**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*

**Dasari Bangaru Sindhu**

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

**Dayala Badrinadh Reddy**

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

**Girijasree D M**

**(Reg. No.: 121003094, 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**

**ACKNOWLEDGEMENTS**

First of all, we express our gratitude to Dr. S. Vaidhyasubramaniam, Vice Chancellor, SASTRA Deemed University, who provided all facilities and necessary encouragement during the course of our study. We extend our sincere thanks to Prof. R. Chandra Mouli, Registrar, SASTRA Deemed University for providing the opportunity to pursue this project. It is our privilege to express our sincerest regards to our project coordinator, Prof. Umamakeswari A, Dean (SOC), CSE Associate Dean who motivated us during the project.

We owe a debit of deepest gratitude to our mentor Dr. R S Raghav for his valuable inputs, able guidance, encouragement, whole-hearted cooperation and constructive criticism throughout the duration of our project on the topic ‘A Privacy-Conserving Framework for an Effective Data Distribution in Vehicular Network’. We take this opportunity to thank all our lecturers who have directly or indirectly helped our project.

**Table of Contents**

|  |  |
| --- | --- |
| **Title** | **Page No.** |
| Bonafide Certificate | i |
| Acknowledgements | ii |
| Table of Contents | iii |
| List of Figures | iv |
| List of Tables | v |
| Abbreviations | vi |
| Notations | vii |
| Abstract | viii |
| 1. Summary of the base paper | 1 |
| 1. Merits and Demerits of the base paper | 3 |
| 1. Source Code | 5 |
| 1. Snapshots | 14 |
| 1. Conclusion and Future Plans | 17 |
| 1. References | 18 |
| 1. Appendix - Base Paper | 19 |

**List of Figures**

**ABBREVATIONS**

|  |  |
| --- | --- |
| CCM | Centre Cloud Manger |
| RSU | Road Side Unit |
| VN | Vehicular Network |
| EPDQD | Efficient Privacy-Preserving Data Query and Dissemination Scheme |
| PVQS | Privacy-Preserving and Verifiable Querying Scheme |
| TRAD | Traditional Scheme |
| CRT | Chinese Remainder Theorem |
| RLC | Reputation Label Certificate |
| IBS | Identity Based Signature |
| MAC | Message Authentication Code |

**NOTATIONS**

**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

**Summary of the Base Paper**

|  |  |
| --- | --- |
| Title | An efficient privacy-preserving data query and dissemination scheme in vehicular cloud |
| Journal | Pervasive and Mobile Computing |
| Publisher | ELSEVIER |
| Year | 2020 |
| Indexed in | Scopus / SCI |

This study mainly concerns about protecting privacy of the users who use vehicular networks in the evolving technological world. (Vehicular networks are major advancements in network and automobile industry). The major components of vehicular network are Central Cloud Manager (CCM), Road Side Unit (RSU) and Vehicles. When a vehicle enters the road the Central Cloud Manager (CCM) they get registered with it and the public parameters of the vehicles are maintained by the CCM. The Central Cloud Manager computes all the public parameters and delivers them securely to the vehicles. The approach provided in this study is Efficient Privacy-Preserving Data Query and Dissemination (EPDQD) which helps protect the privacy of users. With the increase in vehicular networks there is chance of threat imposed on the privacy of vehicle users who query the Road Side Unit (RSU) for any data. When user queries the RSU, it will authenticate the user for providing data. When RSU gets compromised, the credentials of the user might be at risk and there is chance for the crime. The approach provided in this study will help mitigate the threat posed to vehicle owners. In this approach the vehicles’ details are maintained by the trusted party CCM. When vehicle registers with CCM the public and private key of vehicles and RSU is computed by CCM and are delivered to them securely by using encryption scheme. The vehicles which have same destination forms vehicular cloud, the vehicles try to query RSU. After the formulation of query group, the vehicles query RSU simultaneously. Since it is not possible for all vehicles to query simultaneously, the vehicle which wants to query RSU sends a co-operation request to other vehicles in the cloud. When other vehicles accept co-operation request that vehicle forms a secure session with the vehicles that accepted the request. The vehicle computes secure key and delivers it to the vehicles using encryption. The vehicles query RSU at a time and when RSU receives the queries it aggregates the query requests and answers all of them. After the query request aggregation, the RSU replaces the query with the requested data and sends the data as aggregate. The vehicles then take the data for which they have queried. Here Bilinear Pairing and Chinese Remainder Theorem (CRT) are used for computing secure session key and generating secure key for query parameters. With the use of Bilinear Pairing and Chinese Remainder Theorem we achieve unlinkability and the origin of the user remains unknown. With this approach we protect the privacy of user. The use of Bilinear pairing achieves less computational complexity and will be much helpful when the traffic increases and maintaining vehicles.

**Merits and Demerits**

**Existing methods:**

To solve the threats that arise in Vehicular networks as mentioned earlier, few techniques were developed over time which have their own pros and cons.

1. Pseudonym technology:

Pseudonym technology aids in maintaining the user anonymity while letting the user to perform the task uninterruptedly. It is a way of providing an alias or a substitute to the original identity of the user. In schemes based on this technology vehicles will change their pseudonyms frequently in some specified fashion. In the paper ‘An RSU-aided distributed trust framework for pseudonym-enabled privacy preservation in VANETs’, a distributed trust framework is presented in which RSU allots ‘Reputation Label Certificate (RLC)’ for every vehicle to measure how reliable the message is. Whether the security and privacy of the vehicle should be conserved or not depends on its RLC which will be stored in a common database.

Despite of using pseudonym technology, it is still possible to link the changing pseudonym to the vehicle in some untimely events. Suppose, when a group of vehicles are moving on the road and in an untimely event where only one vehicle changes its pseudonym then its possible for a malicious user to link the pseudonyms before and after. Also, *Location* and *Velocity* details broadcasted by the vehicles in *safety messages* can reveal details which makes privacy vulnerable.

1. Privacy-Preserving and Verifiable Querying Scheme (PVQS):

The paper ‘A Privacy-Preserving and Verifiable Querying Scheme in Vehicular Fog Data Dissemination’ presents the scheme that makes use of Paillier encryption and Invertible matrix to achieve privacy and confidentiality. In this scheme, data aggregation is done by a secure multi-dimensional scheme which will be encrypted using ‘Homomorphic Paillier Cryptosystem’. Also, Identity-Based Signature (IBS) scheme is employed to verify the integrity of the data queries.

However, the PVQS cannot be deployed in a high vehicle density scenario, because of the computational overhead that comes with the homomorphic encryption. Also, the scheme is vulnerable to collusion attacks where multiple vehicles come together to attack other vehicles in the network.

**Proposed method:**

Efficient Privacy-Preserving Data Query and Dissemination Scheme (EPDQD):

The current work describes about EPDQD Scheme which uses a lightweight homomorphic encryption technique and Chinese Remainder Theorem (CRT). The scheme presents a four-step process System initialization, Query group formulation, Query request generation and Query request aggregation and reading. Also, non-interactive secure session keys and message authentication codes (MAC) are employed which improve further the security of the scheme.

Merits:

* Achieves *unlinkability* i.e., makes it impossible to map the query request and its origin.
* Works efficiently even in highly vehicle dense scenarios, because of low computational complexity and less communication overhead.
* Resists several security attacks and threats.

Demerits:

* The proposed scheme is still not good enough to resist some collusion attacks.

**SOURCE CODE**

**SNAPSHOTS**

**CONCLUSIONS AND FUTURE PLANS**

**APPENDIX – BASE PAPER**

**REFERENCES**