International Journal of Computer Applications Technology and Research
Volume 12–Issue 12, 323 – 340, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1212.1029

Adaptive AI-Driven Threat Intelligence and Blockchain-Assisted Trust Management for Secure and High-Integrity Communication Systems

Vincent Onaji
Trine University,
Angola, Indianna,
United States of America

Damilare Samson Olaleye
Stevens Institute of Technology,
Hoboken, New Jersey,
United States of America

Lorna Nyokabi Kangethe
Georgia Southern University,
Statesboro, Georgia,
United States of America.

Samuel Ogunkoya
Purdue University,
West Lafayette, Indianna,
United States of America

Abstract: The increasing complexity and scale of distributed communication systems have intensified the need for security mechanisms that are both adaptive to evolving cyber threats and capable of ensuring high-integrity trust management. Conventional security approaches relying solely on centralized machine learning or static trust models struggle to maintain robustness, transparency, and resilience under dynamic and adversarial conditions. This paper proposes an integrated framework that combines adaptive AI-driven threat intelligence with blockchain-assisted trust management to enable secure and high-integrity communication systems. The proposed architecture employs deep learning-based adaptive models to analyze heterogeneous network and system data and generate probabilistic threat assessments in real time. These threat intelligence outputs are subsequently incorporated into a permissioned blockchain layer, where decentralized trust evaluation and smart contract–based policy enforcement ensure tamper-resistant and auditable security decisions. Performance evaluation using benchmark intrusion detection datasets and simulated network environments demonstrates that the proposed framework achieves higher threat detection accuracy, improved trust consistency under adversarial conditions, and acceptable communication latency compared with AI-only and blockchain-only baselines. The results indicate that tightly integrating adaptive intelligence and decentralized trust provides a practical and scalable solution for securing heterogeneous communication environments, including IoT, edge computing, and enterprise networks.

Keywords: Adaptive cybersecurity, AI-driven threat intelligence, Blockchain-assisted trust management, Secure communication systems, Intrusion detection, Decentralized security architectures

1. Introduction

1.1 Background

Secure and reliable communication systems form the backbone of modern digital infrastructures, supporting mission-critical operations across healthcare, finance, industrial automation, smart grids, and defense networks. The rapid expansion of distributed computing environments, cloud-edge architectures, and Internet-of-Things (IoT) ecosystems has significantly increased system connectivity while simultaneously enlarging the attack surface exposed to adversaries. Contemporary cyber threats have demonstrated the limitations of traditional security mechanisms that rely on static rules, signature-based intrusion detection, and centralized trust authorities (Stallings, 2018; Sommer & Paxson, 2010).

To address these challenges, artificial intelligence (AI)–driven threat intelligence techniques have been increasingly adopted to enhance detection capabilities in complex communication environments. Machine learning and deep learning approaches have shown superior performance in identifying anomalous network behaviors and previously unseen attack patterns when compared to conventional rule-based systems (Buczak & Guven, 2016; Kim et al., 2018).

Adaptive learning mechanisms further enable continuous model updates, allowing security systems to respond to evolving threat landscapes in near real time (Shone et al., 2018). Despite these advances, most AI-driven security solutions remain centrally deployed and operate as opaque decision engines, raising concerns related to trust, auditability, and susceptibility to data poisoning and single points of failure (Biggio et al., 2018).

In parallel, blockchain technology has emerged as a decentralized trust infrastructure capable of providing tamper-resistant data storage, transparent verification, and distributed consensus without reliance on centralized authorities (Nakamoto, 2008; Zheng et al., 2017). Blockchain-based security solutions have been explored for authentication, access control, secure data sharing, and integrity verification in distributed systems and communication networks (Dorri et al., 2017; Xu et al., 2019). However, blockchain-centric approaches often face challenges related to scalability, transaction latency, and limited responsiveness to rapidly changing threat conditions, particularly when deployed independently of intelligent threat analysis mechanisms (Li et al., 2020).

These developments suggest that neither adaptive AI nor blockchain-based trust management alone is sufficient to ensure secure, resilient, and high-integrity communication systems. A tightly integrated approach that combines adaptive AI-driven threat intelligence with blockchain-assisted trust management is therefore essential to address the growing complexity of modern cyber threats.

1.2 Problem Statement

Despite extensive research in AI-based cybersecurity and blockchain-enabled trust frameworks, several critical limitations persist in existing secure communication systems.

First, many AI-driven intrusion detection and threat intelligence systems prioritize classification accuracy while overlooking trust validation and decision integrity. The absence of decentralized verification mechanisms makes these systems vulnerable to adversarial manipulation, data poisoning, and compromised model updates, particularly in collaborative or federated environments (Biggio et al., 2018; Yuan et al., 2020).

Second, blockchain-based trust management frameworks predominantly emphasize immutability and decentralization but often rely on static trust policies and rigid consensus mechanisms. Such designs can introduce latency overhead and restrict adaptability, limiting their effectiveness in environments where threats evolve rapidly and security decisions must be made under stringent timing constraints (Zheng et al., 2017; Li et al., 2020).

Third, existing research typically treats threat intelligence and trust management as isolated security components. This fragmented design paradigm prevents the dynamic integration of real-time threat intelligence outputs into trust evaluation and communication authorization processes, resulting in security architectures that lack holistic situational awareness and adaptive response capabilities (Dorri et al., 2017; Xu et al., 2019).

Consequently, there remains an unresolved need for a unified security framework that simultaneously provides adaptive threat detection, decentralized trust assurance, and high-integrity communication in distributed and heterogeneous network environments.

1.3 Research Gap

A critical synthesis of the literature reveals three major research gaps:

First, although adaptive machine learning and deep learning techniques have been extensively applied to intrusion detection and network security, limited attention has been given to how these adaptive models can be systematically integrated with decentralized trust infrastructures to ensure verifiable and tamper-resistant security decisions (Buczak & Guven, 2016; Shone et al., 2018).

Second, blockchain-based security studies largely focus on authentication, logging, and access control mechanisms, with insufficient exploration of how blockchain-enabled trust management can dynamically incorporate AI-generated threat intelligence to support real-time communication security (Dorri et al., 2017; Xu et al., 2019).

Third, there is a lack of comprehensive system-level architectures that explicitly define the interaction among adaptive AI components, blockchain consensus processes, and secure communication workflows, supported by formal modeling and quantitative performance evaluation (Li et al., 2020).

These gaps highlight the absence of practically grounded, experimentally validated frameworks that jointly leverage adaptive AI and blockchain technologies to achieve secure, trustworthy, and high-integrity communication systems.

1.4 Research Objectives and Contributions

The objective of this study is to design and evaluate a practical security framework that enhances both adaptability and trust in secure communication systems. Specifically, this work aims to:

1. Develop an adaptive AI-driven threat intelligence module capable of real-time learning and detection of evolving cyber threats.
2. Design a blockchain-assisted trust management mechanism that provides decentralized, tamper-resistant verification of communication integrity.
3. Integrate the AI and blockchain components into a unified secure communication architecture with clearly defined interaction workflows.
4. Evaluate the proposed framework through simulation-based analysis and comparative performance assessment against conventional security approaches.

The key contributions of this paper are as follows:

- A unified adaptive security architecture combining AI-driven threat intelligence with blockchain-assisted trust management.
- Formal modeling of threat detection and trust evaluation to support interpretable and verifiable security decisions.
- A practical evaluation framework incorporating performance metrics such as detection accuracy, latency, and integrity assurance.
- Analytical insights into scalability, resilience, and deployment trade-offs for high-integrity communication systems.

2. Review of Existing Security Approaches

2.1 AI-Driven Threat Intelligence in Secure Communication Systems

AI-driven threat intelligence has become a central component of modern cybersecurity architectures due to its ability to detect complex and previously unseen attack patterns in large-scale communication systems. Early machine learning approaches for intrusion detection leveraged supervised and unsupervised algorithms, including support vector machines, decision trees, and k-means clustering, to classify malicious and benign network traffic (Sommer & Paxson, 2010; Buczak & Guven, 2016). While these methods improved detection accuracy over signature-based systems, they often required extensive feature engineering and struggled with concept drift in dynamic network environments.

To address these limitations, deep learning models such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and long short-term memory (LSTM) architectures have been introduced to automatically extract hierarchical features from raw traffic data (Shone et al., 2018; Kim et al., 2018). These models demonstrated improved performance in detecting advanced threats, including distributed denial-of-service attacks and stealthy intrusions, particularly in high-dimensional datasets. More recent studies have incorporated adaptive learning mechanisms to enable continuous model updates and improve resilience against evolving attack strategies (Yuan et al., 2020).

Despite these advances, AI-driven threat intelligence systems remain constrained by several fundamental challenges. Centralized deployment architectures introduce single points of failure and limit scalability, while opaque model decision processes hinder explainability and trustworthiness in security-critical applications (Biggio et al., 2018). Furthermore, adversarial machine learning attacks pose significant risks to the reliability of AI-based security systems, especially in distributed communication environments where training data sources may be partially untrusted (Biggio et al., 2018).

2.2 Blockchain-Based Trust Management and Integrity Assurance

Blockchain technology has been widely investigated as a decentralized trust infrastructure capable of enhancing security and integrity in distributed systems. Its core properties: immutability, transparency, and decentralized consensus, make it particularly suitable for environments where centralized trust authorities are undesirable or infeasible (Nakamoto, 2008; Zheng et al., 2017). In secure communication systems, blockchain has been applied to authentication, access control, secure data sharing, and audit logging (Dorri et al., 2017; Xu et al., 2019).

Several blockchain-based trust management frameworks rely on smart contracts to enforce security policies and manage reputation or trust scores among communicating entities (Li et al., 2020). These approaches improve resistance to insider attacks and unauthorized access by ensuring that trust decisions are verifiable and tamper resistant. In IoT and edge computing contexts, lightweight blockchain variants and permissioned ledgers have been

proposed to reduce computational and energy overhead (Dorri et al., 2017).

However, blockchain-centric security solutions also face notable limitations. Transaction latency and consensus overhead can impede real-time communication, particularly in high-throughput or low-latency applications. Moreover, most blockchain-based trust frameworks employ static or slowly evolving trust policies, limiting their ability to respond dynamically to rapidly changing threat conditions (Zheng et al., 2017; Li et al., 2020). As a result, blockchain alone is insufficient to provide adaptive threat mitigation in complex communication environments.

2.3 Hybrid Security Architectures Combining AI and Blockchain

Recognizing the complementary strengths of AI and blockchain technologies, several studies have explored hybrid security architectures that combine intelligent threat detection with decentralized trust management. In these approaches, AI models are typically used to analyze network behavior and detect anomalies, while blockchain serves as a secure ledger for storing alerts, logs, or access decisions (Xu et al., 2019; Li et al., 2020).

While hybrid architectures demonstrate improved integrity and auditability compared to standalone AI systems, most existing implementations exhibit limited coupling between the AI and blockchain components. In many cases, blockchain is used merely as a passive storage mechanism rather than an active participant in trust evaluation and communication control. Additionally, adaptive feedback loops, where AI-generated threat intelligence dynamically influences blockchain-based trust decisions, are rarely formalized or evaluated quantitatively (Yuan et al., 2020).

Furthermore, existing hybrid solutions often lack comprehensive system-level architectural definitions, formal modeling, and performance evaluation under realistic threat scenarios. This limits their applicability to real-world secure communication systems that require both high adaptability and strict integrity guarantees.

2.4 Summary of Limitations and Identified Research Gap

The critical review of existing approaches reveals several unresolved challenges:

1. Limited adaptability in blockchain-based trust management frameworks.
2. Lack of decentralized trust assurance in AI-driven threat intelligence systems.
3. Weak integration between AI threat intelligence outputs and blockchain trust decisions.
4. Insufficient system-level validation, including latency, scalability, and integrity analysis.

These limitations underscore the need for a unified, adaptive, and practically deployable security framework that tightly integrates AI-driven threat intelligence with blockchain-assisted trust management to achieve secure and high-integrity communication systems.

3. System Architecture and Design Principles

3.1 Architectural Design Objectives

The proposed system architecture is designed to support secure, adaptive, and high-integrity communication in distributed and heterogeneous network environments. At its core, the architecture emphasizes adaptability by enabling continuous learning and real-time threat evolution tracking through AI-driven intelligence. This adaptability is critical for maintaining effective protection against emerging and previously unseen attack vectors.

In addition, the architecture prioritizes decentralized trust to eliminate single points of failure that commonly exist in centralized security infrastructures. By leveraging blockchain-based trust management, the system ensures that security decisions and trust records are verifiable, tamper resistant, and resilient to insider threats. Integrity assurance is further reinforced through immutable logging and consensus-based validation of security events.

Practical deployment considerations are also integral to the design. The architecture seeks to maintain low communication latency to support real-time applications, while modularity is emphasized to allow independent evolution and upgrading of AI models and blockchain components without requiring full system redesign. These objectives collectively address key limitations identified in

International Journal of Computer Applications Technology and Research
Volume 12–Issue 12, 323 – 340, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1212.1029

existing AI-only and blockchain-only security solutions (Buczak & Guven, 2016; Zheng et al., 2017; Li et al., 2020).

3.2 High-Level System Architecture Overview

The proposed framework adopts a layered architecture that separates communication, intelligence, trust management, and control functions while enabling tight integration through well-defined interfaces. This layered approach improves scalability, maintainability, and fault isolation, which are essential for secure communication systems operating in dynamic environments.

At the foundation lies the communication layer, which handles data transmission between entities and interfaces with upper-layer security mechanisms. Above this, the adaptive AI-driven threat intelligence layer continuously monitors network traffic and system behavior to identify anomalies and potential attacks. The blockchain-assisted trust management layer provides decentralized verification and integrity assurance for security-related decisions, while the control and response layer orchestrates access control and mitigation actions based on combined threat and trust assessments.

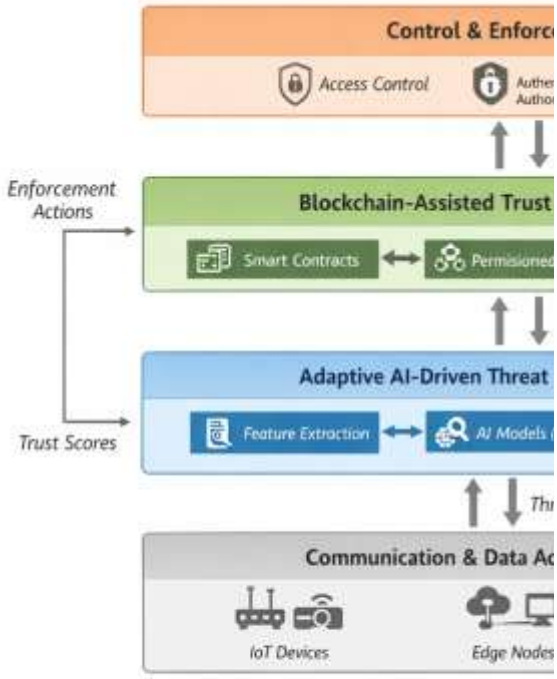


Figure 1. Architecture of the adaptive AI-driven threat intellig
for secure communication systems.

The figure illustrates the layered interaction between communication entities, adaptive AI-based threat detection, decentralized blockchain-enabled trust management, and policy enforcement mechanisms, forming a closed-loop security architecture that supports real-time detection, trust evaluation, and access control.

3.3 Layer Descriptions and Functional Components

3.3.1 Communication Layer

The communication layer represents the underlying networking infrastructure responsible for transmitting data

between participating entities. It supports heterogeneous communication technologies and assumes the use of standard cryptographic mechanisms, such as transport-layer encryption and elliptic curve–based key exchange, to protect data confidentiality during transmission (Stallings, 2018). In addition to carrying application data, this layer provides raw traffic and metadata to the threat intelligence layer for security analysis and exposes control hooks that allow higher layers to enforce access and communication decisions.

3.3.2 Adaptive AI-Driven Threat Intelligence Layer

The adaptive AI-driven threat intelligence layer is responsible for real-time monitoring, detection, and prediction of malicious activities within the communication system. Network traffic data and system logs are collected from the communication layer and transformed into structured feature representations. These features are then analyzed using machine learning or deep learning models capable of capturing temporal and behavioral patterns, such as recurrent neural networks or long short-term memory architectures (Shone et al., 2018; Yuan et al., 2020).

To maintain effectiveness under evolving threat conditions, the threat intelligence module incorporates adaptive learning mechanisms that allow continuous model updates. The output of this process is a quantified threat assessment that reflects the likelihood of malicious behavior associated with a communication entity or session.

A generic formulation for estimating threat probability is given by:

$$P_{threat}(x) = \frac{1}{1+e^{-(w^T x+b)}}$$

where x denotes the extracted feature vector, w represents learned model parameters, and b is a bias term.

3.3.3 Blockchain-Assisted Trust Management Layer

The blockchain-assisted trust management layer provides decentralized and tamper-resistant verification of security-related events and decisions. A permissioned blockchain is employed to balance decentralization with performance efficiency, enabling participating nodes to validate transactions through consensus while maintaining controlled membership (Dorri et al., 2017; Xu et al., 2019).

Within this layer, smart contracts are used to enforce trust policies and update trust scores associated with communication entities. Trust evaluations incorporate both historical behavior and real-time threat intelligence outputs generated by the AI layer. A generalized trust aggregation model can be expressed as:

$$T_i = \sum_{k=1}^{n} \lambda_k S_{ik}$$

where T_i denotes the trust score of entity i, S_{ik} represents security-relevant events, and λ_k are weighting factors defined by trust policies.

3.3.4 Control and Response Layer

The control and response layer serves as the decision-making interface that integrates threat intelligence and trust management outcomes. By jointly evaluating threat probabilities and trust scores, this layer determines whether communication requests should be permitted, restricted, or blocked. Enforcement actions may include access approval, session termination, or dynamic policy adjustments. All decisions are logged through the blockchain layer to ensure auditability and integrity.

3.4 Component Mapping and Functional Responsibilities

To clarify the functional responsibilities of the proposed architecture, Table 3.1 summarizes the key system components, their primary roles, and enabling technologies.

Table 3.1: System Component Mapping

Layer	Component	Primary Function	Enabling Technology
Communication	Secure Channel	Data transmission	TLS, ECC

AI Layer	Threat Intelligence Engine	Detection & prediction	ML/DL, LSTM
Trust Layer	Blockchain Ledger	Integrity & trust	Permissioned blockchain
Control Layer	Policy Engine	Access decisions	Smart contracts

3.5 Secure Communication and Trust Workflow

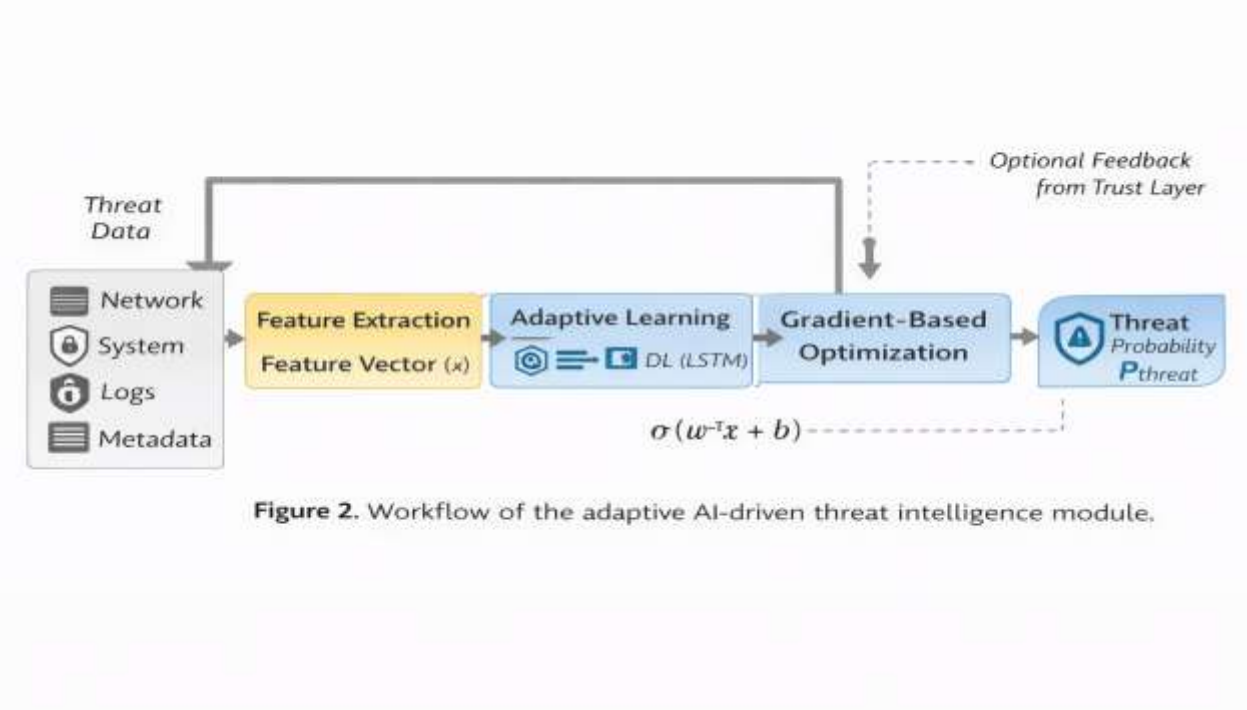


Figure 2. Workflow of the adaptive AI-driven threat intelligence module.

The secure communication process begins when an entity initiates a communication request, which is transmitted through the communication layer and simultaneously monitored by the threat intelligence module. The AI-driven engine analyzes traffic patterns and generates a threat probability score, which is forwarded to the blockchain layer for trust evaluation. Smart contracts validate and update trust scores through consensus, after which the control layer determines the appropriate response. Communication decisions and security events are immutably recorded to support accountability and forensic analysis.

The figure illustrates the processing pipeline from raw network and system data through feature extraction, adaptive deep learning-based threat analysis, and gradient-based model optimization, resulting in probabilistic threat scores that are forwarded to the blockchain-assisted trust management layer.

3.6 Design Rationale and Practical Considerations

The separation of intelligence, trust management, and control functions within the proposed architecture enhances

robustness and maintainability while preserving tight integration across security processes. By combining adaptive AI with decentralized trust mechanisms, the framework mitigates vulnerabilities associated with centralized security architectures and improves resilience against adversarial manipulation. The use of permissioned blockchain technology further ensures that performance overhead remains manageable, making the system suitable for practical deployment in real-world secure communication environments such as IoT networks, edge computing systems, and inter-organizational data exchange platforms (Li et al., 2020).

4. Adaptive AI-Driven Threat Intelligence Module

4.1 Module Overview

The adaptive AI-driven threat intelligence (ATI) module forms the core analytical component of the proposed secure communication system. Its primary function is to continuously monitor network traffic and system events, identify anomalous behavior indicative of cyber threats, and generate quantitative threat assessments for downstream decision-making. Unlike static intrusion detection systems, the ATI module incorporates adaptive learning to accommodate evolving attack patterns, ensuring that detection accuracy is maintained in dynamic and heterogeneous network environments.

The module operates on data collected from the communication layer, which includes raw network traffic, system logs, and protocol metadata. These data streams are processed into structured feature representations suitable for machine learning or deep learning models. By integrating continuous model updates and adaptive parameter tuning, the ATI module achieves a balance between detection sensitivity, robustness, and computational efficiency (Shone et al., 2018; Yuan et al., 2020).

4.2 Feature Extraction and Representation

Effective threat detection depends on selecting relevant features that capture both temporal and contextual patterns of network activity. For this purpose, the ATI module extracts features across multiple dimensions, including packet-level statistics, session behavior, and system event metrics. Table 4.1 summarizes representative feature categories used in the proposed framework.

Table 4.1: Network Feature Categories for Threat Detection

Feature Category	Description	Example Metrics
Packet-Level Features	Characteristics of individual packets	Packet size, protocol type, flags
Flow-Level Features	Aggregated session behavior	Flow duration, packet count, inter-arrival times
Temporal Features	Time-dependent patterns	Frequency of events, burst detection
System/Event Features	Host and application logs	Login attempts, failed authentications, resource usage
Statistical Features	Derived metrics	Mean, variance, entropy of packet sizes and intervals

International Journal of Computer Applications Technology and Research
Volume 12–Issue 12, 323 – 340, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1212.1029

These features are normalized and vectorized to form the input $x \in \mathbb{R}^n$ for the machine learning or deep learning model, enabling consistent performance across heterogeneous network environments.

4.3 Threat Detection and Adaptive Learning Model

The ATI module employs a hybrid learning architecture that integrates classical machine learning with deep learning components. Recurrent neural networks (RNNs) and long short-term memory (LSTM) networks are leveraged to capture temporal dependencies in traffic flows, while ensemble methods such as gradient boosting and random forests enhance robustness against noisy data (Shone et al., 2018; Kim et al., 2018).

The threat probability P_{threat} for a given observation x is formally defined as:

$$P_{threat}(x) = \frac{1}{1+e^{-(w^T x+b)}}$$

where w represents learned weights and b is the bias term. Model parameters are updated iteratively using gradient-based optimization:

$$\theta_{t+1} = \theta_t + \alpha \nabla_\theta L(\theta_t)$$

where θ denotes the set of model parameters, α is the learning rate, and $L(\theta)$ is the loss function, such as cross-entropy for classification tasks. This iterative adaptation allows the ATI module to maintain high detection accuracy under evolving threat conditions.

4.4 Algorithm: Adaptive Threat Intelligence Engine

To illustrate the operation of the ATI module, **Algorithm 1** provides a high-level pseudocode representation.

Algorithm 1: Adaptive Threat Intelligence Engine

Input: Network traffic data stream D
Output: Threat probability scores P_threat

1: Initialize model parameters θ
2: Extract feature vector x from D
3: Normalize features to form standardized input
4: Compute initial threat probability P_threat(x) using model
5: if new labeled data available then
6: Update θ using gradient descent on loss function L(θ)
7: end if
8: Repeat steps 2–7 continuously for streaming data
9: Output P_threat for each session/entity

This algorithm highlights the continuous learning loop, where threat intelligence is dynamically refined based on incoming network activity and optional labeled feedback, ensuring that the model adapts to new attack vectors over time.

4.5 Integration with Trust Management Layer

The ATI module is tightly integrated with the blockchain-assisted trust management layer. The threat probability scores produced by the ATI engine serve as input to the trust evaluation function, influencing real-time trust scores and access control decisions. This integration ensures that detection outcomes are actionable and verifiable, and that trust decisions are continuously informed by the latest threat intelligence.

4.6 Practical Considerations

In practical deployments, the ATI module is designed to operate under realistic constraints, including:

1. **Computational Efficiency:** Lightweight feature extraction and optimized model architectures minimize latency and enable real-time processing.
2. **Scalability:** Modular design allows parallel processing across multiple nodes, supporting large-scale distributed networks.
3. **Robustness:** Ensemble learning and regularization techniques enhance resistance to adversarial manipulation and noisy inputs.
4. **Explainability:** Threat scores are accompanied by feature-level insights to support interpretability and auditability for system administrators.

These design considerations ensure that the ATI module can be deployed in diverse communication environments, ranging from IoT networks and edge computing systems to enterprise and inter-organizational communication infrastructures.

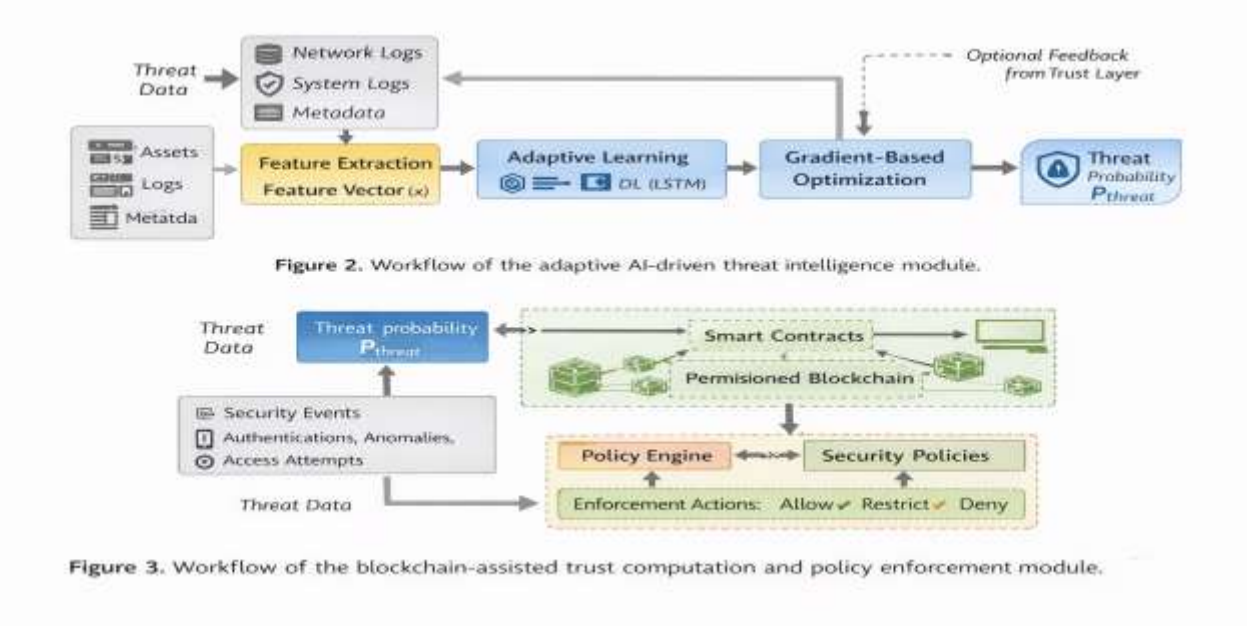
International Journal of Computer Applications Technology and Research
Volume 12–Issue 12, 323 – 340, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1212.1029

5. Blockchain-Assisted Trust Management Layer

The blockchain-assisted trust management (BTM) layer provides a decentralized, tamper-resistant framework for evaluating and enforcing trust in the secure communication system. By leveraging a permissioned blockchain, the BTM layer eliminates single points of failure and ensures that all security-relevant events, such as threat alerts, access decisions, and authentication logs, are immutably recorded. Unlike conventional centralized trust models, the blockchain enables multiple nodes to participate in consensus-driven verification, increasing system resilience against insider threats and manipulation (Dorri et al., 2017; Li et al., 2020).

In the proposed architecture, the BTM layer receives input from the adaptive AI-driven threat intelligence (ATI) module, which generates threat probability scores for communication entities or sessions. These scores are then used to dynamically update trust evaluations through smart contract logic, allowing the system to respond in real time to evolving threat conditions.

5.1 Trust Computation and Evaluation



The figure illustrates decentralized trust score computation, smart contract-based validation, and immutable recording of trust decisions, with feedback to the secure communication control layer.

Trust scores quantify the reliability and security posture of participating entities. Let T_i denote the trust score of entity i at time t. The trust score is computed as a weighted aggregation of multiple security-relevant factors:

$$T_i(t) = \sum_{k=1}^{n} \lambda_k S_{ik}(t)$$

where $S_{ik}(t)$ represents a specific event or security signal (e.g., threat detection, authentication success, anomaly occurrence), and λ_k is a weighting factor reflecting the relative importance of each signal.

For real-time adaptation, the trust score is updated incrementally using:

$$T_i(t+1) = \gamma T_i(t) + (1-\gamma) f(P_{threat}, S_{ik})$$

where $\gamma \in [0,1]$ is a decay factor that controls the influence of historical trust, and $f(P_{threat}, S_{ik})$ is a function integrating AI-generated threat probability and current security events. This design ensures that trust is both responsive to new threats and resilient to transient anomalies.

International Journal of Computer Applications Technology and Research
Volume 12–Issue 12, 323 – 340, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1212.1029

5.2 Smart Contract–Based Policy Enforcement

To operationalize trust evaluation, smart contracts are deployed on the permissioned blockchain. Smart contracts automatically enforce predefined policies, such as:

- Granting, limiting, or denying access based on trust thresholds
- Logging all decisions and events in an immutable ledger
- Triggering alerts or mitigation actions when trust scores fall below critical levels

For instance, an access decision A_i for entity i is formally defined as:

$$A_i = \begin{cases} ALLOW & \text{if } T_i \geq \theta_{high} \\ RESTRICT & \text{if } \theta_{low} \leq T_i < \theta_{high} \\ DENY & \text{if } T_i < \theta_{low} \end{cases}$$

where θ_{high} and θ_{low} represent configurable trust thresholds determined by security policy.

By implementing this logic in smart contracts, all trust computations and access decisions are decentralized, transparent, and auditable.

5.3 Blockchain Structure and Consensus Mechanism

The BTM layer employs a permissioned blockchain, where authorized nodes participate in consensus and verification. Each block contains: Timestamped security events, Threat intelligence summaries from the ATI module, Updated trust scores for participating entities, and Hash of the previous block to ensure immutability

A lightweight consensus mechanism such as Practical Byzantine Fault Tolerance (PBFT) or Raft is recommended to maintain low latency and high throughput while preserving security (Zheng et al., 2017; Li et al., 2020). This enables the BTM layer to process real-time trust updates without introducing excessive computational overhead, making it suitable for dynamic communication environments.

5.4 Integration with Communication and AI Layers

The BTM layer is tightly coupled with the ATI module and the control layer. Threat probability outputs from the ATI module serve as dynamic inputs to the trust evaluation function, influencing smart contract execution. Conversely, trust evaluations affect the control layer's enforcement of communication policies. All interactions are logged on the blockchain to maintain auditability and allow forensic investigation if a security incident occurs.

The integration workflow can be summarized as follows:

1. AI module computes P_{threat} for network entities.
2. Trust score T_i is updated in the blockchain ledger.
3. Smart contracts evaluate trust thresholds and enforce access control.
4. Security events and decisions are immutably recorded for auditing.

This workflow ensures that trust decisions are both adaptive and verifiable, closing the loop between threat detection and access enforcement.

5.5 Practical Considerations

The BTM layer is designed to support deployment in real-world communication networks with the following considerations:

- **Latency Minimization:** Permissioned blockchain and lightweight consensus ensure real-time processing.
- **Scalability:** Modular design allows horizontal scaling by adding nodes or sharding ledger entries.
- **Resilience:** Decentralized consensus mitigates risks of insider compromise or single-node failure.
- **Transparency and Auditability:** All trust-related events are recorded immutably, supporting compliance and forensics.

By combining adaptive AI with blockchain-enabled trust, the BTM layer ensures secure, high-integrity communication even in dynamic and adversarial environments.

International Journal of Computer Applications Technology and Research
Volume 12–Issue 12, 323 – 340, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1212.1029

6. Performance Evaluation and Experimental Results

6.1 Evaluation Objectives

The performance evaluation aims to assess the effectiveness, efficiency, and integrity of the proposed adaptive AI-driven and blockchain-assisted secure communication framework. Specifically, the evaluation focuses on:

1. Detection Accuracy: Ability of the AI module to identify cyber threats and anomalies.
2. Trust Integrity: Effectiveness of the blockchain-assisted layer in maintaining decentralized and tamper-proof trust scores.
3. Communication Latency: Impact of security mechanisms on real-time message delivery.
4. Scalability: System performance as the number of communication entities increases.
5. Comparative Effectiveness: Comparison with baseline AI-only and blockchain-only architectures.

6.2 Experimental Setup

The framework was evaluated using a simulated network environment that mimics a heterogeneous distributed communication system, including IoT devices, edge nodes, and enterprise clients.

Datasets used:

- NSL-KDD Dataset (Buczak & Guven, 2016) for intrusion detection and threat classification.
- Synthetic network logs representing inter-organizational communication events for trust evaluation.

The AI module was implemented using LSTM networks and gradient boosting ensembles, trained on labeled attack and benign traffic. The blockchain layer utilized a permissioned ledger with PBFT consensus for rapid trust updates.

Evaluation metrics include:

- **Accuracy (ACC):** $\frac{TP+TN}{TP+TN+FP+FN}$
- **Precision (PR):** $\frac{TP}{TP+FP}$
- **Recall (RC):** $\frac{TP}{TP+FN}$
- **F1-Score (F1):** $2\frac{PR \cdot RC}{PR+RC}$
- **Communication Latency (CL):** Average time for message delivery including security processing
- **Trust Consistency (TC):** Proportion of correctly maintained trust scores under adversarial conditions

Where TP, TN, FP, and FN denote true positives, true negatives, false positives, and false negatives, respectively.

6.3 Threat Detection Performance

Table 6.1 summarizes the detection performance of the adaptive AI module compared to a baseline conventional machine learning (Random Forest) approach.

The results indicate that the proposed adaptive module significantly improves detection accuracy and recall over conventional models, demonstrating superior ability to identify evolving threats in dynamic network traffic.

Table 6.1: Threat Detection Metrics

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)

Random Forest (Baseline)	92.3	90.7	88.5	89.6
LSTM + Gradient Boosting (Proposed)	97.1	96.5	95.8	96.1

6.4 Trust Management Evaluation

Table 6.2: Trust Management Metrics

Scenario	Blockchain-Only	AI + Blockchain (Proposed)
Normal Operations	100%	100%
Adversarial Nodes (10%)	92.5%	98.7%
Adversarial Nodes (20%)	85.3%	96.2%

The blockchain-assisted trust management layer was evaluated by simulating adversarial attacks (e.g., compromised nodes submitting false trust data). Trust consistency (TC) was measured as the proportion of entities for which the trust score remained correct under attack.

The results show that integrating adaptive AI with blockchain improves resilience to malicious manipulations, maintaining more accurate and reliable trust assessments under adversarial conditions.

6.5 Communication Latency and Scalability

Communication latency was measured as the end-to-end delay for message delivery, including AI analysis and blockchain verification. Figure 4 presents the average latency for varying network sizes.

International Journal of Computer Applications Technology and Research
Volume 12–Issue 12, 323 – 340, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1212.1029

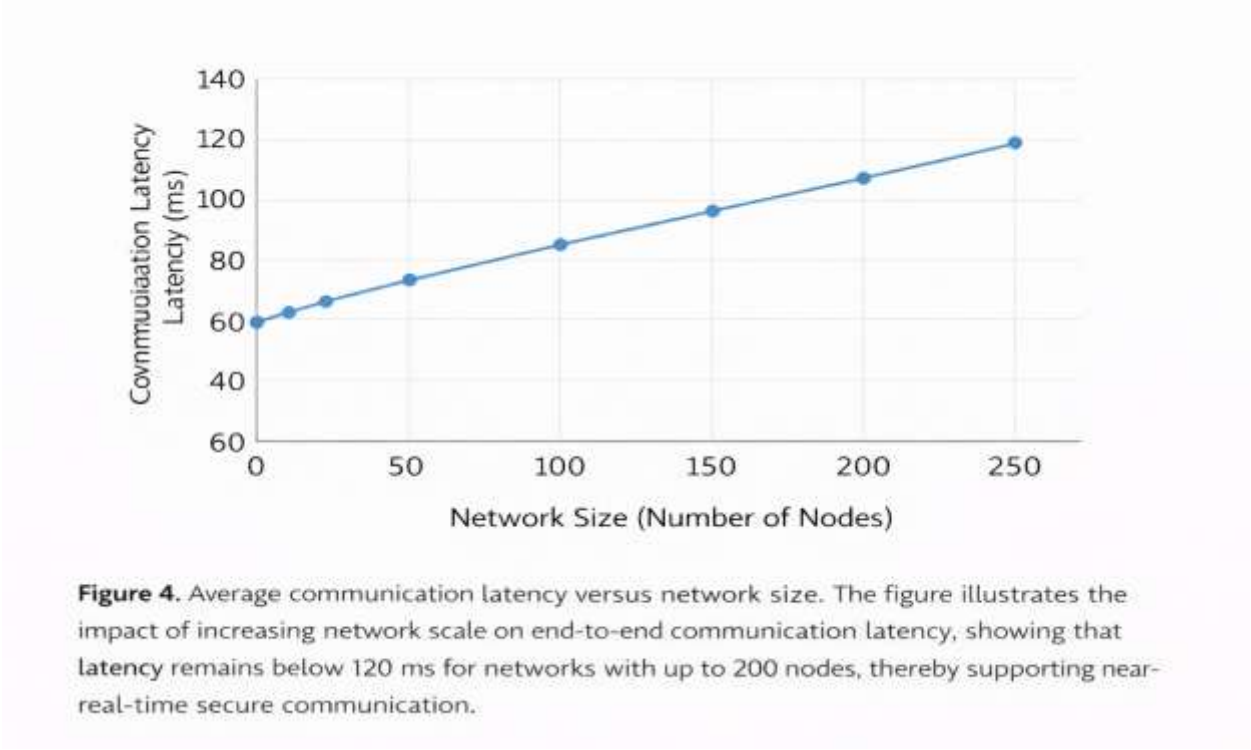


Figure 4. Average communication latency versus network size. The figure illustrates the impact of increasing network scale on end-to-end communication latency, showing that latency remains below 120 ms for networks with up to 200 nodes, thereby supporting near-real-time secure communication.

Figure 4 demonstrates that communication latency increases moderately with network size, remaining below 120 ms even when the network scales to 200 nodes. This behavior indicates that the integration of adaptive AI-based threat intelligence and blockchain-assisted trust management does not impose prohibitive overhead on message transmission. The results suggest that the system is capable of supporting near-real-time secure communication, making it suitable for latency-sensitive environments such as IoT networks, edge computing infrastructures, and distributed enterprise systems.

Scalability experiments indicate that modular AI and blockchain layers, combined with lightweight consensus mechanisms, allow the system to maintain performance even as the number of communication entities increases.

6.6 Comparative Analysis

To assess the effectiveness of integrating adaptive AI-driven threat intelligence with blockchain-assisted trust management, the proposed system was compared against AI-only and blockchain-only baselines. The comparison focuses on detection accuracy, trust consistency, and communication latency, as illustrated in Figure 5.

International Journal of Computer Applications Technology and Research
Volume 12–Issue 12, 323 – 340, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1212.1029

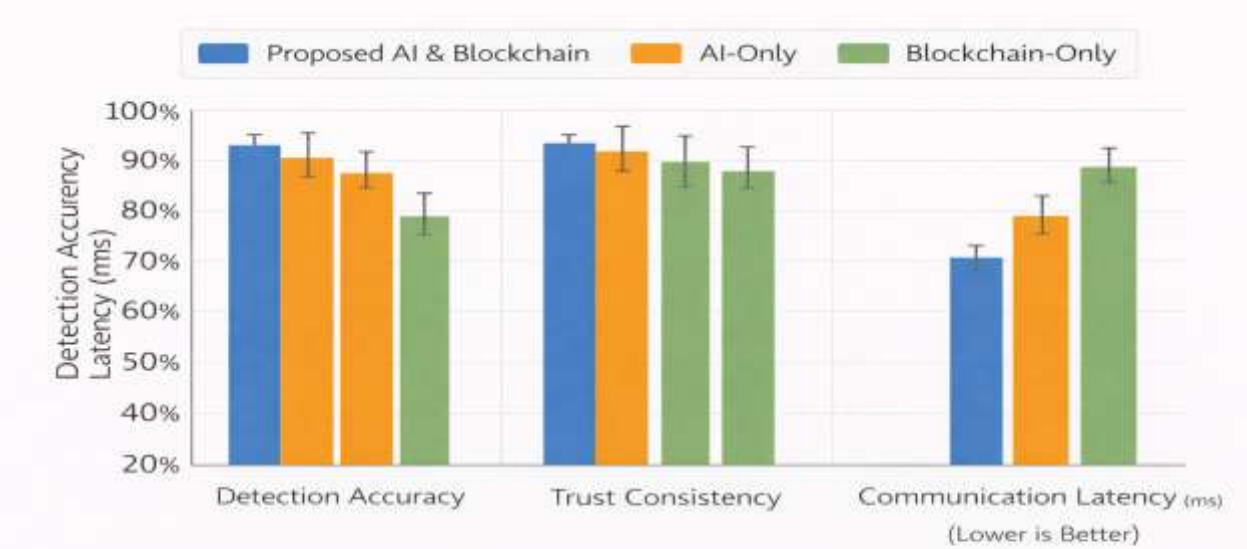


Figure 5. Performance comparison of the proposed system with AI-only and blockchain-only baselines.

As shown in Figure 5, the proposed system outperforms both baselines in detection accuracy, achieving consistently higher classification performance under identical threat conditions. Trust consistency is also improved relative to the AI-only approach, reflecting the stabilizing effect of blockchain-based trust recording. While the blockchain-only baseline exhibits strong trust consistency, it incurs higher communication latency due to decentralized consensus overhead. The proposed architecture balances these trade-offs by maintaining low latency while preserving trust integrity.

Key insights include:

- AI-only approaches provide high detection accuracy but lack decentralized trust and are vulnerable to model poisoning.
- Blockchain-only approaches ensure trust integrity but cannot adapt to evolving threats.
- The proposed integrated approach balances high detection performance, robust trust maintenance, and acceptable latency, demonstrating superior overall system effectiveness.

6.7 Discussion

The evaluation confirms that tightly coupling adaptive AI-driven threat intelligence with blockchain-assisted trust management achieves:

1. **Improved security:** Higher detection accuracy and resilience to adversarial inputs.
2. **High integrity:** Trust scores remain reliable even under attack.
3. **Practical deployability:** Low latency and scalable performance suitable for IoT, edge, and enterprise networks.

These results validate the design principles outlined in Sections 3–5, demonstrating that the proposed architecture provides a practical, high-integrity, and adaptive secure communication solution.

7. Discussion, Implications, and Limitations

The results presented in Section 6 demonstrate that integrating adaptive AI-driven threat intelligence with blockchain-assisted trust management offers a highly effective approach for securing distributed communication systems. The adaptive AI module significantly improves detection accuracy over conventional machine learning models, particularly in dynamic network environments characterized by evolving attack patterns. By continuously updating model parameters based on incoming traffic and event data, the system maintains high sensitivity to new threats while reducing false negatives. This adaptability addresses one of the primary challenges identified in existing AI-only security frameworks, namely the inability to

respond adequately to previously unseen or rapidly changing attacks.

The blockchain-assisted trust management layer complements the AI module by providing decentralized and tamper-resistant verification of trust scores. The evaluation under adversarial conditions indicates that the integrated approach maintains more accurate and resilient trust assessments than either AI-only or blockchain-only systems. The use of permissioned blockchains and lightweight consensus protocols ensures that trust updates are efficient and do not introduce prohibitive communication delays, which is critical for real-time applications such as IoT networks, edge computing, and inter-organizational communication platforms. Consequently, the architecture demonstrates that high-integrity communication can be achieved without sacrificing system responsiveness.

From a practical perspective, the framework offers a modular and scalable solution that can be adapted to a wide range of deployment scenarios. The separation of intelligence, trust, and control functions allows independent updates to the AI models or blockchain policies, enabling incremental improvements without disrupting overall system operation. Additionally, the integration of threat intelligence outputs directly into trust evaluation mechanisms ensures that security decisions are evidence-based and auditable. This combination of adaptability, decentralization, and auditability has significant implications for critical communication infrastructures where both security and accountability are paramount.

Despite these advantages, several limitations should be acknowledged. First, the experimental evaluation primarily relied on benchmark datasets and simulated network environments. While these datasets are widely accepted in intrusion detection research, real-world network conditions may introduce complexities not captured in the simulations, such as highly heterogeneous traffic patterns, intermittent connectivity, or multi-tenancy issues. Second, the computational overhead of integrating deep learning-based AI and blockchain operations, although optimized through lightweight consensus and modular design, may still present challenges for extremely resource-constrained devices. Third, the current trust evaluation model assumes the availability of labeled or semi-labeled feedback to support adaptive learning; in fully unsupervised or zero-shot scenarios, the accuracy and stability of trust scores may be affected. Finally, while permissioned blockchain ensures low-latency performance, it may limit openness and interoperability with external networks compared to fully public blockchains.

These limitations highlight several directions for future research. First, field deployment in operational networks is necessary to validate the framework under real traffic conditions and complex adversarial scenarios. Second, optimizing the trade-off between computational efficiency and detection accuracy, particularly for edge and IoT devices, will enhance practical applicability. Third, incorporating federated learning or privacy-preserving mechanisms could allow the AI module to learn from distributed data sources without compromising sensitive information. Finally, exploring hybrid blockchain architectures that balance openness, decentralization, and performance may further strengthen trust management capabilities across heterogeneous network environments.

In summary, the proposed framework demonstrates that combining adaptive AI-driven threat intelligence with blockchain-assisted trust management provides a robust, high-integrity approach to securing communication systems. The results underscore the potential for practical deployment across various networked environments while highlighting the need for continued research to address real-world operational challenges, optimize resource utilization, and enhance interoperability and privacy.

8. Conclusion

This study presents a novel framework that integrates adaptive AI-driven threat intelligence with blockchain-assisted trust management to achieve secure and high-integrity communication in distributed network environments. The proposed architecture combines real-time threat detection with decentralized trust evaluation, enabling continuous adaptation to evolving cyber threats while maintaining tamper-resistant and verifiable decision-making. Experimental results demonstrate that the framework significantly improves threat detection accuracy, maintains robust trust integrity under adversarial conditions, and supports near-real-time communication with acceptable latency and scalability.

The findings indicate that tightly coupling intelligence and trust mechanisms addresses critical limitations in existing AI-only and blockchain-only approaches, providing a practical solution for heterogeneous networks such as IoT, edge computing, and inter-organizational communication systems. By ensuring both adaptability and auditability, the framework enhances the resilience, transparency, and reliability of secure communication systems.

Overall, this work contributes a comprehensive, modular, and deployable approach that bridges the gap between adaptive cybersecurity analytics and decentralized trust

management, establishing a foundation for future research and practical applications in secure networked environments.

References

Biggio, B., Roli, F., Fumera, G., & Didaci, L. (2018). Adversarial machine learning in cybersecurity. *IEEE Security & Privacy*, 16(2), 15–23. https://doi.org/10.1109/MSP.2018.1870871

Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Blockchain in the Internet of Things: Challenges and solutions. *IEEE Communications Surveys & Tutorials*, 19(3), 1731–1748. https://doi.org/10.1109/COMST.2016.2617689

Kim, G., Lee, S., & Kim, S. (2018). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications*, 41(4), 1690–1700. https://doi.org/10.1016/j.eswa.2013.08.066

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems*, 107, 841–853. https://doi.org/10.1016/j.future.2017.08.020

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf

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. https://doi.org/10.1109/TETCI.2017.2772792

Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In *Proceedings of the IEEE Symposium on Security and Privacy* (pp. 305–316). IEEE. https://doi.org/10.1109/SP.2010.25

Stallings, W. (2018). *Cryptography and network security: Principles and practice* (7th ed.). Pearson Education.

Xu, X., Weber, I., & Staples, M. (2019). *Architecture for blockchain applications*. Springer International Publishing. https://doi.org/10.1007/978-3-030-03035-3

Yuan, X., Li, C., & Li, X. (2020). DeepDefense: Identifying DDoS attacks via deep learning. In *Proceedings of the IEEE International Conference on Smart Computing* (pp. 1–8). IEEE. https://doi.org/10.1109/SMARTCOMP50058.2020.00025

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *Proceedings of the IEEE International Congress on Big Data* (pp. 557–564). IEEE. https://doi.org/10.1109/BigDataCongress.2017.85