edge-Based Smart NIDS for IoT Environments

The proliferation of **Internet of Things (IoT)** devices introduces a new set of vulnerabilities due to limited computing resources and a vast, distributed attack surface. Traditional NIDS are not always suited for such environments.

**Edge-based Smart NIDS** aim to address this by deploying lightweight AI/ML models directly on or near IoT devices, enabling real-time, localized threat detection with minimal latency.

Future research in this area may focus on:

- Energy-efficient ML algorithms for edge hardware
- Federated learning among IoT nodes
- Integration with blockchain to maintain secure, distributed logs

This direction is crucial for securing smart homes, industrial systems, and next-generation urban infrastructure.

These emerging technologies represent the next frontier in the evolution of NIDS. Their successful integration will not only improve detection capabilities but also ensure scalability, trust, and adaptability in increasingly complex and decentralized network environments.

**Table 1:** Future Directions for Smart NIDS

| Future Direction | Description | Benefits |
|---|---|---|
| **Explainable AI (XAI)** | Makes AI decisions transparent and interpretable | Increases trust, aids in compliance, enhances analyst understanding |
| **Federated Machine** | Decentralized model training | Preserves privacy, enables collaborative |

| Future Direction | Description | Benefits |
|---|---|---|
| **Learning (FL)** | without sharing raw data | learning, reduces central resource usage |
| **Quantum-Resistant Blockchain** | Uses cryptographic techniques secure against quantum computing threats | Ensures long-term integrity of logs, strengthens blockchain security in future environments |
| **Edge-Based Smart NIDS** | Deploys lightweight NIDS at or near IoT devices | Reduces latency, supports real-time detection, improves scalability in distributed networks |

## 9. CONCLUSION

The increasing frequency and complexity of cyber threats have exposed the limitations of traditional Network Intrusion Detection Systems, particularly in their ability to detect unknown or evolving attack vectors. This paper has explored how Artificial Intelligence (AI), Machine Learning (ML), and Blockchain technologies are collectively transforming NIDS into intelligent, adaptive, and resilient defense mechanisms.

AI enhances decision-making capabilities by simulating human cognition, while ML enables systems to learn from network behavior and continuously improve detection accuracy. Blockchain, with its decentralized and immutable nature, ensures the integrity and traceability of security logs, strengthening trust and auditability. When integrated, these technologies form a synergistic framework that addresses the critical challenges of detection accuracy, data integrity, scalability, and real-time responsiveness.

While implementation challenges remain—such as computational overhead, data privacy concerns, and the need for interpretability—the trajectory of research and development points toward increasingly autonomous and collaborative NIDS architectures. Future innovations such as Explainable AI, Federated Learning, Quantum-Resistant Blockchain, and edge-based deployment are poised to further elevate the effectiveness of Smart NIDS across various domains.

Ultimately, the convergence of AI, ML, and Blockchain represents not just an upgrade to legacy systems, but a paradigm shift in how intrusion detection is conceptualized and operationalized in modern cybersecurity ecosystems.

## ACKNOWLEDGEMENTS

I sincerely thank my guide, **Mr. G. S. Udaya Kiran Babu, for** their support and guidance throughout this project work. I also extend my gratitude to **Dr. D William Albert,** Head of the Department, for providing the resources and encouragement needed to complete this work successfully.

## 10. REFERENCES

[1] Moustafa, N., Slay, J. (2016). UNSW-NB15: A Dataset for Network Intrusion Detection.

[2] Kim, G., Lee, S., & Kim, S. (2014). A Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection.

[3] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Blockchain-Based Logging for Network Forensics.

[4] Shone, N., et al. (2018). Deep Learning Approaches to Network Intrusion Detection.

[5] Singh, A., & Chatterjee, K. (2020). A Secure Logging Framework for Network Forensics Using Blockchain.

[6] Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). *2015 Military Communications and Information Systems Conference (MilCIS)*, IEEE.

[7] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2(1), 41-50.

[8] Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications*, 41(4), 1690-1700.

[9] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Blockchain for future smart cities: A review. *Journal of Ambient Intelligence and Humanized Computing*, 9(5), 1687–1700.

[10] Dhanabal, L., & Shantharajah, S. P. (2015). A study on NSL-KDD dataset for intrusion detection system based on classification algorithms. *International Journal of Advanced Research in Computer and Communication Engineering*, 4(6), 446-452.

[11] Li, T., & Wang, H. (2020). Blockchain for cybersecurity: A review. *IEEE Access*, 8, 181234-181251.

[12] Alsuhibany, S. A., & Alhaidari, F. A. (2022). Federated learning-based intrusion detection system for IoT security. *Sensors*, 22(1), 182.

[13] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82, 395-411.

[14] Ahmad, I., Basheri, M., Iqbal, M. J., & Rahim, A. (2018). Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection. *IEEE Access*, 6, 33789-33795.

[15] Liu, H., Lang, B., Liu, M., & Yan, H. (2020). CNN and RNN based payload classification methods for attack detection. *Knowledge-Based Systems*, 163, 332-341.

[16] Dr. Syed Gilani Pasha, dr. Saba fatima, dr. Vidya Pol, dr john e p,dr. Rolly gupta,dr. Brijesh shankarrao Deshmukh (2024) Revolutionizing Healthcare: The Challenges & Role of Artificial Intelligence Healthca e Management Practice for India's Economic Transformation. Frontiers in Health Informatics, 13 (7), 149-163

[17] Reddy, B. B. ., Pasha, S. G. ., Kameswari, M. ., Chinkera, R. ., Fatima, S. ., Bhargava, R. & Shrivastava, A. . (2024). Classification Approach for Face Spoof Detection in Artificial Neural Network Based on IoT Concepts. International Journal of Intelligent Systems and Applications in Engineering, 12(13s), 79–91. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/4570