International Journal of Engineering Research and Development
***e**-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com*
Volume 3, Issue 9 (September 2012), PP. 07-14

Analysis of Cloud Computing & Emergence of Linear Programming

G.DivyaTara[1], M.Vijay Kamal[2], K.C.Ravi Kumar[3]
[1,2,3]Sridevi Women's Engineering College Hyderabad

Abstract*—Cloud Computing provides robust computational power to the society at reduced cost that enables customers with minimum computational resources to outsource their large computation workloads to the cloud, and economically enjoy the massive computational power, bandwidth, storage, and even appropriate software that can be shared in a pay-per-use manner. Tremendous advantage is the primary goal that prevents the wide range of computing model for customers when their confidential data are consumed during the computing process. Problem solving is a technique to reach the practical goal of particular mechanisms that not only solves the problems but can also protect from malicious behaviors. Linear programming is an operation research technique formulating private data by the customer for LP problem as a set of matrices and vectors, to develop a set of efficient privacy-preserving problem transformation techniques, which allow customers to transform original LP problem into some arbitrary one while protecting sensitive input/output information. We identify that LP problem solving in EXCEL mechanism is efficient additional cost on both cloud server and comparative analysis presents the follow of Linear programming in cloud computing is practical mechanism design.

***Keywords*—Cloud Computing, Microsoft EXCEL, Secure, Linear Programming, Encryption.**

I. INTRODUCTION

Linear programming can be used to solve many practical problems that are distributed and require protection of the input data. In supply chain planning the participating companies need to exchange information about production costs and capacities. Cloud computing is the best for outsourcing applications focuses on compute capabilities as the deciding factor will be public private hybrid cloud a high level decision is made for each platform class. Cloud computing provides convenient network access to shared pool of configurable computing resources that can be rapidly deployed with great efficiency and minimal management. By outsourcing the work into the cloud customers could enjoy the literally unlimited computing resources in a pay per use without committing any large capital outlays in the purchase of both hardware and software operations.

Tremendous advantages of outsourcing computations to the commercial public cloud customer's direct control over the systems that process their data during the computation which inevitably brings in security concerns and outsourced computation workloads often contain sensitive information such as the business financial records, research data or personally identifiable information. To secure against unauthorized information leakage sensitive data is to be encrypted before outsourcing so as to provide end to end data confidentiality assurance in the cloud normal data encryption techniques in essence prevent cloud from performing any meaningful operation of the underlying plaintext data [1], making the computation over encrypted data a very hard problem. On the other hand, the operational details inside the cloud are not transparent enough to customers [2]. As a result, there do exist various motivations for cloud server to behave unfaithfully and to return incorrect results, i.e., they may behave beyond the classical semi-honest model. For example, for the computations that require a large amount of computing resources, there are huge financial incentives for the cloud to be "lazy" if the customers cannot tell the correctness of the output. Besides, possible software bugs, hardware failures, or even outsider attacks might also affect the quality of the computed results. Thus, cloud is intrinsically not secure from the viewpoint of customers. A secure mechanism without for secure computation outsourcing, i.e., to protect the sensitive input and output information of the workloads and to validate the integrity of the computation analysis it would be hard to expect cloud customers to turn over control of their workloads from local machines to cloud solely based on its economic savings and resource flexibility.

II. SECTION

Related Work

Secure computing outsourcing that fulfills all aforementioned requirements such as input output privacy, correctness. soundness guarantee has been shown feasible in theory by Gennaro et al. It is currently not practical due to its huge computation complexity instead of outsourcing general functions in the security community, Atallah et al explore a list of work for securely outsourcing specific applications. The customized solutions are expected to be more efficient than the general way of constructing the circuits. A set of problem dependent disguising techniques are proposed for different scientific applications like linear algebra sorting, string pattern matching etc Atallah et al give two protocol designs for both secure sequence comparison outsourcing and secure algebraic computation outsourcing. However both protocols use heavy cryptographic primitive such as homomorphism encryptions and/or oblivious transfer and do not scale well for large problem set. Atallah et al. give a provably secure protocol for secure outsourcing matrix multiplications based on secret sharing. While this work outperforms their previous work in the sense of single server assumption and computation efficiency (no expensive cryptographic primitives), the drawback is the large communication overhead. Namely, due to secret sharing technique, all scalar operations in original matrix multiplication are expanded to polynomials, introducing significant amount of overhead. Considering the case of the result verification, the communication overhead must be further doubled, due to the introducing of additional pre-computed "random noise" matrices.

Another existing work list of work that relates to secure multiparty computation introduced by Yao and later extended by Goldreich et al. and many others. Secure multiparty computation allows two or more parties to jointly compute some general function while hiding their inputs to each other. General SMC can be very inefficient Du and Atallah et al. have proposed a series of customized solutions under the SMC context to a spectrum of special computation problems, such as privacy-preserving cooperative statistical analysis, scientific computation, geometric computations, sequence comparisons, etc. [3]. However, directly applying these approaches to the cloud computing model for secure computation outsourcing would still be problematic. The major reason is that they did not address the asymmetry among the computational powers possessed by cloud and the customers, i.e., all these schemes in the context of SMC impose each involved parties comparable computation burdens, which we specifically avoid in the mechanism design by shifting as much as possible computation burden to cloud only. Another reason is the asymmetric security requirement. In SMC no single involved party knows all the problem input information, making result verification a very difficult task. But in our model, we can explicitly exploit the fact that the customer knows all input information and thus design efficient result verification mechanism. Detecting the unfaithful behaviors for computation outsourcing is not an easy task, even without consideration of input/output privacy. Verifiable computation delegation, where a computationally weak customer can verify the correctness of the delegated computation results from a powerful but untrusted server without investing too much resources, has found great interests in theoretical computer science community. Some recent general result can be found in Goldwasser et al. [4]. In distributed computing and targeting the specific computation delegation of one-way function inversion, Golle et al. [5] propose to insert some pre-computed results (images of "ringers") along with the computation workload to defeat untrusted (or lazy) workers. In [6], Du. et al. propose a method of cheating detection for general computation outsourcing in grid computing. The server is required to provide a commitment via a Merkle tree based on the results it computed. The customer can then use the commitment combined with a sampling approach to carry out the result verification (without re-doing much of the outsourced work.) However, all above schemes allow server actually see the data and result it is computing with, which is strictly prohibited in the cloud computing model for data privacy. Thus, the problem of result verification essentially becomes more difficult, when both input/output privacy is demanded.

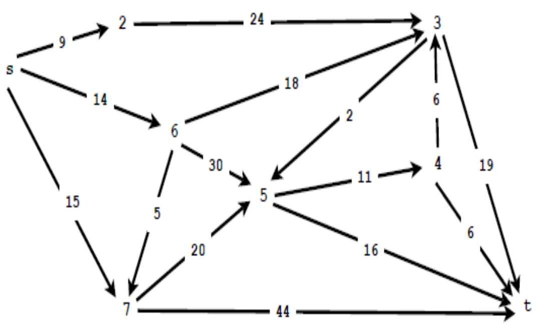
III. SECTION

3.1. Linear Programming

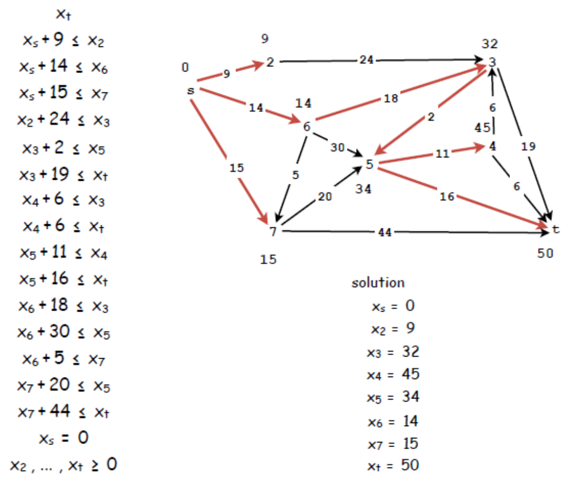
Process of formulating an LP model for a problem and solution to LP for a specific problem gives solution to the problem

Identify variables
Define Constraints (=and≠)
Define Objective function

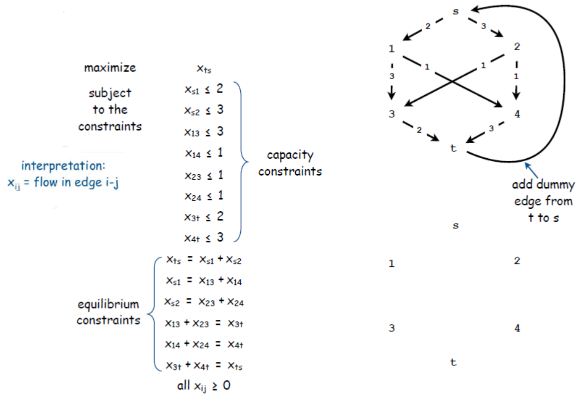
Single source shortest paths problem
Given weighted digraph single sources
Distance from s to v length of the shortest path from s to v
Goals find distance and shortest path from s to every other vertex.

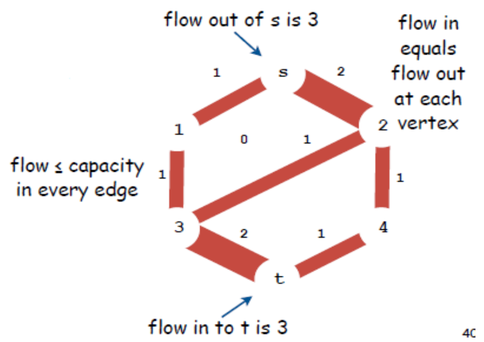


LP formulation of single source shortest paths problem
One variable per vertex one inequality per edge



One variable per edge, one equality per vertex.





3.2. Applications of Linear programming

CPLEX is revolutionized linear program created over 20 years ago it was the first commercial linear optimizer on the market written in the C language and it operation research's unprecedented flexibility reliability and performance to create novel optimization algorithms models. The name CPLEX is a pun built on the concept of a simplex algorithm written in C-simplex algorithm invented by George Dantzig in 1947 became the basis for the entire field of mathematical optimization and provided the first practical method to solve a linear programming problem. Business managers can use optimization to produce concrete measurable improvements in performance As abstract as the mathematics appears to be, it has powerful capabilities that enable businesses to reduce costs, improve profitability, use resources effectively, reduce risks, and provide benefits in many other key dimensions. Furthermore, optimization can automate decision processes to improve speed of responses and allow managers to focus their attention on critical uncertainties rather than routine matters. And these benefits have been demonstrated in numerous real-world implementations. Get your feet wet by first understanding what optimization can do for your business.

The concept behind a linear programming problem is simple. It consists for four basic components:

- Decision variables represent quantities to be determined
- Objective function represents how the decision variables affect the cost or value to be optimized (minimized or maximized)
- Constraints represent how the decision variables use resources, which are available in limited quantities

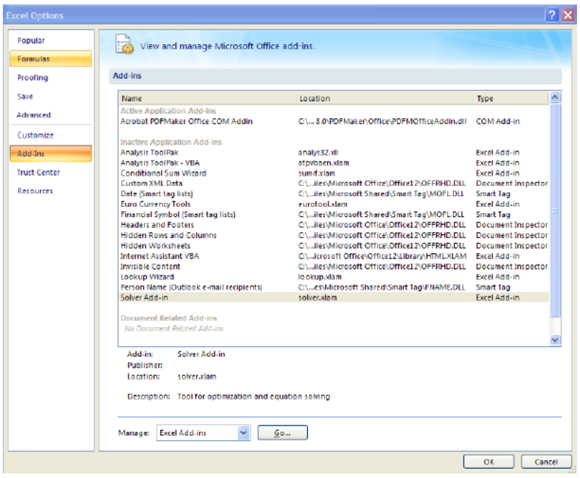
- Data quantifies the relationships represented in the objective function and the constraints

In a linear program**,** the objective function and the constraints are linear relationships, meaning that the effect of changing a decision variable is proportional to its magnitude. While this requirement may seem overly restrictive, many real-world business problems can be formulated in this manner. That provides a powerful and robust analytical methodology for supporting fact-based decision making. For example: If you want to decide how to supply of each kind of product in order to minimize your costs, you have to do that within a set of constraints. For instance you have to be able to produce enough to satisfy the demand on all your various products and you have to do it within the capacity you have, which can produce units at a given cost.

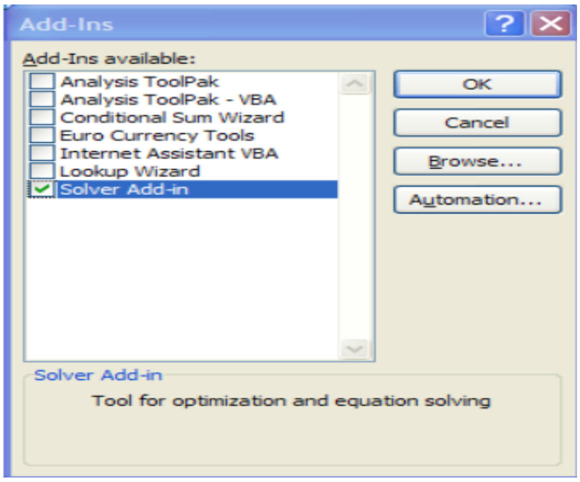
3.3. Linear Programming in EXCEL

Application type is Microsoft Excel version 2007 is to find the linear program using excel

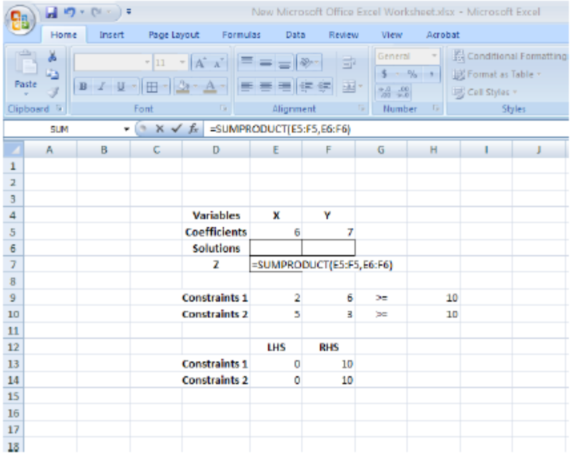
1. Install Solver Add-In



2. In the Add-Ins box select solver Add-In click Go.



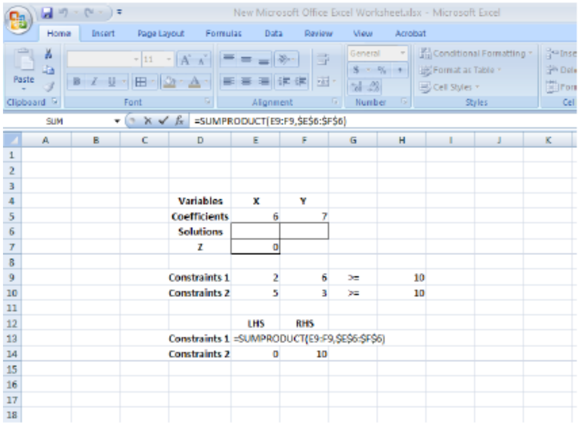
3. In the Add-Ins available box, check the analysis Toolpak and then OK



Example

Min Z = 6X + 7Y

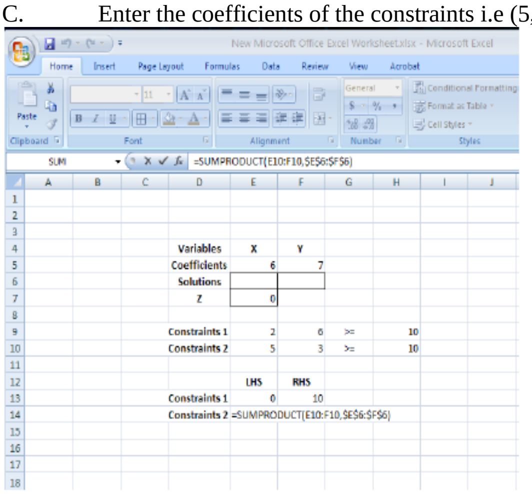
s.t 2X + 6Y â‰¥ 10
5X + 3Y â‰¥ 10
X,Y â‰¥ 0



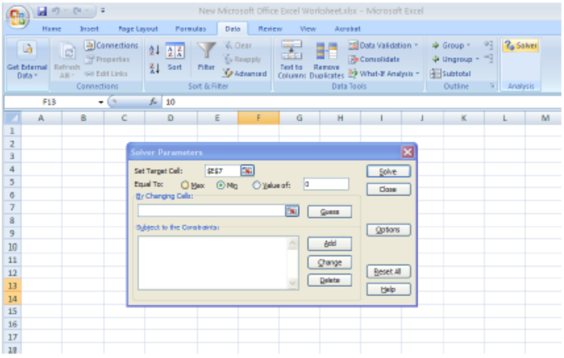
A. Enter the coefficients of the objective function Z i.e (6.7) in cells E5 and F5

B. Enter the coefficients of the constraints i.e (2,6) and RHS value 10 in cells E9, F9 and H9 respectively

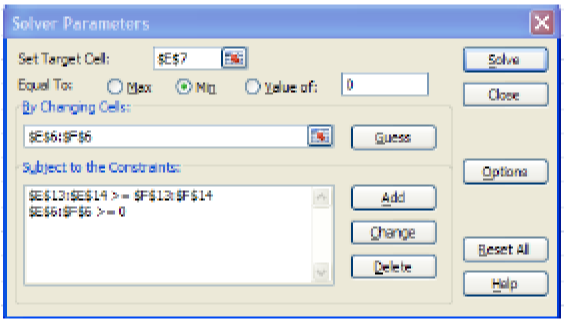
C. Enter the coefficients of the constraints i.e (5,3) and RHS value in cells E10,F10 and H10 respectively.



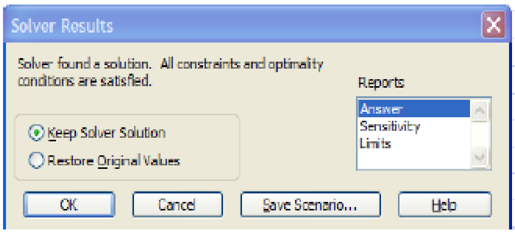
In this for the objective function value enter the formula for computing
Z=SUMPRODUCTS(E5:F%,E6:F6) formula uses the coefficient values and also the solution values for variables X and Y are to be solved.



Now the excel solver will be used in the data tab click solver as follows



Now set the target cell for the objective function Z value i.2 $ E$7 and check the equal to minimum option
For changing cell elect the solution values of the variables X & 7 i.e $E$6:$F$6
For subject to the constraints left side>=right side click on the Add option and select $E$13:$E$14>=$E$13:$E$14.
Now solution needs to be positive as $E$6:$F$6>0



Select the solve button the solver results appears a window check the keep solver solution and the answer in the reports section on the right side finally click ok button

Variables	X	Y		
Coefficients	6	7		
Solutions	1.25	1.25		
Z	16.25			
Constraints 1	2	6	>=	10
Constraints 2	5	3	>=	10
	LHS	RHS		
Constraints 1	10	10		
Constraints 2	10	10		

The solution values for variables X & Y and for the objective function Z.

IV. SECTION

4.1. Problem definition

Problem solving is a goal to achieve to success analysis results, previous problem solving techniques have implemented and used in many applications even to develop more secure problem solving technique we have introduced Linear programming in Cloud computing.

4.2. Comparative Analysis on LP Cloud Computing

In Previous work Secure Multi-party Computation allows two or more parties to jointly compute some general function while hiding their inputs to each other. Series of customized solutions under the SMC context to a spectrum of special computation problems, such as privacy-preserving cooperative statistical analysis, scientific computation, geometric computations, sequence comparisons. Compare to existing analysis practically efficient mechanisms for secure outsourcing of linear programming (LP) computations. Linear programming is an algorithmic and computational tool which captures the first order effects of various system parameters that should be optimized, and is essential to engineering optimization. It has been widely used in various engineering disciplines that analyze and optimize real-world systems, such as packet routing, flow control, power management of data centers. Because LP computations require a substantial amount of computational power and usually involve confidential data, propose to explicitly decompose the LP computation outsourcing into public LP solvers running on the cloud and private LP parameters owned by the customer. The flexibility of such decomposition allows us to explore higher-level abstraction of LP computations than the general circuit representation for the real efficiency with benefits security is the primary obstacle that prevents the wide adoption of this promising computing model, especially for customers when their confidential data are consumed and produced during the computation.

4.3. Implementation

Customer can use this computational tool which captures the first order effects of various system parameters that should be optimized, and is essential to engineering optimization. It has been widely used in various engineering disciplines that analyze and optimize real-world systems, such as packet routing, flow control, power management of data centers. Such a method of result validation can be very efficient and incurs close-to-zero additional overhead on both customer and cloud server. With correctly verified result, customer can use the secret transformation to map back the desired solution for his original LP problem

Apply this problem transformation for mechanism design. The general framework is adopted from a generic approach, while our instantiation is completely different and novel. In this framework, the process on cloud server can be represented by algorithm Proof Gen and the process on customer can be organized. This is a randomized key generation algorithm which takes a system security parameter k, and returns a secret key K that is used later by customer to encrypt the target LP problem. This algorithm encrypts the input tuple Φ into Φ_k with the secret key K. According to problem transformation, the encrypted input Φ_k has the same form as Φ, and thus defines the problem to be solved in the cloud. This algorithm augments a generic solver that solves the problem Φ K to produce both the output y and a proof ┌. The output y later decrypts to x, and ┌ is used later by the customer to verify the correctness of y or x. The mechanism must produce an output that can be decrypted and verified successfully by the customer. Process generates the results analysis.

V. CONCLUSION

This work shows the formalize the problem of Linear Programming of securely outsourcing computations in cloud computing, and provide such a practical mechanism design which fulfills input/output privacy, quality attributes, cheating resilience, and efficiency. Explicitly decomposing LP computation outsourcing into public LP solvers and private data, our mechanism design is able to explore appropriate security/efficiency tradeoffs via higher level LP computation than the general circuit representation. We develop problem transformation techniques that enable customers to secretly transform the original LP into some arbitrary one while protecting sensitive input/output information. We also investigate linear programming and derive a set of necessary and sufficient condition for result in Microsoft EXCEL verification.

REFERENCE

[1]. Sun Microsystems, Inc., "Building customer trust in cloud computing with transparent security," 2009, online at https://www.sun.com/offers/ details/sun transparency.xml.

[2]. M. J. Atallah, K. N. Pantazopoulos, J. R. Rice, and E. H. Spafford, "Secure outsourcing of scientific computations," *Advances in Computers*, vol. 54, pp. 216–272, 2001.

[3]. W. Du and M. J. Atallah, "Secure multi-party computation problems and their applications: a review and open problems," in *Proc. of NewSecurity Paradigms Workshop (NSPW)*, 2001, pp. 13–22.

[4]. S. Goldwasser, Y. T. Kalai, and G. N. Rothblum, "Delegating computation: interactive proofs for muggles," in *Proc. of STOC*, 2008, pp. 113–122.

[5]. P. Golle and I. Mironov, "Uncheatable distributed computations," in *Proc. of CT-RSA*, 2001, pp. 425–440.

[6]. W. Du, J. Jia, M. Mangal, and M. Murugesan, "Uncheatable grid computing," in *Proc. of ICDCS*, 2004, pp. 4–11.

[7]. J. Li and M. J. Atallah, "Secure and private collaborative linear programming," in *Proc. of CollaborateCom*, Nov. 2006.

[8]. www.webinova.in/academic_projects/...21/.../WNV_ADP012.doc

[9]. P. Mell and T. Grance, "Draft nist working definition of cloud computing," Referenced on Jan. 23rd, 2010 Online at http://csrc.nist.gov/ groups/SNS/cloud-computing/index.html, 2010.

[10]. Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," 2009, online at http://www.cloudsecurityalliance.org.

[11]. C. Gentry, "Computing arbitrary functions of encrypted data," *Commun.ACM*, vol. 53, no. 3, pp. 97–105, 2010.

G.Divya Tara pursuing M.Tech from SriDevi Womens Engineering. B.Tech CSE from Jyothishmathi College of Engineering & Technology. Her research work includes cloud computing, Datamining.

M.Vijaykamal B.E (CSE) from Gulbarga University and M.Tech (Software Engineering) from JNTU Hyderabad currently he is working as Assoc Prof Department of IT in SriDevi Women's Engineering College. He is having 10 years of Academic Experience and Life member in Computer society of India(CSI) & International Association of Computer Science and Information Technology (IACSIT). He was participated in Several National & International Conferences and Seminars and Published Several Papers. His research area includes Data Mining, Information Security.

K.C Ravi Kumar M.Tech CSE from JNTU Hyderabad currently he is the Head of the department for M.Tech CSE programme in SriDevi Women's Engineering College having 17 years of Academic Experience. He is life member of IEEE & IST areas of research include Data Mining & Data Warehousing Information Retrival Systems Information Security.