**A PRIVACY-CONSERVING FRAMEWORK FOR AN EFFECTIVE DATA DISTRIBUTION IN VEHICULAR NETWORK**

*Report submitted to the SASTRA Deemed to be University*

*as the requirement for the course*

BCSCCS708: **MINI PROJECT**

*Submitted by*

**Girijasree D M**

**(Reg. No.: 121003094, B. Tech CSE)**

**Dasari Bangaru Sindhu**

**(Reg. No.: 121003072, B. Tech CSE)**

**Dayala Badrinadh Reddy**

**(Reg. No.: 121003073, B. Tech CSE)**

**December 2021**



**SCHOOL OF COMPUTING**

**THANJAVUR, TAMIL NADU, INDIA – 613 401**



**SCHOOL OF COMPUTING**

**THANJAVUR – 613 401**

**Bonafide Certificate**

This is to certify that the report titled “A Privacy-Conserving Framework for an Effective Data Distribution in Vehicular Network” submitted as a requirement for the course, BCSCCS708: **MINI PROJECT** for B.Tech. is a bonafide record of the work done by **Ms. Dasari Bangaru Sindhu (Reg. No.121003072, B. Tech CSE), Mr. Dayala Badrinadh Reddy (Reg. No.121003073, B. Tech CSE), Ms. Girijasree D M (Reg. No.121003094, B. Tech CSE)** during the academic year 2020-21, in the School of Computing, under my supervision.

**Signature of Project Supervisor :**

**Name with Affiliation :**

**Date :**

Mini Project *Viva voce* held on \_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Examiner 1 Examiner 2**

**ABSTRACT**

Vehicular networks (VN) are result of advancements in automobile Industry, wireless technologies and ad-hoc networking. In recent years, Vehicular network has become vulnerable because of interference of unethical and unreliable vehicular nodes. The role of data in vehicular network is vital to carry communication between vehicular nodes and Road Side Units (RSU). It faces some privacy and security threats because of hindrance of malicious vehicular nodes, which should be addressed and solved in a proper way. RSU play many roles such as data disseminators, identifying the accurate location of servers, managing the security and traffic flow in VANET.

In order to mitigate threats posed, an effective privacy-preserving data query and dissemination approach (EPDQD) is proposed. Bilinear pairings and Chinese Remainder Theorem combined together to provide a secured framework for data distribution in VANET. Bilinear pairings (a pairing based cryptographic technique) is used to secure data query request and Chinese Remainder theorem to recover those queries safely. EPDQD comprises of key factors such as a) Confidentiality b) Non-interactive secure session key c) Message authentication code d) Authentication of data query requests e) Data integrity of data transmission. The proposed EPDQD outperforms other algorithms like TRAD, PVQS by providing less computational complexity value and communication overhead.

**KEY WORDS:** VANET, Data Query, Data Distribution, Privacy-Preserving, Cryptographic techniques

**Table of Contents**

|  |  |
| --- | --- |
| **Title** | **Page No.** |
| Bonafide Certificate | 2 |
| Abstract | 3 |
| List of Figures |  |
| List of Tables |  |
| Abstract |  |
| 1. Summary of the base paper |  |
| 1. Merits and Demerits of the base paper |  |
| 1. Source Code |  |
| 1. Snapshots |  |
| 1. Conclusion and Future Plans |  |
| 1. References |  |
| 1. Appendix -Base Paper |  |