# THESIS TITLE

A DISSERTATION PART-I REPORT SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

**MASTER OF TECHNOLOGY (CS)**

BY

**STUDENT NAME**

**ROLL No. ---------**

UNDER THE GUIDANCE

OF

**GUIDE NAME**

DESIGNATION AND DEPT. NAME

DEPARTMENT OF COMPUTER SCIENCE & IT

SCHOOL OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY

MAULANA AZAD NATIONAL URDU UNIVERSITY, HYDERABAD
GACHIBOWLI, HYDERABAD - 500032, INDIA

2016

# MAULANA AZAD NATIONAL URDU UNIVERSITY

**Gachibowli, Hyderabad-500032**

## Certificate

This is to certify that project report entitled **"THESIS TITLE"** submitted by **Student name** bearing Roll No……. in partial fulfillment of the requirements for the award of **Master of Technology (CS)** Degree during 2014-2015 at the **Department of CS&IT** is an authentic work carried out by him/her under our guidance and supervision.

The results presented in this report have been verified and are found to be satisfactory. The results embodied in this dissertation have not been submitted to any other University or Institute for the award of any other degree or diploma.

**Student Name & Signature**

**Supervisor Signature**

**DRC Members Signature**

**Head**
**Department of CS&IT**

# CANDIDATE'S DECLARATION

I hereby declare that the thesis work presented in this report entitled "**TITLE (IN CAPITAL LETTERS)"** towards the partial fulfillment of the requirement for the award of the degree of **Master of Technology (Computer Science)** submitted in the **Department of CS&IT**, Maulana Azad National Urdu University, Hyderabad, Telangana, India is an authentic record of my own work carried out under the guidance of **(Name & Designation of Guide)**, **Department of CS&IT,** Maulana Azad National Urdu University, Hyderabad (Telangana).

I have not submitted the matter embodied in this project report for the award of any other degree or diploma to any other University or Institute.

Date:

Place: **(Student Name)**

# ACKNOWLEDGEMENT

I express my sincere gratitude towards my **Supervisor** (**Name & Designation), Department of CS&IT**, MANUU Hyderabad for consistently providing me with the required guidance to help me in the timely and successful completion of this report.

I am deeply indebted to **Coordinator (Name & Designation), Department of CS&IT, MANUU** for his valuable suggestions and support. In spite of his extremely busy schedules in Department, he was always available to share with me his deep insights, wide knowledge and extensive experience.

I sincerely thank **Professor Abdul Wahid**, **Dean School of Computer Science & Information Technology, Head Department of CS&IT** for giving sufficient guidance for completing the project in time.

I express my whole hearted gratitude to **VC sir name, MANUU,** for providing the excellent environment for carrying through our academic schedules and project with ease.

I would like to thank all my friends and especially my classmates for all the thoughtful and mind stimulating discussions we had, which prompted us to think beyond the obvious. I have enjoyed their company so much during my stay at MANUU.

STUDENT NAME

ROLL No.

## ABSTRACT

The abstract should be well written, clearly defining the objective of the work which has been carried out in the present project report. It should precisely indicate the original project goals that were defined and if the same have been achieved. If the same were achieved the results of the work must be high-lighted. If the same were not achieved, the reasons for the same must be briefly explained and it should be explained as to what mid-course corrections were introduced and what was achieved.

# TABLE OF CONTENTS

Comprehensive list of references must be given as per IEEE Standard/format. All these references must be linked to the text of the project report. For example, reference no (5) must be shown superscript [5] or [5] or as [5] along with the text.

# LIST OF FIGURES (Template)

# LIST OF TABLES (Template)

# ABBREVIATIONS AND ACRONYMS (Template)

| | |
|---|---|
| 3DES | triple data encryption standard |
| AK | Authorization key |
| AES | advanced encryption standard |
| AMC | adaptive modulation and coding |
| ASA | authentication and service authorization |
| ARQ | automatic repeat request |
| ATM | asynchronous transfer mode |
| BE | best effort |
| BER | bit error rate |
| BPSK | binary phase shift keying |
| BR | bandwidth request |
| BS | base station |
| BW | bandwidth |
| BWA | broadband wireless access |
| C/I | carrier-to-interference ratio |
| C/N | carrier-to-noise ratio |
| CA | certification authority |
| CBC | cipher block chining |
| CBC-MAC | cipher block chaining message authentication code |
| CCM | CTR mode with CBC-MAC |
| CCS | common channel signaling |
| CDMA | code division multiple access |
| ChID | channel identifier |
| CID | connection identifier |
| CINR | carrier-to-interference-and-noise ratio |
| CPS | common part sublayer |
| CRC | cyclic redundancy check |
| CS | convergence sublayer |

# CHAPTER 1

# INTRODUCTION

# CHAPTER 2

# LITERATURE SURVEY

# CHAPTER 3

# PROPOSED WORK

# CHAPTER 4

# IMPLEMENTATION

# CHAPTER 5

# RESULT ANALYSIS

# CHAPTER 6

# CONCLUSION AND FUTURE WORK

# REFERENCES

# PUBLICATIONS

# INTRODUCTION

## 1.1. OVERVIEW:

The objective of data mining is to generalize across populations, rather than reveal information about individuals. The hitches that data mining works by evaluating individual data that subject to privacy concerns. Thus, the true problem is not data mining, but the way data mining is done. However, the concern among privacy advocates is well founded, as bringing data together to support data mining makes misuse easier. Much of this information has already been collected, however it is held by various organizations. Separation of control and individual safeguards prevent correlation of this information, providing acceptable privacy in practice. However, this separation also makes it difficult to use the information for purposes that would benefit to society, such as identifying criminal activity. Proposals toshare information across agencies, most recentlytocombatterrorism,wouldeliminatethesafeguardsimposedbyseparationoftheinformation.

## 1.2. MOTIVATION:

The title "Privacy Preservation in Collaborative Data Mining as Goal Oriented Attack Model" is justified by the implementation of Homomorphic Encryption to secure the mined data between the user and the server.

Thegoalofdataminingis toextractormineknowledgefromlargeamounts data. However, details often collected by several different sites. Privacy, legal and commercial concerns restrict centralized access to this data. Theoretical results from the area of secure multi party computation in cryptography prove that assuming the existence of trapdoor permutations; one may provide secure protocols for any two party's computationaswellasforanymultipartycomputationwithhonestmajority.However, the general methods are far too inefficient and impractical for computing complex

functions oninputsconsistingoflargesets ofdata.Whatremains openiscomeupwitha setoftechniques toachievethisefficientlywithinaquantifiablesecurityframework.The distributeddatamodel consideredistheheterogeneousdatabasescenariowithdifferent features ofthesamesetofdatabeingcollectedbydifferentsites.

This thesis argues thatitisindeedpossibletohaveefficientandpractical techniquesforusefulprivacy-preservingminingofknowledgefromlargeamountsof data. The dissertation presents several privacy preserving data mining algorithms operatingoververtICallypartitioneddata.Thesetof underlyingtechniquessolving independentsub-problemsarealsopresented.Together, theseenablethesecure“mining" ofknowledge.

In today’sinformation age,datacollectionisubiquitous,andevery transactionis recordedsomewhere.The resultingdatasets canconsistofterabytes orevenpetabytes of data,so efficiencyand scalabilityistheprimaryconsiderationofmost datamining algorithms.Datamining technology hasemergedasameansofidentifyingpatternsand trendsfromlargequantities ofdata.Mosttools operatebygatheringalldataintoacentral site,then runningan algorithm againstthatdata.However,privacy concernscan prevent buildingacentralizedwarehouseanddatamaybedistributedamongseveral custodians, noneof whichareallowedtotransfertheirdatatoanothersite.Theproblemisthat computingassociation rules.Thegoalistoproduceassociation rulesthathold globally while limitingthe information shared about each site. Previous workin privacy preservingdatamininghasaddressed twoissues.In one,the aimispreservingcustomer privacyby distortingthedatavalues. Theideaisthat thedistorteddatadoesnotreveal privateinformationandthusissafetouseformining.Thekey resultisthatthedistorted data,andinformationonthedistributionoftherandom datausedtodistortthedata,can beusedtogenerateanapproximationtotheoriginaldatavalues.

Recentadvancesindatacollection,datadissemination andrelated technologies haveinauguratedaneweraof researchwhereexistingdataminingalgorithmsshouldbe reconsideredfrom thepointofviewofprivacypreservation.Theneedforprivacyis sometimesduetolaw(e.g.,formedical databases)orcanbemotivatedbybusiness interests.However,therearesituationswherethesharingofdatacanleadtomutual

# REFERENCES


[1]. Maryam Alnuaimi, Mohamed Boulmalf, Farag Sallabi and Abderrahmane Lakas Khaled Shuaid, "Performance Evaluation of IEEE 802.15.4: Experimental and simulation Results," *Journal of Communications*, vol. 2, pp. 29-37, June 2007.

[2]. K. Shuaib and I. Jawhar M. Alnuaimi, "Performance Evaluation of IEEE 802.15.4 Physical Layer Using Matlab/Simulink," in *Innovations in information technology*, Nov 2006., pp. 1-5.

[3]. Farahani Shashin, *ZigBee wireless networks and Transceivers*. Amsterdam, USA: Newnes publications, 2008.

[4]. Sohraby, K Jana, R. Chonggang Wang, Lusheng Ji, and M. Daneshmand, "Voice communications over ZigBee networks," *IEEE communications magazine*, vol. 46, pp. 121-127, january 2008.

[5]. ZigBee Aliance. (2006, December) ZigBee Specification.

[6]. Chi-Chun Huang, Jian-Ming Huang, Chih-Yi Chang and Chih-Peng Li Chua-Chin Wang, "ZigBee 868/915-MHz Modulator/Demodulator for Wireless Personal Area Network," *IEEE transactions on Very Large Scale Integration(VLSI) systems*, vol. 46, pp. 936-939, July 2008.

[7]. Dayan Adionel Guimar˜aes, *Digital Transmission: A Simulation-Aided Introduction with VisSim/Comm*. NewYork, USA: Springer, 2009.

[8]. Nam-Jin Oh and Sang-Gug Lee, "Building a 2.4-GHZ radio transceiver using IEEE 802.15.4," *Circuits and Devices Magazine, IEEE*, vol. 21, no. 6, pp. 43-51, Jan - Feb 2006.

[9]. Theodore S Rappaport, *Wireless Communications, Principles & Practice*. New Jersey, USA: Prentice Hall publications, 2002.

[10]. Simon Haykin, *Communication Systems*, 4th ed. NewYork, USA: John wiley , 2001.

[11]. Herbert Taub and Donald L Schilling, *Principles of Communication systems*, 2nd ed. NOIDA, INDIA: Tata McGraw-Hill publications, 1999.

[12]. Gronemeyer S and McBride A, "MSK & offset QPSK modulation," *IEEE transactions on communications*, vol. 24, no. 8, pp. 809-820, August 1976.

[13]. Fleisher S.M. and Qu S, "Multifrequency minimum shift keying," *IEEE journal on selected areas of communications*, vol. 10, no. 8, pp. 1243-1253, october 1992.

[14]. Aarno Pärssinen, *Direct conversion receivers in wideband systems*. Dordrecht, United States of America: Kluwer Academic Publishers, 2002.

[15]. D. Morais and K. Feher, "Bandwidth Efficiency and Probability of Error Performance of MSK and Offset QPSK Systems," *IEEE transactions on communications*, vol. 27, no. 12, pp. 1794-1801, December 1979.

[16]. Scolari N and Enz C.C., "Digital receiver architectures for the IEEE 802.15.4 standard," in *ISCAS '04. Proceedings of the 2004 International Symposium on Circuits and Systems*, vol. 4, 2004, pp. 345-348.

[17]. Ali Abuelmaatti, Iain Thayne and Steve Reaumont, "A new approach to QPSK : Mechanism and implementation," in *IEEE Wireless Communications and Networking Conference*, 2007, pp. 2393-2398.

[18]. Amoroso F and Kivett J, "Simplified MSK Signaling Technique," *IEEE transactions on communications*, vol. 25, no. 4, pp. 433-441, April 1977.

# PUBLICATIONS

[1]. Ravikanth Kanna, Sarat Kumar Patra, Kiran Kumar Gurrala, Badugu Suresh, V V Satyanarayana, "Design of ZigBee transmitter using MATLAB/Simulink", *International journal of systems simulation,* pp.23-28, March 2011.