PRESERVING DATA PRIVACY IN WIRELESS COMMUNICATION NETWORK

A FINAL YEAR CAPSTONE DESIGN PROJECT

(Phase-I)

Submitted by

**V.Pavan Kumar Reddy (9918004173)**

**S.Arshad Ali (9918004160)**

**B.Hemanth(9918004171)**

in partial fulfillment for the award of the degree

of

BACHELOR OF TECHNOLOGY

IN

# COMPUTER SCIENCE AND ENGINEERING



SCHOOL OF COMPUTING

COMPUTER SCIENCE AND ENGINEERING

KALASALINGAM ACADEMY OF RESEARCH

AND EDUCATION

KRISHNANKOIL 626 126

Academic Year 2021-2022

DECLARATION

We affirm that the project work titled “PRESERVING DATA PRIVACY IN WIRELESS COMMUNICATION NETWORK” being submitted in partial fulfillment for the award of the degree of Bachelor of Technology in Computer Science and Engineering is the original work carried out by us. It has not formed the part of any other project work submitted for award of any degree or diploma, either in this or any other University.

V.Pavan Kumar Reddy

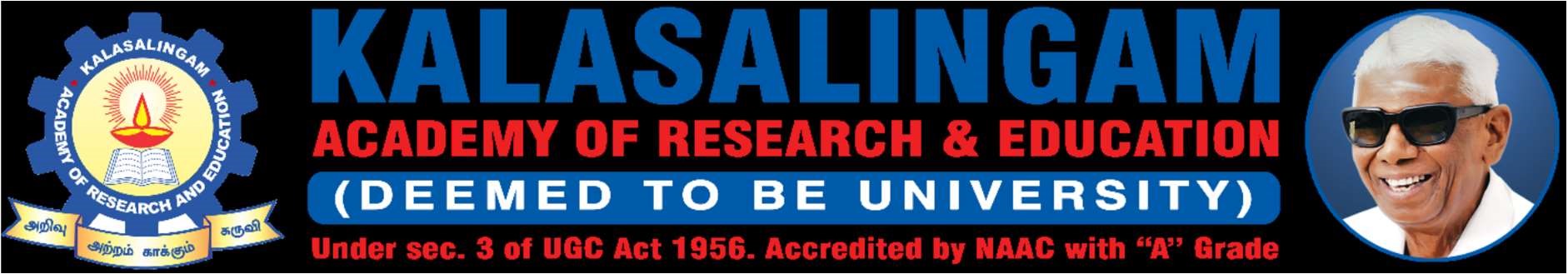
(9918004173)

S.Arshad Ali

(9918004160)

B.Hemanth

(9918004171)



# BONAFIDE CERTIFICATE

Certified that this project report “PRESERVING DATA PRIVACY IN WIRELESS COMMUNICATION NETWORK” is the bonafide work of “V.Pavan Kumar Reddy, S.Arshad Ali, B.Hemanth” who carried out the project work under my supervision.

SUPERVISOR HEAD OF THE DEPARTMENT

Mr.P.VELMURUGADASS Dr. A. FRANCIS SAVIOUR DEVARAJ

Assistant Professor Professor/Head

Computer Science and Engineering Computer Science and Engineering

Kalasalingam Academy of Research and Kalasalingam Academy of Research Education and Education

Krishnankoil 626126 Krishnankoil 626126

Submitted for the Project Viva-voce examination held on.......................................

Internal Examiner External Examiner

# ACKNOWLEDGEMENT

First and foremost, I wish to thank the Almighty God for his grace and benediction to complete this Project work successfully. I would like to convey my special thanks from the bottom of my heart to my dear Parents and affectionate Family members for their honest support for the completion of this Project work.

I express deep sense of gratitude to “Kalvivallal” Thiru. T. Kalasalingam B.com., Founder Chairman, “Ilayavallal” Dr.K.Sridharan Ph.D., Chancellor, Dr.S.Shasi Anand, Ph.D., Vice President (Academic), Mr.S.Arjun Kalasalingam M.S., Vice President (Administration) , Dr.R.Nagaraj, Vice-Chancellor, Dr.V.Vasudevan Ph.D., Registrar , Dr.P.Deepalakshmi M.E., Ph.D., Dean (School of Computing) . And also a special thanks to Dr. A. Francis Saviour Devaraj . Head, Department of CSE, Kalasalingam Academy of Research and Education for granting the permission and providing necessary facilities to carry out Project work.

I would like to express my special appreciation and profound thanks to my enthusiastic Project Supervisor, Mr.P.Velumurugadass, Assistant Professor/CSE of Kalasalingam Academy of Research and Education [KARE] for his inspiring guidance, constant encouragement with my work during all stages. I am extremely glad that I had a chance to do my Project under my Guide, who truly practices and appreciates deep thinking. I will be forever indebted to my Guide for all the time he has spent with me in discussions. And during the most difficult times when writing this report, he gave me the moral support and the freedom I needed to move on.

Besides my Project guide, I would like to thank the rest of Class committee members and all faculty members and Non-Teaching staff for their insightful comments and encouragement. Finally, but by no means least, thanks go to all my school and college teachers, well wishers, friends for almost unbelievable support.



School of Computing

Project Summary

|  |  |  |
| --- | --- | --- |
| Project Title | Preserving DataPrivacy In Wireless Communication Network | |
| Project Team Members (Name with Register No) | V.Pavan Kumar Reddy (9918004173)  S.Arshad Ali (9918004160)  B.Hemanth (9918004171) | |
| Guide Name/Designation | Mr.P.Velumurugsdass  Assistant Professor, Department of Computer Science and Engineering | |
| Program Concentration Area | Preserving Data Privacy | |
| Technical Requirements | AWK and TCL scripts, NS-3-3 simulator | |
| Area | Codes & Standards / Realistic Constraints | Tick  ✓ |
| Economic |  |  |
| Environmental |  |  |
| Social | This project helps to increase the privacy protection level | ✓ |
| Ethical |  |  |
| Health and Safety |  |  |
| Manufacturability |  |  |
| Sustainability |  |  |

**Realistic Constraints:**

**Social:**

The usage of mobile devices and Internet-connected devices are becoming rapidly common, and such devices are more integrated with our society (e.g. in the case of embedded, wearable devices are more integrated with our human body). Malicious activities often take place when data are not encrypted during data transmissions and data encryption may not be deployed due to performance considerations. Therefore, the data which is stored on these devices should need to be protected.

**Engineering Standard:**

# The project is based on IEEE -2019 - Secure Data Aggregation to Preserved Data and Key Privacy in Wireless Sensor Networks

Preserving data privacy which is highly sensitive that was stored in applications. This can work for large data transmissions by providing the maximum privacy protection and it will minimize the privacy leakage even when the third-party will monitor communications

**Table of Contents**

|  |  |  |
| --- | --- | --- |
| **CHAPTER**  **NO.** | **TITLE** | **PAGE NO.** |
|  | **ABSTRACT** | 8 |
|  | **LIST OF FIGURES** |  |
| **1.** | **INTRODUCTION** | 9 |
| 1.1 | Overview | 9 |
| **2.** | **LITERATURE SURVEY** | 13 |
| **3.** | **PROBLEM DEFINITION** | 15 |
| 3.1 | Objective and Scope | 15 |
| **4.** | **PROJECT PLAN** | 16 |
| 4.1 | Proposed Model | 18 |
| **5.** | **SYSTEM ANALYSIS** | 19 |
| **6.** | **PROJECT DELIVERABLE** | 21 |
| **8.** | **REFERENCES** | 22 |

**LIST OF ABBREVIATIONS**

|  |  |
| --- | --- |
| **Abbreviation** | **Full form** |
| **ODA** | Optimal Data Alternative’s |
| **DPP** | Dynamic privacy protection |
| **CODP** | Content-Oriented Data Pair |
| **DC** | Data Collisions |

**ABSTRACT**

The technologies now-a-days are increasing gradually. In our digitalized society, with respect to technologies, the data is also increasing rapidly. It is important to provide privacy for the sensitive data. So, in this project, we are providing privacy for this data by using Dynamic Privacy Protection model rather than using conventional encryption.

In a present scenario, with mobile devices and other Internet connected devices (e.g: sensors) becoming the normal in our digitalized society, the capacity to ensure the security of data-in-transit and at-rest without involving in unrealistic performance overheads is crucial. If adequate security and privacy-preserving measures are not in place, a user’s privacy could be compromised due to data leakage. Here, we are discussing the Dynamic Privacy Protection model as it is designed for ensuring user’s privacy even in large volumes of data.

**CHAPTER – 1**

**INTRODUCTION**

* 1. **OVERVIEW**

Wireless Communication is the fastest growing and most vibrant technological area in the communication field. Wireless Communication may be a method of transmitting information from one point to other, without using any connection like wires, cables, or any physical medium.

Generally, during a communication system, information is transmitted from transmitter to receiver that's placed over a limited distance. With the assistance of Wireless Communication, the transmitter and receiver are often placed anywhere between few meters (like a T.V. Remote Control) to a couple of thousand kilometres (Satellite Communication).

We sleep in a World of communication and Wireless Communication, especially , may be a key a part of our lives. Some of the commonly used Wireless Communication Systems in our day–to– day life are: Mobile Phones, GPS Receivers, Remote Controls, Bluetooth Audio and Wi-Fi etc.

The most commonly used wireless communication system is that the mobile Technology. The development of mobile cellular devices changed the World like no other technology. Today’s mobile phones aren’t limited to only making calls but are integrated with numerous other features like Bluetooth, Wi-Fi, GPS, and FM Radio.

The latest generation of Mobile Communication Technology is 5G (which is indeed successor to the widely adapted 4G). Apart from increased data transfer rates (technologists claim data rates in the order of Gbps), 5G Networks are also aimed at Internet of Things (IoT) related applications and future automobiles.

Along with Mobile applications, there are also other technologies like the Internet of Things(IoT), Machine Learning, etc., These technologies use different devices like sensors, actuators, Gateways, etc., These devices collect users' data and key information. For any Internet of things applications, these devices are very normal because these devices can reduce human intervention.

Now-a-days, using a mobile device is normal. If we are using IoT applications like smart homes, smart apps, wearable devices, etc.., then the data will be generated from these applications. Some sensitive data like user’s movements, locations, etc.., should be protected. If sensitive data is leaked, then the privacy for that data will not be there.

Mobile devices have emerged with the latest technologies like big-data, IoT, Cloud Computing, etc..,. So the data is generated from mobiles also. For instance, location-oriented mobile applications(apps), applications on wearable devices, and real-time telehealth apps usually produce a large amount of data that contain user private information, such as location and movements.

To provide privacy and security, we will use conventional encryption. Encryption provides privacy and security for data-at-rest and data-in-transit, including in wireless communication environments. In encryption, we will use methods like AES(Advanced Encryption Standard). Here, we will use full encrypted data for security.

Malicious activities often take place when data are not encrypted during data transmissions and data encryption may not be deployed due to performance considerations. Thus, here, we proposed to selectively encrypt data, based on the requirements and constraints of the associated hardware or software.

Specifically, we model the conditions of hardware/software to be constraints that are required to be satisfied by data encryption prior to data transmission. For instance, for a real-time service app, the longest acceptable execution time can be configured as a timing constraint. The basic premise of our proposed model is generating an optimal solution to maximize the privacy protection levels by leveraging existing computing resources.

The output of this Dynamic Privacy Protection model is the plan which will minimize the data leakage of user. This model uses content-oriented approach to selectively encrypt data for the purpose of privacy protection. Here, we are enhancing the privacy protection level by using this content-oriented approach based on dynamic programming.

The proposed model will work even in large data transmissions by providing the maximum privacy protection and it will minimize privacy leakage even the third party will monitor communications.

In this model, we emphasize the importance of protecting the data that can result in the violation of a user’s privacy when different data are combined. To achieve this goal, we define the Content-Oriented Data Pairs. To allow for the “manipulation” of data encryption operations dynamically, we present the Optimal Data Alternatives (ODA) algorithm designed to produce the selective encryption plan for non-Content Oriented Data Pairs data. The Optimal Data Alternatives algorithm minimizes the likelihood of privacy leakage from using data mining techniques when adversaries monitor multiple channels. Also, the Optimal Data Alternatives algorithm can produce an optimal solution, in the sense of maximizing the privacy level by satisfying the constraints.

**LITERATURE SURVEY**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SLNO** | **Title** | **Author** | **Advantages** | **Disadvantages** |
| 1 | An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones | Taint Droid, Peter Gilbert, William enck | 1) It was designed to address privacy challenges due to data collections operated by a thirdparty.  2)It also ensure user data privacy | 1) It do not solve data leakage issues entirely, since the security of the wireless data transmission is not considered. |
| 2 | Polynomial regression-based privacy-preserving data aggregation approach designed for WSNs. | Miao Peng, Yang Xiao, Suat Ozdemir | 1)Ensures User data privacy. 2)It will not reduces the functionalities. | 1) Reduces functionalities. |
| **3** | Migrating a fine-granularity access control model to the cloud server to reduce the rate of data over-collection | Xingfeng ye, Bakh Khoussainov | 1)Ensures User data privacy. 2)It will not reduces the functionalities. | 1)It will not work for wireless communication networks |
| **4** | Privacy enhancing approach designed to mitigate risks due to power data aggregation from internal attacks in a smart grid. | C. Fan, S. Huang, and Y. Lai. | 1)Provides Security. 2)Computing cost is less when compared to others. | 1)Reduces Functionalities. |
| **5** | Multi-access control model as an alternative of securing privacy when data are shared among several social networking platforms | Hongxin Hu, Gali-joon ahn, Jan jorgensen | 1)It provides security and privacy. | 1)It will not work well with complex networking environments. |

**CHAPTER – 3**

**PROBLEM DEFINITION**

**3.1 PROJECT OBJECTIVE AND SCOPE**

The main objective of this project is to maximize the privacy protection level. Here, we are trying to increase the privacy protection level for the data. To minimize the data leakage of mobile device user privacy. To design an optimal solution for maximizing the protection level.

**CHAPTER – 4**

**PROJECT PLAN**

As we are trying to increase the privacy protection level, to implement this, first we have to represent a node for communication. We should organize the nodes in a mesh structure. Once the nodes are arranged, then we should establish a connection so that the messages between those nodes should be transfer to other nodes.

While the message is transferring, the node which is sending that message should able to know the neighbouring node which is receiving the message. Finding the neighbouring node is an important task in the first step.

The second step is classifying the messages into two categories which are sensitive data and Nonsensitive message. This Data sensitivity will be categorized manually by using keywords. For example, in medical records, the sensitive data is heart rate, blood level, etc. So we will group them in sensitive messages.

In this, first, we will create a sink node among all the nodes. All the sensitive data or Non-sensitive data will be store at sink node. Here we will be able to see the path from the node which is generating sensitive data to sink node. A shortest routing algorithm is used here for the path between the data generating node and sink node. It is used for both sensitive data and Non-sensitive data and here we are naming it as real-time event for sensitive data and Non-real time event for Non-sensitive data. Once the transmission is started, we are going to see a circles between nodes which represents the transmission between the node and the neighbouring node.

The third step is implementing the Dynamic privacy protection model which is a combination of Content-oriented Data Pairs and Optimal Data Alternative’s algorithm. In this step, the Optimal Data Alternative algorithm implementation will be done and by using this algorithm, we will achieve the content-oriented Data pairs identification. The output of this step is a D-Table, which is a data protection plan to determine which data need to be encrypted. After finding the Content Oriented Data Pairs, a selective encryption algorithm is used for these pairs and another encryption algorithm will be used for Non Content-oriented Data Pairs.

The inputs of ODA algorithm include a Value Table (V-Table) and the constraint C. The V-Table is generated using the V-Table Generation algorithm. The purpose of generating a V-Table is to apply dynamic programming. Here, the V-table is also called the former which is an input to the Algorithm. The Optimal Data Alternatives algorithm is designed to create an optimal solution to obtain the maximum P value by considering the computing resource constraints

**4.1 PROPOSED MODEL**

Dynamic Privacy Protection Model

There are three main components in this process, namely:

1) Security Classifications

2) Content-Oriented Data Pairs

3) Input Data table

**1)Security classification**: Security Classifications refers to a configuration procedure that defines

the privacy weight for each data type that is associated with the content. classifications.

**2)Content-oriented data pairs identification (CODP):** We define the Content-Oriented Data

Pair (CODP) as those data that will result in the compromise of one’s privacy when examined

collectively. To put it another way, if an adversary acquires two data or data packages at the same time, privacy can be compromised. However, an adversary is not able to compromise the

user’s privacy if the adversary only obtains one of the data or data packages. Any two data or data packages that meet this criterion are considered CODPs.

For example, a mobile app sends out data consist of both username data and user location data.

Revealing both data can result in privacy leakage issue; thus, username and user locations data are

paired because these are sensitive data. If these data is leaked, then user’s privacy will also be leak.

**3) Input data table:** We use the higher-level security mode to find at least one party of the

identified CODPs. Therefore, the original input data table, I-Table, needs to be modified using the

outcomes of the CODPs identifications.

Next step we will need to

identify content-oriented data pairs based on the outcomes of the security

**CHAPTER - 5**

**SYSTEM ANALYSIS**

There are several things that should be considered to make sure the development stage of the system can run successfully. There are software and hardware specification. Software is a conceptual entity which is a set of computer programs, procedures, and associated documentation concerned with the operation of a data processing system. Hardware is component devices which are typically installed into or peripheral to a computer case to create a personal computer upon which system software is installed including a firmware interface.

**Hardware Requirements**

Hardware requirements for the implementation and testing this project are mentioned as below:

➢ **Processor:** Any processor with speed above 500 MHz.

➢ **RAM:** 4GB

. ➢ **Hard Disk:** 256 GB.

➢ **Input device:** Standard Keyboard and Mouse.

➢ **Output device**: VGA and High Resolution Monitor.

**Software Requirements**

Software requirements for the implementation and testing of this project are mentioned as below.

➢ **Operating System:** UBUNTU

➢ **Tool:** NS-3.35, xgraph

➢ **Language:** TCL and AWK

**CHAPTER – 6**

**PROJECT DELIVERABLE**

* This project delivers the preserving data privacy of mobile device of an user who are using the device in wireless communication environment.
* It enhance the overall privacy protection level based on dynamic programming and we can increase the privacy protection level by using algorithms

**CHAPTER 7**

**REFERENCES**

[1]. Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao. A survey on security and privacy issues in internet-of-things. IEEE Internet of Things Journal, 4(5):1250 – 1258, 2017.

[2]. J. Zhou, Z. Cao, X. Dong, and X. Lin. Security and privacy in cloud-assisted wireless wearable communications: Challenges, solutions, and future directions. IEEE Wireless Communications, 22(2):136–144, 2015. [3]. S. Ozdemir, M. Peng, and Y. Xiao. PRDA: polynomial regression based privacy-preserving data aggregation for wireless sensor networks. WCMC, 15(4):615–628, 2015.

[4]. J. Sun, R. Zhang, and Y. Zhang. Privacy-preserving spatiotemporal matching for secure device-to-device communications. IEEE Internet of Things Journal, 3(6):1048–1060, 2016.

[5]. I. Vergara-Laurens, L. Jaimes, and M. Labrador. Privacy preserving mechanisms for crowdsensing: Survey and research challenges. IEEE Internet of Things Journal, 4(4):855 – 869, 2017.