AI-Driven Fog Computing and Blockchain Security for Vehicular Networks

Research Proposal

Prepared by:

Muhammad Talha

Ateeq Ur Rehman

Supervised by:

Dr. Khushbu Khalid

Department of Computer Science & Information Technology

Lahore Garrison University

Lahore

April 14, 2025

Abstract

Vehicular Ad-Hoc Networks (VANETs) are increasingly vital to intelligent transportation systems but face significant security challenges. This research proposes an integrated security framework that combines Artificial Intelligence (AI), fog computing, and blockchain technology to address these vulnerabilities. The framework aims to leverage AI for real-time anomaly and intrusion detection, fog computing for low-latency processing near the network edge, and blockchain for secure, tamper-proof data transactions and authentication. Our methodology includes simulation-based experiments using NS-3 and Veins simulators, performance evaluation under various attack scenarios, and validation against real-world vehicular datasets. The expected outcomes include a novel architecture for VANET security, improved detection rates for security threats, reduced response latency through fog computing, and enhanced data integrity through blockchain integration. This research will contribute to the development of safer and more resilient intelligent transportation systems by addressing current security gaps in vehicular networks.

---

1. Introduction

1.1 Background

Vehicular Ad-Hoc Networks (VANETs) represent a critical component of Intelligent Transportation Systems (ITS), enabling communication between vehicles (V2V) and between vehicles and infrastructure (V2I). These communications support applications ranging from safety warnings and traffic management to infotainment services. However, the open nature of wireless communication channels, the high mobility of nodes, and the critical nature of transmitted information make VANETs particularly vulnerable to various security threats.

Traditional security mechanisms often fail to address the unique challenges posed by VANETs, including their dynamic topology, stringent latency requirements, and the potential severity of security breaches that could lead to life-threatening situations. Recent advances in AI, fog computing, and blockchain technologies offer promising approaches to enhance VANET security, but their integration remains largely unexplored.

1.2 Security Challenges in VANETs

VANETs face numerous security challenges, including:

- **Authentication and Privacy**: Ensuring that vehicles can be authenticated while preserving driver privacy.
- **Data Integrity and Confidentiality**: Protecting the integrity and confidentiality of transmitted data.
- **Availability**: Safeguarding against Denial-of-Service (DoS) attacks that could disrupt critical communications.
- **Non-repudiation**: Ensuring that vehicles cannot deny sending specific messages.
- **Real-time Response**: Meeting strict latency requirements for security mechanisms in safety-critical applications.
- **Scalability**: Handling security in large-scale networks with thousands of vehicles.

1.3 Emerging Technologies

Three key technologies show particular promise for addressing VANET security challenges:

Artificial Intelligence (AI): AI techniques, particularly machine learning and deep learning, can detect anomalies, identify intrusions, and predict potential threats in real-time.

Fog Computing: By extending cloud capabilities to the edge of the network, fog computing reduces latency and bandwidth usage, enabling faster security responses.

Blockchain Technology: Blockchain provides decentralized, tamper-proof data storage and transaction validation, which can enhance authentication, trust management, and data integrity in VANETs.

1.4 Research Motivation

While individual applications of AI, fog computing, and blockchain in VANET security have been explored, their integrated application remains underinvestigated. This research is motivated by the potential of

combining these technologies to create a comprehensive security framework that addresses multiple VANET security challenges simultaneously. By leveraging the strengths of each technology, we aim to develop a solution that offers enhanced security, privacy, and efficiency for vehicular networks.

---

2. Literature Review

2.1 Security Vulnerabilities and Attack Vectors in VANETs

VANETs are susceptible to various attacks that exploit their open wireless medium and distributed nature. Zeadally et al. (2019) provided a comprehensive analysis of security threats in VANETs, categorizing them into attacks on availability, authenticity, confidentiality, and data integrity. Their work highlighted the need for multi-layered security approaches to address these diverse threats.

Bukhari et al. (2021) examined emerging attack vectors in vehicular networks, identifying new threats such as machine learning-based attacks and GPS spoofing. Their research emphasized the evolving nature of security challenges in VANETs and the need for adaptive defense mechanisms.

Common attacks against VANETs include:

- **Denial-of-Service (DoS) Attacks**: Overloading communication channels to disrupt services.
- **Sybil Attacks**: Creating multiple fake identities to manipulate traffic data.
- **Eavesdropping and Privacy Attacks**: Unauthorized interception of sensitive information.
- **Man-in-the-Middle (MITM) Attacks**: Altering or intercepting communications between vehicles and infrastructure.
- **Black Hole and Gray Hole Attacks**: Dropping all or selected packets to disrupt communication.
- **Replay Attacks**: Retransmitting valid data to gain unauthorized access or disrupt services.

2.2 AI for Intrusion Detection, Anomaly Detection, and Threat Prediction

AI-driven techniques have shown significant promise for enhancing VANET security. Kaur et al. (2022) proposed a deep learning-based intrusion detection system that achieved high detection accuracy for various attack types. Their approach used convolutional neural networks (CNNs) to identify patterns associated with malicious activities in network traffic.

Alam et al. (2020) implemented a machine learning model for anomaly detection in VANETs, using supervised learning techniques to classify normal and abnormal behaviors. Their research demonstrated improved security performance compared to traditional threshold-based approaches.

Sharma and Verma (2023) developed an AI-based threat prediction framework that uses recurrent neural networks (RNNs) to forecast potential security breaches based on historical data patterns. Their approach enables proactive security measures rather than reactive responses.

Despite these advances, challenges remain in developing AI models that can operate effectively in the resource-constrained and highly dynamic environment of VANETs.

2.3 Role of Fog Computing in Enhancing Security and Reducing Latency

Fog computing extends cloud capabilities to the network edge, offering benefits for VANET security. Rahman et al. (2021) explored the integration of fog computing in VANETs for reducing response time in security threat detection. Their research demonstrated that fog-based security solutions could achieve response times suitable for safety-critical applications.

Chen et al. (2023) investigated privacy-preserving mechanisms in fog-based vehicular networks, proposing techniques for secure data processing at the edge while maintaining user privacy. Their work highlighted the potential of fog computing to balance security requirements with privacy concerns.

The distributed nature of fog computing aligns well with the distributed and mobile characteristics of VANETs, offering potential solutions for scalability and latency challenges in security implementations.

2.4 Blockchain for Secure Data Sharing, Authentication, and Trust Management

Blockchain technology provides a decentralized approach to security that aligns with the distributed nature of VANETs. Li et al. (2020) implemented a blockchain-based trust management system for VANETs to prevent identity spoofing and enhance message reliability. Their approach used a reputation mechanism stored on the blockchain to evaluate the trustworthiness of vehicles.

Singh and Choi (2022) proposed a decentralized authentication mechanism using blockchain to enhance vehicular communication security. Their solution eliminated the need for a central trusted authority while maintaining strong authentication guarantees.

While blockchain offers strong security properties, challenges remain regarding its implementation in VANETs, particularly concerning transaction throughput, consensus mechanism efficiency, and resource requirements.

2.5 Integration of AI, Fog Computing, and Blockchain for VANET Security

Recent research has begun exploring the integration of these technologies. Gupta et al. (2023) developed a hybrid security model combining AI, fog computing, and blockchain for real-time VANET protection. Their architecture used fog nodes for AI-based threat detection and blockchain for secure message dissemination.

Ahmed et al. (2024) proposed an integrated approach using federated learning, fog computing, and blockchain to enhance privacy and security in vehicular networks. Their framework enabled collaborative model training while preserving data privacy through blockchain-based incentive mechanisms.

Despite these initial efforts, there remains a significant research gap in developing comprehensive frameworks that effectively integrate all three technologies while addressing practical challenges related to performance, scalability, and resource constraints.

3. Problem Statement

Despite significant research in VANET security, existing solutions face limitations in addressing the complex and evolving security landscape of vehicular networks. Current approaches often focus on individual security aspects rather than providing comprehensive protection, resulting in fragmented solutions that fail to address the interconnected nature of VANET security challenges.

Specific research gaps include:

1. **Limited Integration**: While AI, fog computing, and blockchain have been applied individually to VANET security, their integrated implementation remains underexplored.
2. **Latency Challenges**: Many existing security solutions cannot meet the stringent latency requirements of safety-critical VANET applications.
3. **Scalability Issues**: Current security mechanisms often struggle to scale effectively in large-scale vehicular networks with thousands of nodes.
4. **Resource Constraints**: The computational and communication resources available in vehicular networks are limited, yet many security solutions assume abundant resources.
5. **Dynamic Threat Landscape**: Emerging attack vectors, including AI-driven attacks, require adaptive security solutions that can evolve with threats.
6. **Privacy-Security Balance**: Achieving a balance between robust security and user privacy remains challenging.

This research aims to address these gaps by developing an integrated security framework that leverages the complementary strengths of AI, fog computing, and blockchain technologies. The primary research question is: How can AI, fog computing, and blockchain be effectively integrated to create a comprehensive, efficient, and scalable security solution for vehicular networks?

---

4. Research Objectives

The overall aim of this research is to develop and evaluate an integrated security framework for VANETs that leverages AI, fog computing, and blockchain technologies. The specific objectives are:

1. **Framework Design**: To design a comprehensive security architecture that integrates AI, fog computing, and blockchain technologies for VANET protection.
   - *Deliverable*: Detailed architecture specifications and component interactions by Month 3.
2. **AI-Based Threat Detection**: To develop and optimize AI models for real-time detection of various attack types in VANETs.
   - *Deliverable*: AI models with detection accuracy above 95% for common attacks by Month 6.
3. **Fog Computing Integration**: To implement and evaluate a fog computing layer that reduces security response latency while optimizing resource usage.

- *Deliverable*: Fog computing implementation that reduces response latency by at least 60% compared to cloud-based solutions by Month 9.

4. **Blockchain Implementation**: To design and implement a blockchain-based mechanism for secure authentication and data integrity in VANETs.
   - *Deliverable*: Blockchain implementation that ensures data integrity with proof-of-concept for critical VANET messages by Month 12.
5. **System Integration**: To integrate the AI, fog computing, and blockchain components into a cohesive security framework.
   - *Deliverable*: Fully integrated system prototype by Month 15.
6. **Performance Evaluation**: To evaluate the performance, security effectiveness, and scalability of the integrated framework under various attack scenarios.
   - *Deliverable*: Comprehensive evaluation results demonstrating framework capabilities by Month 18.
7. **Real-World Validation**: To validate the framework using real-world vehicular datasets and scenarios.
   - *Deliverable*: Validation results using at least two real-world datasets by Month 21.

These objectives are designed to be Specific, Measurable, Achievable, Relevant, and Time-bound (SMART), with clear deliverables and timelines.

---

5. Proposed Methodology

5.1 Overall Approach

The research will follow a systematic approach that includes architecture design, component development, integration, and evaluation. We will use a combination of theoretical analysis, simulation experiments, and validation with real-world datasets.

5.2 System Architecture

The proposed integrated security framework consists of three main layers:

1. **AI Layer**: Responsible for threat detection, anomaly identification, and security intelligence.
2. **Fog Computing Layer**: Provides distributed processing capabilities near the network edge.
3. **Blockchain Layer**: Ensures secure data storage, authentication, and trust management.

![System Architecture Diagram]

5.2.1 AI Layer

The AI layer will incorporate:

- **Deep Learning Models**: Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) for pattern recognition in network traffic.
- **Ensemble Methods**: Combining multiple machine learning algorithms to improve detection accuracy.
- **Federated Learning**: Enabling collaborative model training while preserving data privacy.
- **Reinforcement Learning**: For adaptive security policy enforcement.

5.2.2 Fog Computing Layer

The fog computing layer will include:

- **Distributed Fog Nodes**: Deployed at roadside units (RSUs) and other edge locations.
- **Task Offloading Mechanisms**: To balance computational load among fog nodes.
- **Local Data Processing**: For real-time analysis of security-related data.
- **Hierarchical Processing**: With tasks distributed based on urgency and resource requirements.

5.2.3 Blockchain Layer

The blockchain layer will feature:

- **Lightweight Consensus Mechanism**: Optimized for vehicular networks' constraints.
- **Smart Contracts**: For automated security policy enforcement.
- **Decentralized Identity Management**: For secure vehicle authentication.
- **Immutable Logging**: For non-repudiable security event recording.

5.3 AI-Based Security Algorithms

5.3.1 Intrusion Detection System

We will develop a hybrid intrusion detection system combining:

- **Signature-Based Detection**: For known attack patterns.
- **Anomaly-Based Detection**: Using deep learning to identify deviations from normal behavior.
- **Specification-Based Detection**: Enforcing protocol compliance.

The proposed architecture will use a two-stage detection approach:

1. **Light Processing Stage**: Fast filtering of network traffic using optimized shallow neural networks.
2. **Deep Analysis Stage**: Comprehensive analysis of suspicious traffic using deeper models.

5.3.2 Threat Prediction and Mitigation

For proactive security, we will implement:

- **Time-Series Analysis**: Using LSTM (Long Short-Term Memory) networks to predict attack patterns.
- **Behavioral Analysis**: Modeling normal vehicle behavior to detect anomalies.
- **Graph-Based Analysis**: Examining network topology changes indicative of attacks.

5.4 Fog Computing Implementation

Fog computing will be implemented with the following components:

- **Dynamic Resource Allocation**: Adapting processing distribution based on network conditions.
- **Security Function Virtualization**: Enabling flexible deployment of security functions.
- **Collaborative Processing**: Coordinating security tasks across multiple fog nodes.
- **Edge-Cloud Continuum**: Seamless integration with cloud resources for complex analyses.

5.5 Blockchain Implementation

The blockchain component will include:

- **Modified Proof-of-Authority**: A consensus mechanism suitable for VANET environments.
- **Hierarchical Structure**: With different block types for different security functions.
- **Certificate Management**: For secure key distribution and management.
- **Reputation System**: To evaluate the trustworthiness of network participants.

5.6 Simulation and Evaluation

5.6.1 Simulation Environment

We will use a comprehensive simulation environment combining:

- **Network Simulation**: Using NS-3 and Veins simulators for realistic VANET modeling.
- **Traffic Simulation**: Using SUMO (Simulation of Urban Mobility) for realistic vehicle movement patterns.
- **Security Attack Simulation**: Implementing various attack vectors to test defense mechanisms.

5.6.2 Performance Metrics

The framework will be evaluated using the following metrics:

- **Security Effectiveness**:
  - Detection accuracy, precision, recall, and F1-score
  - False positive and false negative rates
  - Attack detection latency
- **Operational Performance**:
  - End-to-end latency for security operations

- Computational overhead
- Communication overhead
- Scalability with increasing network size

- **Blockchain Performance**:
  - Transaction throughput
  - Consensus latency
  - Storage requirements

5.6.3 Validation Approach

Validation will be performed using:

- **Synthetic Datasets**: Generated through simulation with controlled parameters.
- **Real-World Datasets**: Including the VeReMi dataset for misbehavior detection and the DARPA intrusion detection dataset adapted for vehicular networks.
- **Hardware-in-the-Loop Testing**: Using small-scale testbeds with actual communication devices.

5.7 Implementation Plan

The implementation will follow these stages:

1. **Component Development**: Developing individual AI, fog computing, and blockchain components.
2. **Component Integration**: Integrating the three technologies into a cohesive framework.
3. **Prototype Development**: Creating a proof-of-concept implementation.
4. **Testing and Evaluation**: Comprehensive evaluation under various scenarios.
5. **Refinement**: Iterative improvement based on evaluation results.

---

6. Expected Outcomes and Contributions

This research is expected to produce the following outcomes and contributions:

6.1 Theoretical Contributions

1. **Integrated Security Model**: A novel theoretical framework for combining AI, fog computing, and blockchain in VANET security.
2. **Security Analysis Framework**: A methodology for analyzing the security properties of integrated AI-fog-blockchain systems.
3. **Threat Taxonomy**: An updated taxonomy of VANET security threats and appropriate countermeasures using advanced technologies.
4. **Performance Models**: Mathematical models for predicting the performance of security mechanisms in various VANET scenarios.

6.2 Technical Contributions

1. **Security Architecture**: A comprehensive security architecture that integrates AI, fog computing, and blockchain for VANETs.
2. **AI Models**: Optimized deep learning and machine learning models for VANET security threat detection.
3. **Fog Computing Algorithms**: Resource-efficient algorithms for security processing at the network edge.
4. **Blockchain Protocols**: Lightweight blockchain protocols tailored for vehicular network constraints.
5. **Integration Mechanisms**: Novel methods for integrating the three technologies with minimal overhead.

6.3 Practical Contributions

1. **Software Prototypes**: Proof-of-concept implementations of the key components of the security framework.
2. **Simulation Modules**: Extensions to existing simulation tools for evaluating integrated security solutions.
3. **Best Practices**: Guidelines for implementing secure vehicular networks using the proposed framework.
4. **Deployment Strategies**: Methods for incremental deployment of the security framework in existing infrastructure.

6.4 Expected Improvements

1. **Enhanced Security**: Significant improvement in detection rates for common VANET attacks.
2. **Reduced Latency**: Lower response times for security mechanisms, meeting the requirements of safety-critical applications.
3. **Improved Scalability**: Better performance in large-scale networks compared to existing approaches.
4. **Resource Efficiency**: Lower computational and communication overhead for security mechanisms.
5. **Privacy Preservation**: Enhanced privacy protection while maintaining strong security guarantees.

---

7. Research Timeline

The research will be conducted over a 24-month period, with the following timeline:

Phase	Activities	Timeline	Milestones
Phase 1: Background and Design	Literature review Architecture design Requirement analysis	Months 1-3	M1: Literature review completed M2: Architecture design document
Phase 2: AI Component Development	Dataset preparation Model development Model optimization	Months 4-6	M3: AI models developed M4: AI evaluation report
Phase 3: Fog Computing Implementation	Fog node design Task allocation algorithms Edge processing implementation	Months 7-9	M5: Fog computing prototype M6: Fog performance report
Phase 4: Blockchain Development	Consensus mechanism design Smart contract development Security policy implementation	Months 10-12	M7: Blockchain prototype M8: Blockchain evaluation report
Phase 5: System Integration	Component integration Interface development System-level testing	Months 13-15	M9: Integrated system prototype M10: Integration testing report
Phase 6: Evaluation and Validation	Performance evaluation Security assessment Comparison with existing approaches	Months 16-18	M11: Comprehensive evaluation results M12: Comparative analysis report
Phase 7: Real-world Validation	Real dataset validation Case studies Refinement based on validation	Months 19-21	M13: Validation results M14: Case study reports
Phase 8: Documentation and Dissemination	Documentation completion Research paper preparation Final report compilation	Months 22-24	M15: Final framework documentation M16: Research papers M17: Final research report

---

8. Research Challenges and Mitigation Strategies

We anticipate several challenges in this research and have developed mitigation strategies:

Challenge	Mitigation Strategy
AI Model Complexity vs. Resource Constraints	Develop lightweight models using techniques like knowledge distillation and model compression.
Blockchain Scalability Issues	Implement sharding and hierarchical blockchain structures to improve transaction throughput.
Fog Node Reliability	Design fault-tolerant mechanisms with dynamic task reassignment capabilities.
Integration Complexity	Use a modular design approach with well-defined interfaces between components.
Realistic Evaluation	Combine simulation with hardware-in-the-loop testing and real-world datasets.
Privacy Concerns	Implement privacy-preserving techniques such as differential privacy and secure multi-party computation.

---

9. Ethical Considerations

This research will adhere to ethical principles in cybersecurity research:

1. **Privacy Protection**: Ensuring that any data used in the research is properly anonymized and protected.
2. **Responsible Disclosure**: Following responsible disclosure practices for any vulnerabilities discovered during the research.
3. **Dual-Use Considerations**: Being mindful of the potential dual-use nature of security research and implementing appropriate safeguards.
4. **Resource Consumption**: Designing solutions that minimize environmental impact through efficient resource usage.
5. **Accessibility**: Ensuring that security solutions do not create barriers to access for individuals with disabilities.

---

10. References

1. Zeadally, S., Hunt, R., Chen, Y. S., Irwin, A., & Hassan, A. (2019). "A Survey on Security Threats and Countermeasures in VANETs." IEEE Communications Surveys & Tutorials, 21(2), 1107-1127.
2. Bukhari, S. H. R., Shanmugam, B., Alias, A. S., & Anuar, N. B. (2021). "Emerging Attack Vectors and Security Solutions for Vehicular Networks." Elsevier Computers & Security, 105, 102258.
3. Kaur, H., Singh, G., & Minhas, J. (2022). "Deep Learning-Based Intrusion Detection in VANETs." Springer Wireless Networks, 28(3), 1245-1263.

4. Alam, T., Qamar, S., Dixit, A., & Benaida, M. (2020). "Machine Learning for Anomaly Detection in Vehicular Networks." IEEE Transactions on Intelligent Transportation Systems, 22(9), 5787-5798.
5. Sharma, V., & Verma, A. K. (2023). "AI-Driven Threat Prediction in Vehicular Cybersecurity." ScienceDirect Future Generation Computer Systems, 138, 62-75.
6. Rahman, A., Islam, M. K., Munim, Z. H., & Saha, S. (2021). "Fog Computing for Secure VANET Communication." ACM Transactions on Internet Technology, 21(4), 1-22.
7. Chen, L., Lee, W. C., Chang, C. C., & Chan, K. S. (2023). "Privacy-Preserving Mechanisms in Fog-Based Vehicular Networks." Elsevier Computer Networks, 222, 109440.
8. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). "Blockchain-Based Trust Management in VANETs." IEEE Transactions on Vehicular Technology, 69(6), 5908-5923.
9. Singh, M., & Choi, Y. (2022). "Decentralized Authentication Using Blockchain for Secure Vehicular Networks." Springer Journal of Supercomputing, 78(1), 1-25.
10. Gupta, R., Tanwar, S., Kumar, N., & Guizani, M. (2023). "Hybrid AI-Fog-Blockchain Security Model for VANETs." Elsevier Journal of Network and Computer Applications, 207, 103502.
11. Ahmed, Z., Malik, M. B., Khan, M. A., & Qadir, J. (2024). "Federated Learning and Blockchain for Privacy-Enhanced Vehicular Security." IEEE Transactions on Dependable and Secure Computing, 21(1), 421-435.
12. Hasrouny, H., Samhat, A. E., Bassil, C., & Laouiti, A. (2022). "VANETs Security Challenges and Solutions: A Survey." Vehicular Communications, 7, 7-20.
13. Yang, F., Wang, S., Li, J., Liu, Z., & Sun, Q. (2021). "An Overview of Internet of Vehicles." China Communications, 11(10), 1-15.
14. Kumar, S., & Lim, H. (2023). "Lightweight Authentication Scheme for VANETs Using Fog Computing and Blockchain." IEEE Access, 11, 45876-45890.
15. Liu, Y., Lu, Y., & Li, X. (2022). "A Comprehensive Survey on Blockchain-Enabled IoV Technologies." IEEE Communications Surveys & Tutorials, 24(2), 829-867.
16. Zhang, J., Chen, X., Xiang, Y., Zhou, W., & Wu, J. (2023). "Secure and Privacy-preserving Data Sharing in VANETs: A Survey." IEEE Communications Surveys & Tutorials, 25(3), 1844-1878.
17. Hu, P., Ning, H., Qiu, T., Song, H., Wang, Y., & Yao, X. (2020). "Security and Privacy Preservation Scheme of Face Identification and Resolution Framework Using Fog Computing in Internet of Things." IEEE Internet of Things Journal, 4(5), 1143-1155.
18. Taher, K. A., Naik, T., & Rafiq, A. (2021). "Security and Privacy Challenges in Connected Vehicles and the Role of AI." IEEE Access, 9, 10466-10483.
19. Poularakis, K., Iosifidis, G., & Tassiulas, L. (2022). "Joint Optimization of Task Assignment and Resource Allocation in Edge Computing Systems." IEEE Transactions on Cloud Computing, 10(4), 2568-2583.
20. Wang, L., Liu, G., & Sun, L. (2022). "A Secure and Privacy-Preserving Navigation Scheme Using Spatial Crowdsourcing in Fog-Based VANETs." Sensors, 17(4), 668-682.