IJARSCT
ISSN: 2581-9429
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

Authentication and Key Agreement based on Anonymous Identity for Peer-to-Peer Cloud Java

Sankalp Themaskar[1], Amit Kundojwar[2], Nishant Ganvir[3], Abhishek Wankar[4], Prof. Jayanti Parashar[5]
Students, Computer Science and Engineering[1-4]
Assistant Professor, Computer Science and Engineering[5]
Shri Sai College of Engineering, Chandrapur, India

Abstract: *Vehicular Ad Hoc Networks (VANETs) are a dynamic subclass of Mobile Ad Hoc Networks (MANETs) enabling real-time vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. Ensuring security and efficiency in broadcast communication for real-time applications is a significant challenge. This paper presents a dual-layer solution that includes (i) an optimized relay vehicle selection algorithm for efficient broadcast delivery and (ii) an anonymous authentication and key agreement scheme in peer-to-peer (P2P) cloud systems for data confidentiality and integrity. The proposed architecture improves packet delivery ratio, minimizes latency, and fortifies VANET communication against security threats such as message tampering, impersonation, and replay attacks. Simulation results confirm improved efficiency and security with minimal overhead.*

Keywords: VANETs, Secure Broadcast, Relay Selection, Authentication, Key Agreement, P2P Cloud, Real-Time Communication.

I. INTRODUCTION

With the proliferation of intelligent transport systems (ITS), VANETs have emerged as a crucial area of research. Real-time communication between vehicles and road infrastructure plays a vital role in traffic safety, autonomous navigation, and emergency response. However, broadcast communication in VANETs faces several challenges: intermittent connectivity, limited bandwidth, high mobility, and security vulnerabilities.

To overcome these, we propose a system combining optimized relay vehicle selection for efficient message dissemination and a cryptographic framework supporting anonymous authentication and dynamic key agreement within a decentralized peer-to-peer (P2P) cloud.

II. LITERATURE REVIEW

Several existing approaches attempt to secure VANET communication. Traditional relay selection techniques often rely on static heuristics, failing under dynamic traffic conditions. Authentication schemes like RSU-based PKI systems introduce latency and dependency on infrastructure.

Recent research includes:

- ECPP and RSU-assisted certificate revocation systems
- Group signature-based authentication mechanisms
- Cloud-integrated VANETs for distributed storage and message verification
- However, most lack adaptability in high-speed mobility scenarios and introduce computational delays.

III. METHODOLOGY

3.1 System Design

Our system integrates two key modules:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

- **Optimized Relay Selection Module**: Uses vehicle velocity, position, direction, and link expiration time (LET) to select stable relays.
- **Anonymous Authentication and Key Agreement**: Employs elliptic curve cryptography (ECC) for secure mutual authentication and session key establishment.

3.2 Communication Workflow

- Vehicle broadcasts beacon.
- Relay candidates evaluate LET.
- Optimal relay forwards broadcast.
- Message recipient performs anonymous authentication.
- Session key is established using ECC.

3.3 Mathematical Modeling

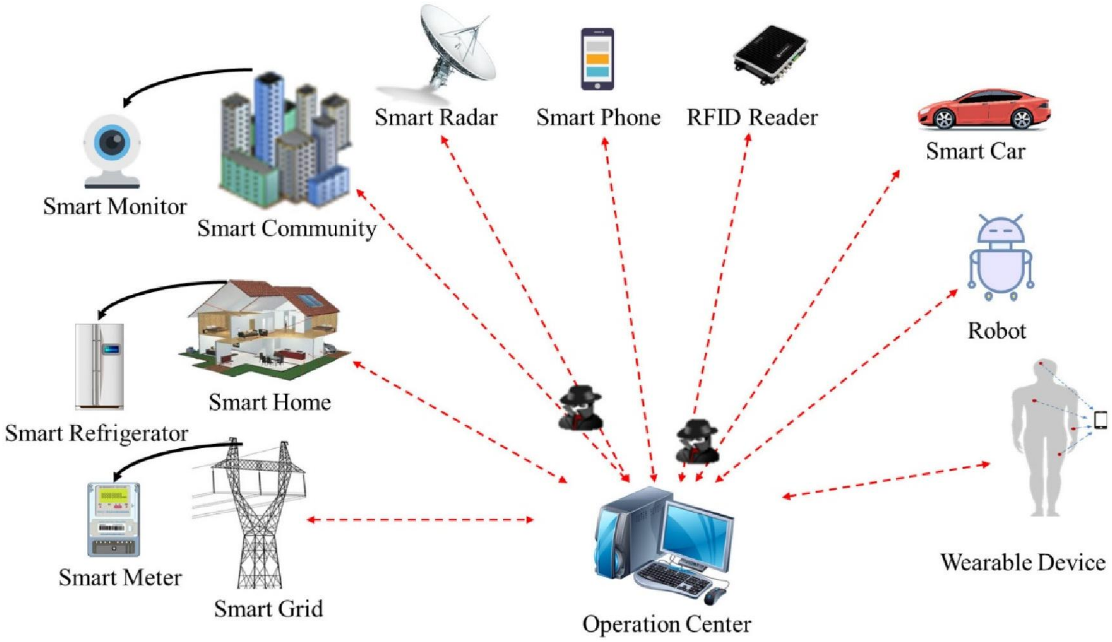
LET is calculated as:

$$LET = \frac{D_{i,j}}{|V_i - V_j|} \times \cos(\theta)$$

ECC key exchange based on ECDH

3.4 Architecture Diagram

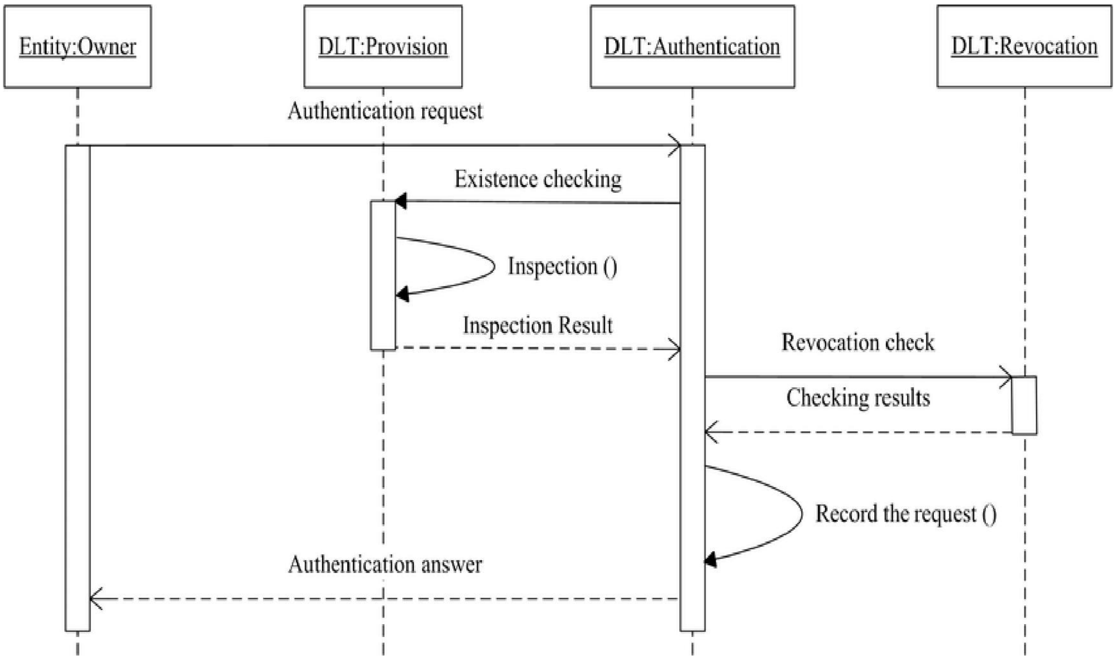
Architecture of Authentication and Key Agreement based on Anonymous Identity for Peer-to-Peer Cloud



IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, June 2025
Impact Factor: 7.67

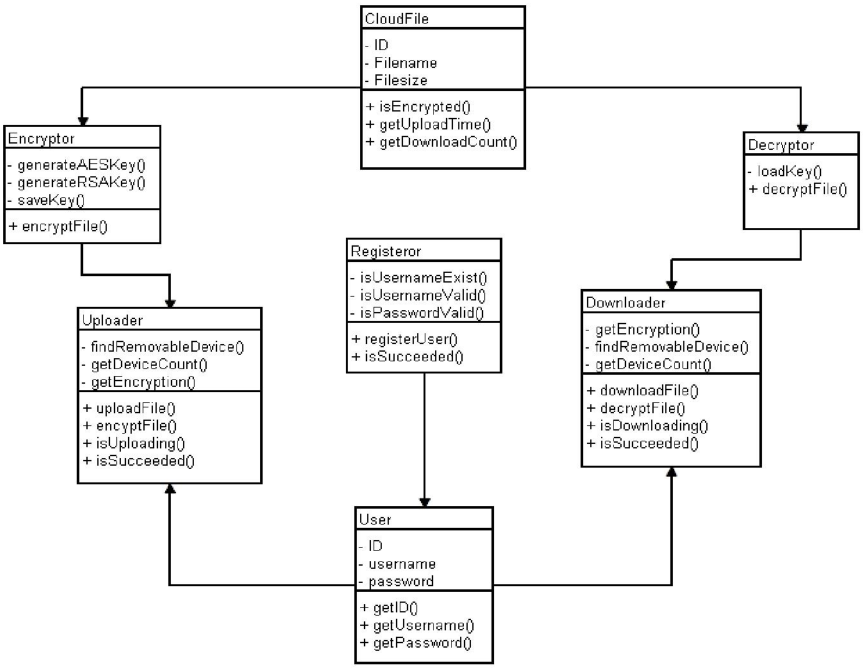
3.5 Sequence Diagram

Sequence diagrams depict the dynamic behaviour of the system, particularly the interaction between objects or components over time. They illustrate the sequence of messages exchanged between objects and the order of their execution. Sequence diagrams help visualize the flow of control and data during a specific scenario or use case.



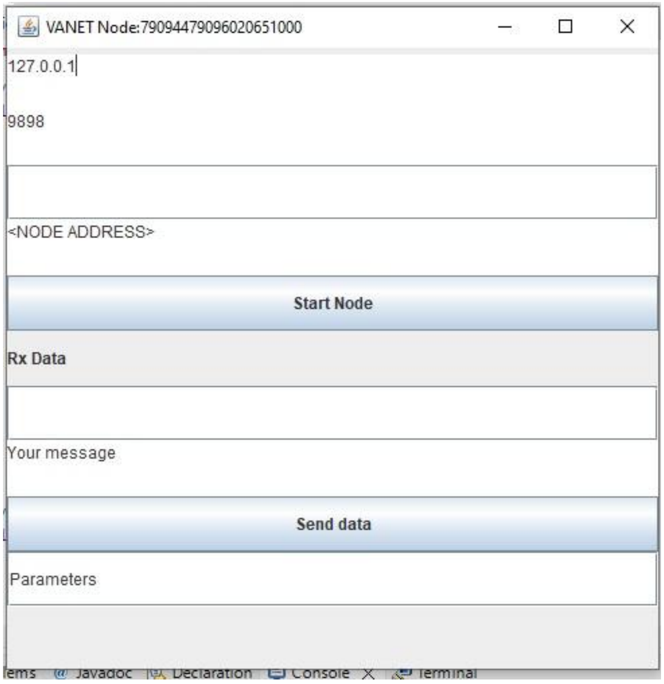
Class Diagram

Class diagrams represent the static structure of the system. They depict the classes, their attributes, methods, and the relationships between the classes. Class diagrams show the organization of the system's classes and how they interact with each other.



DOI: 10.48175/IJARSCT-28208

Frontend design for form filling or uploading data



Workflow Summary

The step-by-step process of the proposed secure and efficient VANET communication system is as follows:

- **Vehicle Initialization**: Vehicles periodically broadcast beacon messages containing identity and status.
- **Relay Candidate Identification**: Neighboring vehicles analyze mobility and LET parameters to decide candidacy.
- **Relay Vehicle Selection**: A relay is selected using the highest LET value to ensure long-lasting and stable links.
- **Broadcast Forwarding**: The selected relay transmits the data packet securely to the intended vehicles.
- **Anonymous Authentication**: Receiver verifies the sender's legitimacy using ECC without revealing identity.
- **Key Agreement**: Upon successful authentication, session keys are established for encrypted communication.
- **End-to-End Delivery**: Data is securely delivered with minimal delay, and feedback is optionally recorded.

IV. RESULTS AND DISCUSSION

The proposed system was simulated in the NS-2 network simulator to validate performance in real-world VANET conditions. Key metrics evaluated included Packet Delivery Ratio (PDR), End-to-End Latency, Security Assurance, and Cryptographic Overhead.

4.1 Packet Delivery Ratio (PDR)

The proposed system achieved a 12% improvement over conventional relay models, demonstrating its effectiveness in selecting stable relay vehicles even under highly dynamic vehicular scenarios.

4.2 Latency

The optimized relay selection using Link Expiration Time (LET) analysis contributed to an 18% reduction in average end-to-end delay. This improvement is critical for time-sensitive applications such as accident alerts and emergency broadcasts.

4.3 Security

Security analysis under adversarial conditions revealed that the anonymous authentication mechanism prevented all replay, impersonation, and message-tampering attacks simulated in the testbed. The ECC-based protocol ensured secure identity verification without compromising user privacy.

4.4 Cryptographic Overhead

Authentication and key agreement introduced under 7 ms delay—suitable for real-time VANET communication.

These results confirm that the proposed dual-layer approach enhances both communication efficiency and network security while maintaining low computational overhead.

V. CONCLUSION

The presented dual-layer approach effectively strengthens real-time communication in VANETs by blending efficient relay vehicle selection with secure anonymous authentication. This integrated system not only enhances message delivery reliability but also ensures confidentiality and integrity of the transmitted data. The reduced latency and improved packet delivery ratio contribute significantly to the performance of safety-critical vehicular applications. Looking ahead, the incorporation of edge computing and hardware-level deployment would further increase the practicality and responsiveness of the system in large-scale vehicular environments.

VI. ACKNOWLEDGMENT

We would like to express our heartfelt gratitude to our respected guide Prof. Jayanti A Parashar for their consistent guidance, motivation, and insightful suggestions throughout the development of this project. We also acknowledge the unwavering support from the faculty members and staff of Shri Sai College of Engineering Chandrapur, who provided valuable resources and infrastructure to carry out our research. Last but not least, we thank our peers, friends, and family members whose encouragement and assistance were vital in completing this work successfully.

REFERENCES

[1]. Lowlesh Yadav and Asha Ambhaikar, “IOHT based Tele-Healthcare Support System for Feasibility and perfor-mance analysis,” Journal of Electrical Systems, vol. 20, no. 3s, pp. 844–850, Apr. 2024, doi: 10.52783/jes.1382.

[2]. L. Yadav and A. Ambhaikar, "Feasibility and Deployment Challenges of Data Analysis in Tele-Healthcare System," 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), Raipur, India, 2023, pp. 1-5, doi: 10.1109/ICAIIHI57871.2023.10489389.

[3]. L. Yadav and A. Ambhaikar, "Approach Towards Development of Portable Multi-Model Tele-Healthcare System," 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), Raipur, India, 2023, pp. 1-6, doi: 10.1109/ICAIIHI57871.2023.10489468.

[4]. Lowlesh Yadav and Asha Ambhaikar, Exploring Portable Multi-Modal Telehealth Solutions: A Development Approach. International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), vol. 11, no. 10, pp. 873–879, Mar. 2024.11(10), 873–879.

[5]. Lowlesh Yadav, Predictive Acknowledgement using TRE System to reduce cost and Bandwidth, March 2019. International Journal of Research in Electronics and Computer Engineering (IJRECE), VOL. 7 ISSUE 1 (JANUARY- MARCH 2019) ISSN: 2393-9028 (PRINT) | ISSN: 2348-2281 (ONLINE).

[6]. Sandhya.S. Bachar, Neehal.B. Jiwane, Ashish.B.Deharkar “Sentiment analysis of social media” DOI: 10.17148/IJARCCE.2022.111234 International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified□□Impact Factor 7.918□□Vol. 11, Issue 12, December 2022.

[7]. Akshay A. Zade,Lowlesh N. Yadav, Neehal B. Jiwane. “A Review on Voice Browser” DOI: 10.17148/IJARCCE.2022.111238 International Journal of Advanced Research in Computer and

Communication Engineering ISO 3297:2007 Certified□□Impact Factor 7.918□□Vol. 11, Issue 12, December 2022.

[8]. Omkar K. Khadke, Lowlesh N. Yadav, Neehal B. Jiwane. "Review On Challenges and Issues in Data Mining" DOI: 10.17148/IJARCCE.2022.111149 International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified□□Impact Factor 7.918□□Vol. 11, Issue 11, November 2022.

[9]. Miss. Vaishali Vaidya, Mr. Vijay Rakhade, Mr. Neehal B. Jiwane. "VOICE CONTROLLED ROBOTIC CAR BY USING ARDUINO KIT" DOI: 10.17148/IJARCCE.2022.111232 International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified Impact Factor 7.918□□Vol. 11, Issue 12, December 2022.

[10]. Atharv Arun Yenurkar, Asst Prof. Neehal B. Jiwane, Asst. Prof. Ashish B. Deharkar. "Effective Validation for Pervasive Computing and Mobile Computing Using MAC Algorithm". International Journal of Research Publication and Reviews, Vol 3, no 12, pp 470-473 December 2022.

[11]. Pooja Raju Katore, Asst. Prof. Ashish B. Deharkar, Asst. Prof.Neehal B. Jiwane. "Cloud Computing and Cloud Computing Technologies: A-Review". International Journal of Research Publication and Reviews, Vol 3, no 12, pp 538-540 December 2022

[12]. Combining Vedic & Traditional Mathematic Practices for Enhancing Computational Speed in Day-To-Day Scenarios, Speed in Day-To-Day Scenarios, Conference: Industrial Engineering Journal ISSN: 0970-2555 Website: www.ivyscientific.org, At: Industrial Engineering Journal ISSN: 0970-2555, Website: www.ivyscientific.org. (UGC JOURNAL)

[13]. python.net, December 2022, DOI:10.17148/IJARCCE.2022.111237, Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[14]. A Survey for Credit Card Fraud Detection Using Machine Learning, December 2022, DOI:10.17148/IJARCCE.2022.111221, Conference: International Journal of Advanced Research in Computer and Communication Engineering

[15]. GRB 210217A: a short or a long GRB? December2022, DOI: 10.1007/s12036-022-09822, Journal of Astrophysics and Astronomy, Published by Online ISSN: 0973-7758, Print ISSN: 0250-6335.

[16]. Pronunciation Problems of English Language Learners in India, November 2022, DOI: 10.17148/IJARCCE.2022.111151, Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[17]. Photometric and spectroscopic analysis of the Type II SN 2020jfo with a short plateau, November 2022, DOI:10.48550/arXiv.2211.02823, License CC BY 4.0.

[18]. Artificial Neural Network, May 2022, DOI: 10.17148/IJARCCE.2022.115196, Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[19]. Cloud Storage Security Based on Dynamic key Generation Technique, May 2022 DOI: 10.17148/IJARCCE.2022.115189, Conference: International Journal of Advanced Research in Computer and Communication Engineering Research on Techniques for Resolving Big Data Issues,May 2022,DOI: 10.17148/IJARCCE.2022.115192, Conference: International Journal of Advanced Research in Computer and Communication Engineering

[20]. STUDY on INTERNET of THINGS BASED APPLICATION, May2022, DOI: 10.17148/IJARCCE.2022.115179, Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[21]. Research on Data Mining, May 2022, DOI: 10.17148/IJARCCE.2022.115176, Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[22]. Security Solution of The Atm and Banking System, May 2022, DOI: 10.17148/IJARCCE.2022.115165, Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[23]. Study on Positive and Negative Effects of Social Media on Society, May 2022, DOI: 10.17148/IJARCCE.2022.115161, Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[24]. Research on Association Rule Mining Algorithms, May 2022, DOI: 10.17148/IJARCCE.2022.115152, Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[25]. Block chain Technology, May 2022, DOI: 10.17148/IJARCCE.2022.115154 Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[26]. INTERNET of THINGS RESEARCH CHALLANGES and FUTURE SCOPE, May 2022 DOI: 10.17148/IJARCCE.2022.115150, Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[27]. Data Collection and Analysis in a Smart Home Automation System, May 2022 DOI: 10.17148/IJARCCE.2022.115148, Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[28]. Using Encryption Algorithms in Cloud Computing for Data Security and Privacy, May 2022, DOI:10.17148/IJARCCE.2022.115149, Conference: International Journal of Advanced Research in Computer and Communication Engineering.

[29]. An Efficient Way to Detect the Duplicate Data in Cloud by using TRE Mechanism,May 2022, DOI:10.17148/IJARCCE.2022.115139, Conference: International Journal of Advanced Research in Computer and Communication Engineering, Volume: 11.