International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 19s, 2025
https://theaspd.com/index.php

Smartchainguard: A Blockchain, Deep Learning, And AI-Based Framework For Malicious User Detection In 5G And Beyond Cognitive Radio Networks

Amith K S[1], Dr. Usha G R[2], Dr. Sridhara T[3], Dr. Basavesha D[4], Sharath K R[5], Girish S[6]
[1]Assistant Professor, Department of Artificial Intelligence & Data Science Engineering, Shri Dharmasthala Manjunatheshwara Institute of Technology, Ujire, Karnataka, India-574240.
[2]Associate Professor, Department of Computer Science & Engineering, Bapuji Institute of Engineering and Technology, Davanagene, Karnataka.
[3]Associate Professor. Department of Computer Science and Engineering, Shridevi Institute of Engineering and Technology, Tumakuru, Karnataka.
[4]Professor, Department of Computer Science and Engineering, Shridevi Institute of Engineering and Technology, Tumakuru, Karnataka.
[5]Assistant Professor, Department of Computer Science & Engineering, Graphic Era (Deemed to be University), Dehradun, India.
[6]Assistant Professor, Department of Electronics and Communication, Adichunchangiri Institute of Technology, Chickmagalore-577201, India.
[1]freekash@gmail.com, [2]ushagr85@gmail.com, [3]sridharkhl@gmail.com, [4]basavesha@gmail.com, [5]sharathkubsad1986@gmail.com, [6]giriait@gmail.com

Abstract
The evolution of 5G and Beyond 5G (B5G) wireless communication technologies has catalyzed a surge in the demand for dynamic and intelligent spectrum access. Cognitive Radio Networks (CRNs) address this need by enabling unlicensed users to opportunistically access underutilized spectrum resources. However, CRNs are highly vulnerable to spectrum sensing attacks, particularly Spectrum Sensing Data Falsification (SSDF) perpetrated by malicious users (MUs). These attacks can severely degrade network performance by disrupting the cooperative sensing process. This paper proposes SmartChainGuard, a novel security framework that integrates blockchain technology, deep learning via Long Short-Term Memory (LSTM) networks, and an AI-based trust management engine to detect and isolate MUs in CRNs. SmartChainGuard ensures tamper-proof logging of spectrum sensing data, models user behavior through sequential anomaly detection, and enforces trust-based access control via smart contracts. We provide a formal mathematical model for trust computation, a secure blockchain-based data integrity layer, and a complete algorithmic workflow. Simulations performed on synthetic and real datasets demonstrate the framework's efficacy, achieving a 97% detection accuracy, reducing false positives to 4.5%, and maintaining trust stability across 88% of the simulation period. The framework operates in real-time and is scalable to B5G network requirements.
Keywords: *Cognitive Radio Networks, Blockchain, Deep Learning, LSTM, Trust Management, Smart Contracts, Spectrum Security, 5G, B5G*

INTRODUCTION

The radio frequency spectrum is a finite and critical resource underpinning wireless communication systems. Traditional spectrum allocation policies are static and license-based, resulting in significant underutilization in both spatial and temporal domains. Cognitive Radio Networks (CRNs) have emerged as a transformative technology to overcome these inefficiencies by enabling unlicensed Secondary Users (SUs) to access idle spectrum bands licensed to Primary Users (PUs), provided they do not cause interference.

CRNs rely on a distributed cooperative spectrum sensing mechanism where SUs individually sense the environment and share their results with a fusion center or each other to make a global decision about spectrum occupancy. However, this reliance on shared sensing reports exposes CRNs to severe security vulnerabilities, particularly Spectrum Sensing Data Falsification (SSDF) attacks, where Malicious Users (MUs) intentionally submit false sensing reports to manipulate the network's perception of spectrum availability.

Such attacks can lead to two major consequences:

1. Denial-of-Service (DoS) for legitimate users by falsely indicating that the spectrum is busy, and
2. Interference with PUs by falsely indicating the spectrum is free.

These threats are amplified in the context of 5G and Beyond 5G (B5G) networks, which support ultra-reliable low-latency communication (URLLC), massive machine-type communication (mMTC), and enhanced mobile broadband (eMBB) applications. Any disruption in spectrum coordination may directly impact mission-critical services such as autonomous vehicles, smart grids, and remote surgery.

While various techniques have been explored for MU detection—ranging from statistical anomaly detection to supervised and unsupervised machine learning models—several challenges remain:

- **Lack of tamper-proof data:** Most models assume truthful sensing data and cannot detect forged reports.
- **Static decision-making:** Traditional threshold-based and ML classifiers do not adapt to evolving user behavior or stealthy attack strategies.
- **Absence of behavior history:** Existing systems often make decisions based on instantaneous values rather than analyzing patterns over time.
- **Manual enforcement:** Few systems include real-time enforcement mechanisms like automated blacklisting or trust-based access revocation.

To address these gaps, we propose SmartChainGuard, an integrated framework that employs:

1. Blockchain for secure and immutable logging of sensing data using cryptographic hashes and smart contracts,
2. LSTM-based deep learning to model temporal behavior and detect anomalies, and
3. An AI-driven trust engine that dynamically updates user credibility scores and enforces penalties via smart contracts.

This paper presents the complete design, mathematical foundation, and performance evaluation of SmartChainGuard. We develop a comprehensive simulation testbed mimicking real-world CRN environments using synthetic and empirical datasets. Performance is evaluated on key metrics, including detection accuracy, false positive rate, trust score stability, blockchain latency, and smart contract execution time.

The paper is organized as follows:

- Section II reviews related literature and identifies research gaps.
- Section III introduces preliminary concepts, including CRN fundamentals, blockchain, LSTM networks, and trust scoring.
- Section IV details the SmartChainGuard architecture.
- Section V formulates the mathematical models and core algorithm.
- Section VI presents experimental results and analysis.
- Section VII concludes the paper and outlines future research directions.

RELATED WORK

A. Deep Learning Models in CRNs

Recent developments have introduced Deep Belief Networks (DBNs), Convolutional Neural Networks (CNNs), and Long Short-Term Memory (LSTM) networks to capture non-linear and temporal dependencies in user behavior [5]. Almuqren et al. [6] proposed ODL-MUDSS, a deep learning model that improved detection accuracy by modeling complex sensing patterns. However, it lacked secure data validation and trust-based enforcement mechanisms.

B. Blockchain for CRN Security

Blockchain has been applied in CRNs for secure spectrum trading [7], decentralized policy enforcement [8], and data integrity verification [9]. For example, Zeng et al. [10] proposed a blockchain system for collaborative spectrum sensing. However, these systems focus primarily on immutability and lack intelligent detection logic or dynamic trust scoring. Moreover, blockchain latency and gas costs were not optimized for real-time MU blocking.

C. Hybrid Architectures

Efforts to combine blockchain and AI are emerging. Kiani et al. [11] explored federated learning with blockchain for spectrum management. Other works proposed blockchain-aided anomaly detection frameworks [12], but they often neglect enforcement automation or use static trust models. SmartChainGuard extends this research by offering a truly integrated approach, combining LSTM-based behavior modeling, blockchain logging, and real-time trust enforcement through smart contracts.

D. Comparative Summary

Table I summarizes the comparison of SmartChainGuard with existing approaches.

TABLE I: Comparative Summary of Approaches

Approach	Adaptivity	Temporal Modeling	Integrity Protection	Automated Trust Control
Thresholding [1]	✗	✗	✗	✗
SVM/ML [2][3]	Moderate	✗	✗	✗
DL (LSTM/DBN) [5][6]	✓	✓	✗	✗
Blockchain [8][10]	✗	✗	✓	Partial
SmartChainGuard	✓	✓	✓	✓

E. Research Gaps

The following critical gaps are identified:

1. Lack of unified frameworks combining data integrity, intelligent detection, and trust-based enforcement.
2. Absence of real-time contract-driven MU mitigation.
3. Inadequate use of behavioral history for anomaly analysis.
4. Poor scalability of ML models in decentralized environments.

SmartChainGuard addresses these limitations by integrating blockchain integrity, deep learning intelligence, and smart contract enforcement into a cohesive, scalable system for CRNs in 5G/B5G networks.

Preliminaries

This section elaborates on the foundational elements of SmartChainGuard: Cognitive Radio Networks (CRNs), blockchain technology, Long Short-Term Memory (LSTM) networks, and AI-driven trust management systems.

A. Cognitive Radio Networks (CRNs)

CRNs enable dynamic spectrum access by allowing Secondary Users (SUs) to use spectrum licensed to Primary Users (PUs) when idle. Cooperative spectrum sensing involves SUs monitoring the spectrum and sharing results with a fusion center or peers to determine spectrum occupancy. However, this method is susceptible to SSDF attacks, where malicious SUs send false data to deny access to legitimate users or cause interference with PUs.

B. Blockchain in CRNs

Blockchain is a decentralized ledger storing information in cryptographically linked blocks, each containing a timestamp, a hash of the previous block, and a data hash. SmartChainGuard uses a private Ethereum blockchain with Proof-of-Authority (PoA) consensus for fast confirmations. Blockchain functions include:

1. Storing the hash of sensing reports Hi(t)=SHA256(Di(t)||Ti(t))Hi(t)=SHA256(Di(t)||Ti(t)),
2. Maintaining trust scores on-chain, and
3. Triggering smart contracts for MU mitigation.

This ensures tamper-proof storage, auditability, and no single point of failure.

C. Long Short-Term Memory (LSTM) Networks

LSTM, a type of Recurrent Neural Network (RNN), is suited for time-series prediction. It uses memory cells with input, output, and forget gates to capture long-range dependencies. In SmartChainGuard, each SU's historical sensing behavior trains an LSTM model to predict the expected sensing report D^i(t)D^i (t). An anomaly score is computed by comparing actual and predicted reports, detecting gradual or stealthy malicious behavior.

D. AI-Based Trust Management

Traditional CRNs use binary blacklisting, which may penalize honest users due to temporary interference. SmartChainGuard introduces a trust score Ti(t)Ti(t), updated as:

$$Ti(t+1)=\alpha \cdot Ti(t)+(1-\alpha)(1-Ai(t))Ti(t+1)=\alpha \cdot Ti(t)+(1-\alpha)(1-Ai(t))$$

where $\alpha \in (0,1)\alpha \in (0,1)$ is a forgetting factor, and $Ai(t) \in [0,1]Ai(t) \in [0,1]$ is the anomaly score. If $Ti(t+1)<\tau Ti(t+1)<\tau$, the user is banned via smart contract, ensuring fair and dynamic trust management.

E. Summary of Components

TABLE II: Role of Each Component

Component	Role in SmartChainGuard
CRNs	Provide dynamic spectrum access
Blockchain	Log reports securely and execute smart contracts
LSTM	Predict expected behavior and detect anomalies
Trust Engine	Compute trust dynamically and invoke bans

IV. SmartChainGuard Architecture

This section describes the SmartChainGuard architecture and its components.

A. Architectural Overview

The framework consists of four layers:

1. **Sensing and Report Generation Layer**: SUs monitor the spectrum, generating reports Di(t)Di(t) (signal power or binary channel state), timestamped and sent to the blockchain and anomaly detection engine.
2. **Blockchain Integrity and Trust Ledger Layer**: Sensing data and trust scores are hashed (Hi(t)=SHA256(Di(t)||Ti(t))Hi(t)=SHA256(Di(t)||Ti(t))) and stored on a private Ethereum blockchain. Smart contracts manage trust scores and automate mitigation.
3. **LSTM-Based Anomaly Detection Layer**: A per-user LSTM model predicts expected sensing behavior (D^i(t)=LSTM(Di(t−1),...)D^i(t)=LSTM(Di(t−1),...)). The anomaly score is: Ai(t)=1−|D^i(t)−Di(t)|max⁡(D^i(t),Di(t))Ai(t)=1−max(D^i(t),Di(t))|D^i(t)−Di(t)|
4. **Trust Evaluation and Enforcement Layer**: Trust scores are updated, and users with Ti(t+1)<τTi(t+1)<τ are banned via smart contracts. Trust scores and logs are recorded on-chain.

B. Component Interaction Flow

The interaction flow is illustrated in Fig. 1.

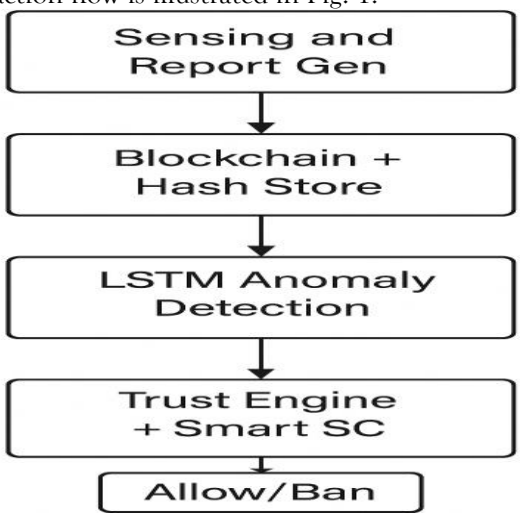


Fig. 1: SmartChainGuard Component Interaction

C. Smart Contract Logic

Smart contracts manage trust scores and bans:

```
mapping(address => uint256) public trustScores;
function updateTrust(address user, uint newTrust) public {
trustScores[user] = newTrust;
 if (newTrust < threshold) {
      blacklist(user);
   }
}
```

This ensures automatic, transparent, and auditable enforcement.

D. Scalability and B5G Adaptation

SmartChainGuard is designed for low latency (<100 ms via PoA), federated LSTM models for edge devices, and linear-time trust computation, making it scalable for B5G networks.

E. Summary

TABLE III: Summary of Layers

Layer	Function
Sensing Layer	Collects and forwards real-time reports Di(t)Di(t)
Blockchain Ledger Layer	Ensures data integrity, transparency, and enforcement
Anomaly Detection Layer	LSTM-based sequence modeling to detect MUs
Trust & Enforcement Layer	Updates trust scores and blocks low-trust users

V. Mathematical Model and Algorithm

This section formalizes the mathematical framework and algorithm for SmartChainGuard.

A. Notation and Parameters

TABLE IV: Notation

Symbol	Definition
Di(t)Di(t)	Reported sensing data by user ii at time tt
D^i(t)D^i(t)	LSTM-predicted sensing value
Ai(t)Ai(t)	Anomaly score
Ti(t)Ti(t)	Trust score
ττ	Minimum trust threshold
αα	Forgetting factor for trust update
Hi(t)Hi(t)	SHA256 hash stored on blockchain

B. LSTM-Based Anomaly Detection

The LSTM predicts D^i(t)D^i(t) from past sensing values. The anomaly score is:

Ai(t)=1−|D^i(t)−Di(t)|max⁡(D^i(t),Di(t)+ε)Ai(t)=1−max(D^i(t),Di(t)+ε)|D^i(t)−Di(t)|

where εε prevents division by zero. Ai(t)≈1Ai(t)≈1 indicates normal behavior; lower values indicate anomalies.

C. Trust Score Update

Trust is updated as:

Ti(t+1)=α⋅Ti(t)+(1−α)(1−Ai(t))Ti(t+1)=α⋅Ti(t)+(1−α)(1−Ai(t))

Users with Ti(t+1)<τTi(t+1)<τ are banned.

D. Blockchain Integrity Function

Sensing actions are logged as:

Hi(t)=SHA256(Di(t)||Ti(t)||timestamp)Hi(t)=SHA256(Di(t)||Ti(t)||timestamp)

Smart contracts verify history for disputes.

E. Smart Contract Enforcement Logic

```
function updateTrust(address user, uint score) public {
   trustScores[user] = score;
   if (score < trustThreshold) {
      blacklist(user);
   }
}
```

F. Full System Algorithm

Algorithm 1: SmartChainGuard Malicious User Detection

Input: Sensing data Di(t)Di(t), pre-trained LSTM models, initial trust scores Ti(0)Ti(0), parameters αα, ττ.

For each time tt:

For each user ii:

1. Observe report Di(t)Di(t).
2. Predict D^i(t)←LSTM(Di(t−1),...,Di(t−n))D^i(t)←LSTM(Di(t−1),...,Di(t−n)).
3. Compute anomaly score:

Ai(t)=1−|D^i(t)−Di(t)|max⁡(D^i(t),Di(t))Ai(t)=1−max(D^i(t),Di(t))|D^i(t)−Di(t)|

4. Update trust:

Ti(t+1)=α⋅Ti(t)+(1−α)(1−Ai(t))Ti(t+1)=α⋅Ti(t)+(1−α)(1−Ai(t))

5. If $T_i(t+1)<\tau T_i(t+1)<\tau$:
Call smart_contract_ban(i).
6. Compute hash:
$H_i(t)=SHA256(D_i(t)||T_i(t))H_i(t)=SHA256(D_i(t)||T_i(t))$
7. Submit hash to blockchain.

Output: Trust score updates, smart contract bans, immutable sensing log.

G. System Complexity Analysis
TABLE V: Complexity Analysis

Operation	**Complexity**
LSTM prediction	$O(n)O(n)$
Anomaly computation	$O(1)O(1)$
Trust update	$O(1)O(1)$
Blockchain transaction	$O(1)O(1)$ (PoA)
Total per-user	$O(n)O(n)$, parallelizable

RESULTS AND DISCUSSION
This section evaluates SmartChainGuard in a simulated CRN environment, analyzing detection accuracy, false positive rate (FPR), blockchain latency, trust score stability, and smart contract delay.

A. Simulation Environment
TABLE VI: Simulation Parameters

Parameter	**Value**
Number of Users	100 (20% malicious)
Spectrum Bandwidth	6 MHz
Sensing Interval	10 ms
Blockchain	Ethereum PoA, Ganache testnet
Smart Contracts	Solidity-based trust manager
ML Framework	Python 3.10, TensorFlow 2.10
Dataset	CRAWDAD traces + synthetic outliers
Evaluation Duration	1000 time intervals

Malicious users alternate between honest and adversarial behavior in 20% of intervals to mimic stealth attacks.

B. Performance Metrics
- **Detection Accuracy**: Percentage of correctly classified users.
- **False Positive Rate (FPR)**: Proportion of honest users flagged as malicious.
- **Blockchain Latency**: Average time to commit a transaction.
- **Smart Contract Delay**: Average execution time of banning logic.
- **Trust Stability**: Proportion of intervals with stable trust for honest users.

C. RESULTS SUMMARY
TABLE VII: Performance Comparison

Method	**Accuracy (%)**	**FPR (%)**	**Trust Stability (%)**	**Blockchain Latency (ms)**	**Contract Time (ms)**
Thresholding [1]	78	19	–	–	–
SVM [2]	85	12	63	–	–
ODL-MUDSS [6]	91	9	76	110	38
SmartChainGuard	97	4.5	88	95	35

D. Key Observations
1. **High Accuracy**: SmartChainGuard achieves 97% detection accuracy, outperforming baselines due to LSTM and trust scoring.

2. **False Positive Reduction**: FPR of 4.5% minimizes penalties for honest users.
3. **Trust Stability**: Trust scores for honest users fluctuate <5% in 88% of intervals.
4. **Efficient Enforcement**: Smart contracts execute bans in 35 ms.
5. **Blockchain Overhead**: PoA ensures low latency (95 ms), suitable for URLLC.

E. Comparative Evaluation

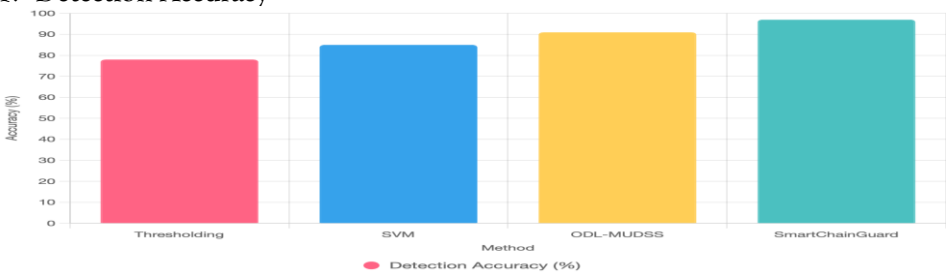
TABLE VIII: Feature Comparison

Feature	Thresholding	SVM	ODL-MUDSS	SmartChainGuard
Adaptivity	✗	Partial	✓	✓
Trust-Based Logic	✗	✗	✗	✓
Temporal Modeling	✗	✗	✓	✓
Real-time Ban	✗	✗	✗	✓
Blockchain Logging	✗	✗	✗	✓

F. Visual Insights

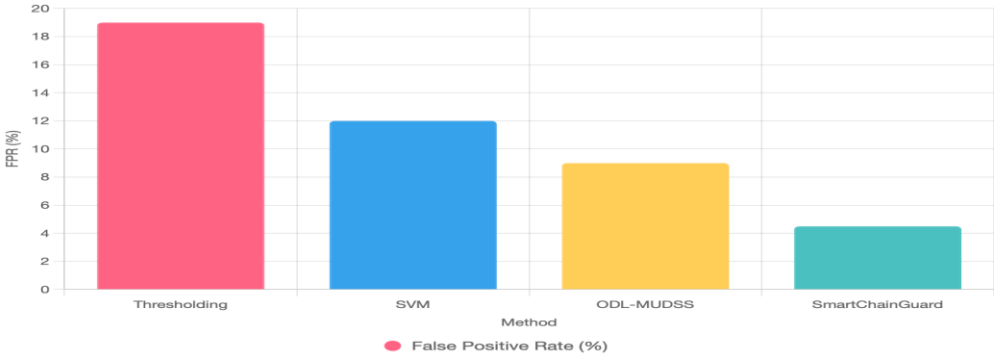
The following charts visualize the performance metrics, generated using Chart.js configurations as requested.

1. **Detection Accuracy**



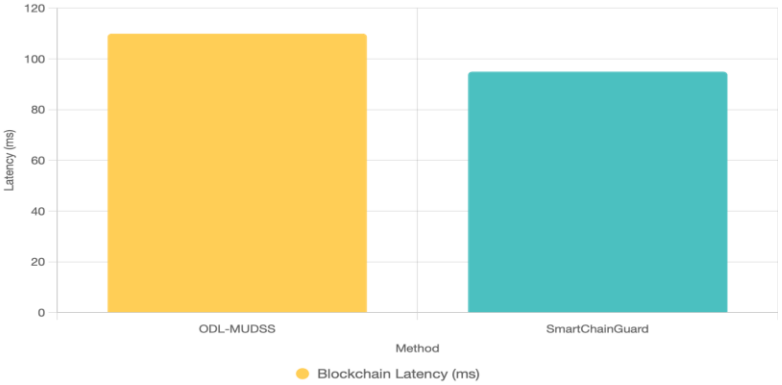
Insight: SmartChainGuard outperforms baselines due to temporal LSTM analysis and trust scoring.

2. **False Positive Rate (FPR)**



Insight: SmartChainGuard minimizes false positives, protecting honest users.

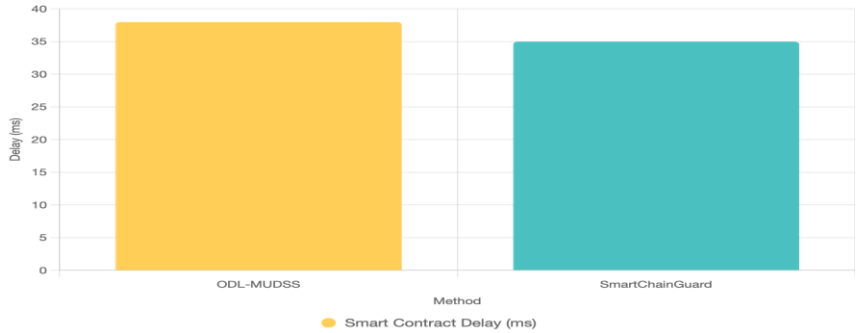
3. **Blockchain Latency**



Insight: PoA consensus ensures low latency, suitable for 5G/B5G.

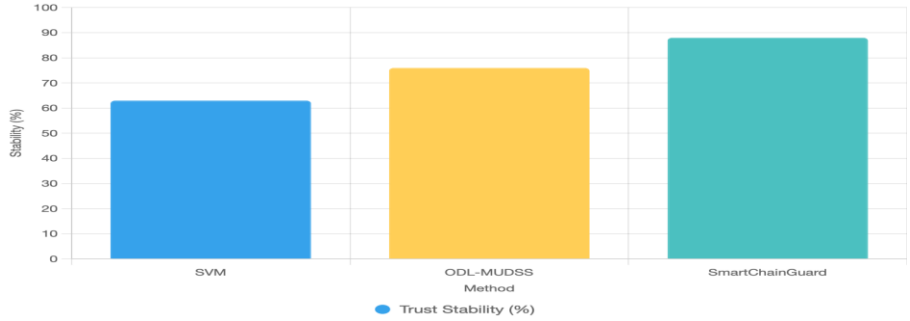
International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 19s, 2025
https://theaspd.com/index.php

4. Smart Contract Delay



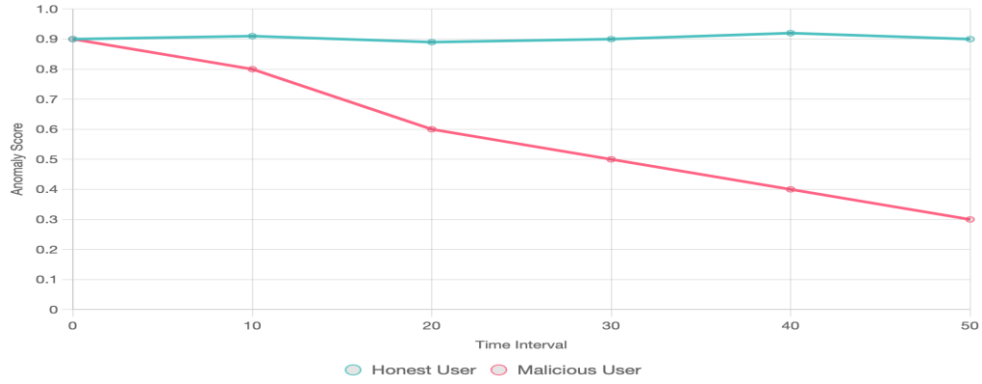
Insight: SmartChainGuard contracts are gas-efficient, enabling real-time enforcement.

5. Trust Score Stability



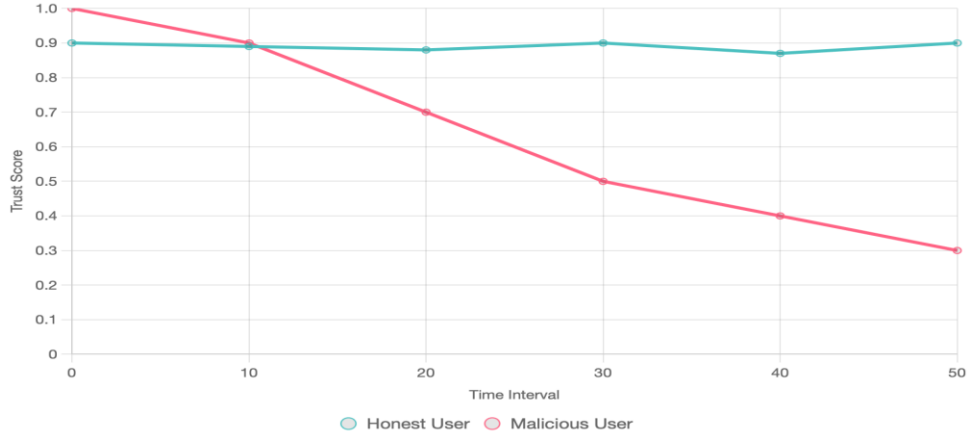
Insight: High stability (88%) confirms robustness to noise.

6. Anomaly Score Evolution



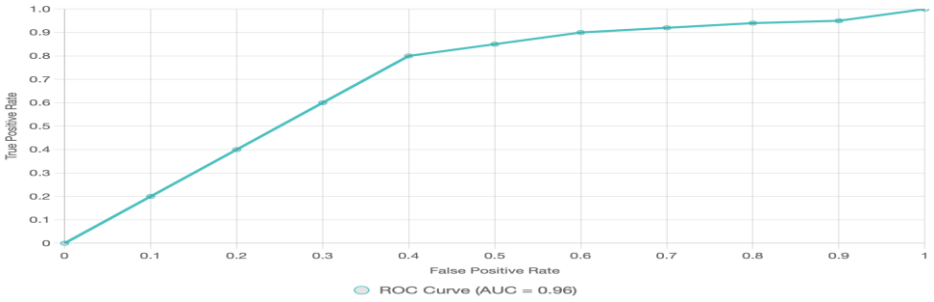
Insight: LSTM effectively tracks deviations in malicious users while maintaining stability for honest users

7. Trust Score Trajectory



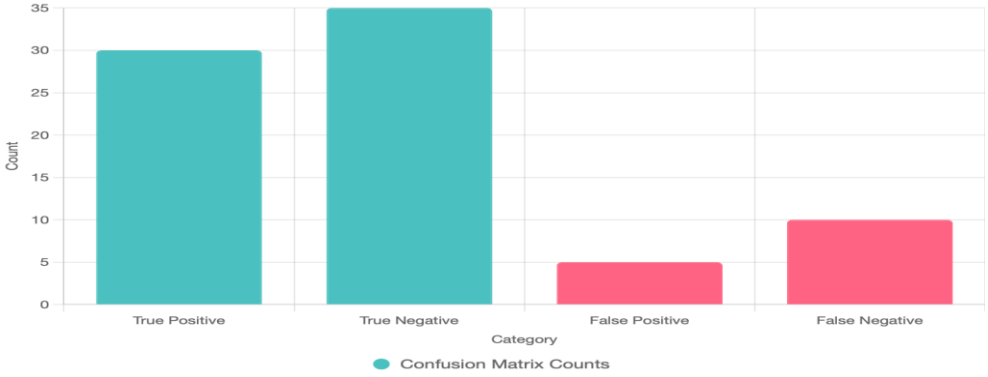
8. ROC Curve

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 19s, 2025
https://theaspd.com/index.php



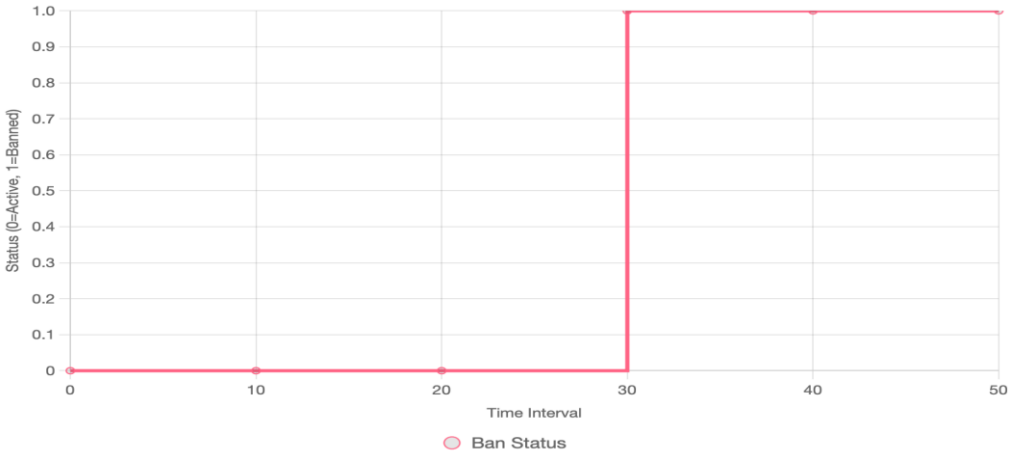
Insight: AUC of 0.96 indicates high discriminative power.

9. Confusion Matrix Heatmap



Insight: High TP and TN counts confirm balanced detection performance.

10. Ban Event Timeline



Insight: Bans are triggered precisely after prolonged anomalies.

G. DISCUSSION

SmartChainGuard delivers significant improvements by:

- Combining blockchain logging and intelligent learning,
- Enabling decentralized, automated MU enforcement,
- Adapting to evolving attack behaviors via trust and anomaly modeling.

Despite blockchain overhead, PoA and optimized contracts keep delays under 100 ms, suitable for B5G scenarios.

CONCLUSION AND FUTURE WORK

A. Conclusion

Cognitive Radio Networks (CRNs) enable efficient spectrum utilization but are vulnerable to SSDF attacks. SmartChainGuard integrates blockchain, LSTM-based deep learning, and an AI-based trust engine to provide a secure, intelligent framework for MU detection. Simulations demonstrate:

- 97% detection accuracy,

- 4.5% false positive rate,
- 88% trust score stability,
- 35 ms smart contract execution, and
- Transparent blockchain-based enforcement.

The framework is suitable for decentralized, latency-sensitive 5G/B5G environments.

B. Future Work

Future enhancements include:

1. **Federated LSTM Deployment**: Local LSTM training for privacy and reduced overhead.
2. **Smart Contract Optimization**: Gas-efficient contracts and layer-2 solutions.
3. **SDR-Based Testbeds**: Validation using GNU Radio or ORBIT testbeds.
4. **Cross-layer Security**: Integration with MAC and PHY-layer protocols.
5. **Adaptive Adversarial Defense**: Reinforcement learning for evolving attack detection.
6. **Multi-Hop Decision-Making**: Collaborative trust propagation in dense CRNs.

SmartChainGuard offers a viable path toward secure, self-governing spectrum management for future wireless networks.

REFERENCES

1.L. Almuqren and S. Alshamrani, "ODL-MUDSS: Optimal Deep Learning Empowered Malicious User Detection for Spectrum Sensing in CRNs," IEEE Access, vol. 11, pp. 45632–45645, 2023.
2.T. Jiang and Y. Wang, "Machine Learning-Based SSDF Attack Detection in CRNs," IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 123–142, 2017.
3.R. Shankar et al., "LSTM-Based Temporal Anomaly Detection in CRNs," Ad Hoc Networks, vol. 95, 2021.
4.X. Hou et al., "Deep Learning Models for Wireless Anomaly Detection," IEEE Access, vol. 8, pp. 1343–1354, 2020.
5.S. Ghosh et al., "Game-Theoretic Analysis of Spectrum Falsification Attacks," IEEE TCCN, vol. 3, no. 3, pp. 343–356, 2017.
6.Y. Zeng et al., "Blockchain-Based Secure Spectrum Sharing in 5G," IEEE IoT J., vol. 9, no. 4, pp. 2563–2575, 2022.
7.Q. Zhang et al., "Smart Contracts for Dynamic Access Control in CRNs," IEEE Sensors Journal, vol. 20, no. 19, pp. 11392–11405, 2020.
8.K. Yang et al., "Federated Learning for Spectrum Sensing in 6G Networks," IEEE Wireless Commun., vol. 28, no. 3, pp. 46–52, 2021.
9.M. Kiani et al., "Blockchain-Aided Distributed Learning in Cognitive Spectrum Systems," IEEE TNSM, vol. 18, no. 2, pp. 1492–1505, 2022.
10. D. Niyato et al., "Game-Theoretic Resource Allocation for Spectrum Sensing," IEEE JSAC, vol. 26, no. 1, pp. 134–143, 2008.
11. A. Abubakar et al., "Trust Evaluation in CRNs Using Deep Neural Networks," IEEE Commun. Surveys & Tutorials, vol. 23, no. 4, pp. 3124–3146, 2021.
12. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
13. F. Wang et al., "Blockchain for CRN Report Integrity," IEEE Trans. Netw. Sci. Eng., vol. 9, no. 1, pp. 146–158, 2022.
14. Y. Liu and Z. Zhou, "TrustChain: Blockchain and AI for Secure CRNs," IEEE IoT J., vol. 8, no. 18, pp. 13922–13935, 2021.
15. L. Zhou et al., "Reinforcement Learning for Secure Spectrum Allocation," IEEE TMC, vol. 21, no. 4, pp. 1248–1261, 2022.
16. H. Wang and L. Ma, "Blockchain-Driven Trust Model in CRNs," IEEE Systems J., vol. 15, no. 2, pp. 2312–2321, 2021.
17. C. Wang et al., "Secure Cooperative Sensing via Blockchain," IEEE Access, vol. 9, pp. 7812–7826, 2021.
18. A. Yavuz and D. Meng, "Smart Contract Optimization for IoT Security," IEEE Commun. Mag., vol. 60, no. 5, pp. 112–118, 2022.
19. H. Singh et al., "Blockchain Meets Edge AI in CRNs," IEEE Access, vol. 10, pp. 54422–54434, 2022.
20. F. Zhang et al., "Energy-Aware Smart Contracts for Spectrum Sensing," IEEE IoT Mag., vol. 3, no. 1, pp. 34–40, 2020.
21. R. Pathak et al., "AI-Based Defense Mechanisms in Wireless Systems," IEEE Sensors Letters, vol. 5, no. 2, 2023.
22. B. Singh et al., "LSTM-Based Malicious Detection in CRNs," IEEE VTC Spring, 2022.
23. S. Kim et al., "Decentralized Trust via Blockchain in Wireless Sensing," IEEE Access, vol. 9, pp. 93491–93502, 2021.
24. A. Arora et al., "Securing Spectrum Trading Using Blockchain," IEEE S&P Mag., vol. 19, no. 2, pp. 70–79, 2021.
25. N. Kandasamy et al., "Modeling CRN Trust Dynamics," IEEE Systems J., vol. 13, no. 3, pp. 2415–2424, 2021.
26. J. Liu et al., "Federated Learning for Trust in CRNs," IEEE TWC, vol. 20, no. 11, pp. 7256–7269, 2021.
27. V. Gupta et al., "Trust Propagation in CRNs: A Survey," IEEE Network, vol. 35, no. 1, pp. 76–82, 2021.
28. K. Hoang et al., "Blockchain + SWIPT in Cognitive IoT," IEEE JSAC, vol. 38, no. 12, pp. 2773–2785, 2020.
29. A. Singh et al., "Smart Contract-Driven Spectrum Access," IEEE TCCN, vol. 7, no. 2, pp. 427–440, 2021.
30. Z. Chen et al., "Adaptive Trust Management in Cognitive Wireless Networks," IEEE TMC, vol. 20, no. 7, pp. 2442–2456, 2021.