IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Issue-8, Aug 2019 E-ISSN: 2347-2693

Securing Cloud Data by Using Multi Keyword Search System

A. Prasannakumar Reddy[1*], M. Vikram[2], N. Sudhakar Reddy[3]

[1,2]Department of Computer Science and Engineering, S V College of Engineering, Tirupati, India
[3]S V College of Engineering, Tirupati, India

[*]Corresponding Author: reddy.apkr@gmail.com, Tel.: +91-91776-85959

DOI: https://doi.org/10.26438/ijcse/v7i8.9498 | Available online at: www.ijcseonline.org

Accepted: 15/Aug/2019, Published: 31/Aug/2019

Abstract— Securing Cloud data is a major task in current ongoing world. Now a days Cloud playing a major role in every technical aspect, for data storage. Here secure data management in Cloud is the major challenge to achieve. Attribute based encryption (ABE) is the most commonly used algorithm for circulated registering, where a data provider redistributes the data that is encoded, to a cloud master association, and can grant the data to customers having express accreditations (or qualities). Regardless, the standard ABE structure doesn't reinforce secure Deduplication, the basic rule for discarding multiple copies of undefined data to save additional room and framework information move limit. Here a trademark based limit structure is presented with checked duplication in a cream cloud setting, where a private cloud is responsible for duplicate disclosure and an open cloud manages the limit. Differentiating the previous systems which support data deduplication, our structure has bi-ideal conditions. Generally it might be used in a rapid manner to secretly give data to customers by choosing access plans as opposed to sharing translating keys. However, it is very helpful in acquiring the thought of semantic security which follows standard mechanism for data protection while the previous mechanism just simply achieved it by describing a flimsier security thought. Also, we put forward a framework to change a figure message more than one access system into figure works of the identical plaintext yet under various access courses of action without revealing the major plaintext.

Keywords— ABE, Storage, Deduplication.

I. INTRODUCTION

Circled managing fairly empowers facts suppliers who need to redistribute their statistics to the cloud[1] without revealing their precarious facts to outdoor get-together and may require clients with indisputable capacities to have the selection to get to the facts. This forecast information ought to be confirmed in blended systems with get admission to manage strategies to manipulate such a volume, that no person alongside clients with developments (talents) of express structures can translate the encoded data. For that a usual encryption method is presented that addresses this issue which is called as property based encryption (ABE), wherein a customer's non-public secret is related to a nice set, a message is encoded underneath a section overview (or access structure) over a large amount of homes, and a purchaser can able to decode a discern content material along with his/her personal key if persons association of traits accomplishes the direction of framework associated with this discern content. Regardless, the same old ABE shape neglects to accomplish secure deduplication, a method to associate extra room and gadget pass speed via losing stupid duplicates of the encoded informational collection away in the cloud. Obviously, the degree that we ought to know, present upgrades for relaxed deduplication are not set up on great based encryption[2]. Unintentionally, considering that. ABE and cozy deduplication had been frequently associated in scattered figuring, its miles talking to plot an appropriated collecting framework having the two houses. We don't forget the going with condition inside the plan of an Attribute-based point of confinement framework helping at ease deduplication[3] of mixed statistics inside the cloud, in such a way the specified cloud may not shop a report more than single time irrespective of the procedure in which that it'd get numerous duplicates of a close encoded document under diversified segments represented to techniques.

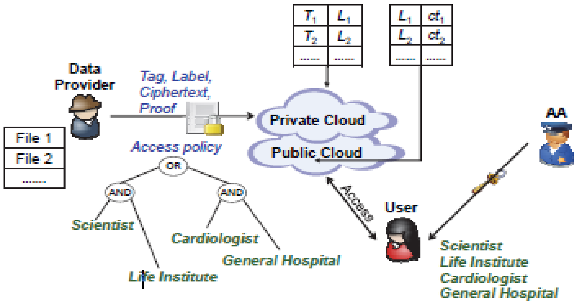


Figure 1. Architecture of Cloud Infrastructure

An information dealer, Bob, expects to move a document to the cloud, and offer with clients having positive accreditations. So as to do in that restrict, Bob encodes M underran get the risk to strategy over a variety of homes, and movements the status out determine content material from the cloud, with a definitive target that singular customers whose publications of motion of features gratifying the entry method can unscramble the parent content. A quick time frame later, every other records provider, Alice, moves determine content material for the almost equal fundamental file But credited to a specific get right of entry to plan A0. Since the report is moved in an encoded structure, the cloud cannot see that the plaintext referring to Alice's discern substance is indistinguishable from that acting in a different way on the subject of Bob's, and could store two times [5]. Clearly, such recreated collecting squanders greater room and correspondence facts pass restriction.

II. RELATED WORK

Secure Deduplication:

By having the main goal of sparing greater area for dispersed gathering associations, Douceur et al. a former scientist proposed the essential reaction for changing request and productivity in acting DEduplication called synchronous encryption, generally which involves process of encoding a message, beneath a message-reasoned key with the goal with sick described plaintexts are mixed to a nearly equal determine works. For this situation, if two customers circulate a similar document, the cloud server can watch the proportionate parent messages and store[5] simply one duplicate of them. Executions and assortments of concurrent encryption have been sent in. To formalize the appropriate protection definition for joined encryption [4], In this paper, a near framework to that during issued to perform comfy deduplication with respect to the personal cloud in the solid headway. In the pressure framework the execution of get admission to manage and the assist of catchphrase seek are exquisite troubles in relaxed scattered restrict shape. In this work, we depicted any other point of view of handy encryption [4] framework, and proposed a solid improvement. It bolsters adaptable different watchwords subset search, and manages the important thing escrow difficulty during the key age method. Pernicious client who sells thriller key for desired role may be prominent. The unwinding interest is usually redistributed to cloud server and the precision of half-unscrambled result can be checked by way of information consumer. The display exam and multiplication show its potential in calculation and farthest factor overhead. Starter consequences display that the test overhead at patron's terminals basically decreased, which noticeably spares the energy for asset pressured devices of customers. We entire the calculation of our storing up structure in Charm, which is a system, made to empower rapid prototyping of cryptographic plans and suggests.

III. METHODOLOGY

Attribute-Based Encryption:

Sahai and Waters presented worth based totally encryption (ABE)[2], and brief span later Goyal et al. represents key-technique ABE (KP-ABE) and discern substance method ABE (CP-ABE) as complimentary varieties of ABE. The sizeable KP-ABE improvement given in understood the monotonic get admission to systems, the essential KP-ABE framework supports the process of declaring non-monotone plans become acquainted with join logically sober minded get right of entry to procedures, after completion of that the rule large magnificence KP-ABE shape was proven by inside the designer specific model. Nevertheless, we apprehend that KP-ABE is much less adaptable than CP-ABE[6] in light of the manner that the way method is settled as soon as the customer's trademark personal keys issued. Bettencourt, The two persons named Sahai along with Waters proposed the foremost CP-ABE improvement, yet it is relaxed under the common social event version. After that Cheung Newport validated a CP ABE scheme that is exhibited to be relaxed underneath the normal released version, even though it truly bolster the AND get admission to structures. ACP-ABE framework beneath further made get right of entry to systems is proposed with the aid of Goyal et al. In mild of the range theoretic uncertainty. So as to beat the deterrent that the dimensions of the trademark space is polynomials forced in the protection parameter and the live plans are constant in advance, Rousak & Waters created a goliath universe CP-ABE framework below the high-request collecting. In this paper, the Rousakis-Water System is considered as the vital route of action for the solid headway.

Algorithm Steps for Attribute-Based Encryption.

Step 1:

Choose file id and file name and file data

Step 2:

Convert the data plain text into encryption format by using encryption algorithm. The input for this algorithm is attribute set γ and MK and after that it generates an output as novel master key MK′, novel public key PK′ and set of proxy rekeys rk which is applicable to all attributes that usually present in the attribute universe U.

Step 3:

After that user send request to the attribute authority for secret key.

Step 4:

Usually in this procedure master key should be always kept secret and make utilised especially for deriving users' private keys, even though the system parameters are generally made public.

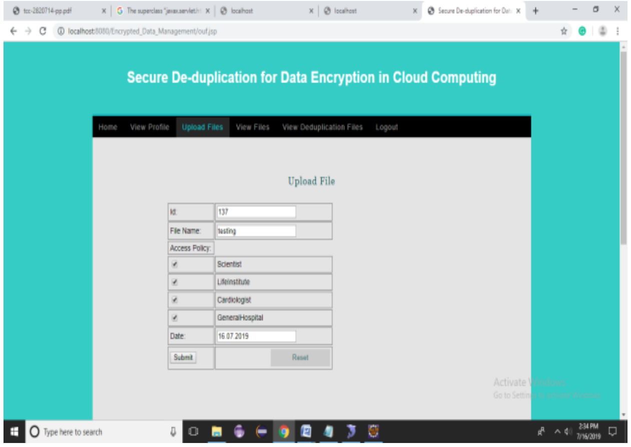
Step 5:

The procedure takes as input, and after that the identifier returns the private key as output for the user.

Step 6:

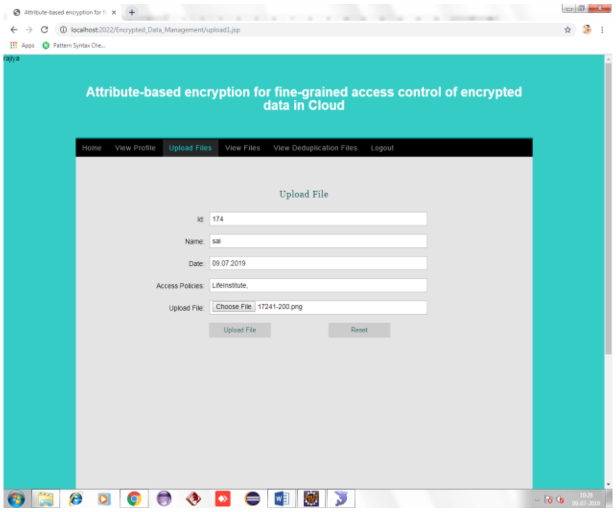
Decrypt the file using that key. And download that file.

IV. RESULTS AND DISCUSSION


Secure De-duplication for Data Encryption in Cloud Computing
Home View Profile Upload Files View Files View Deduplication Files Logout
Upload File
Submit
Reset

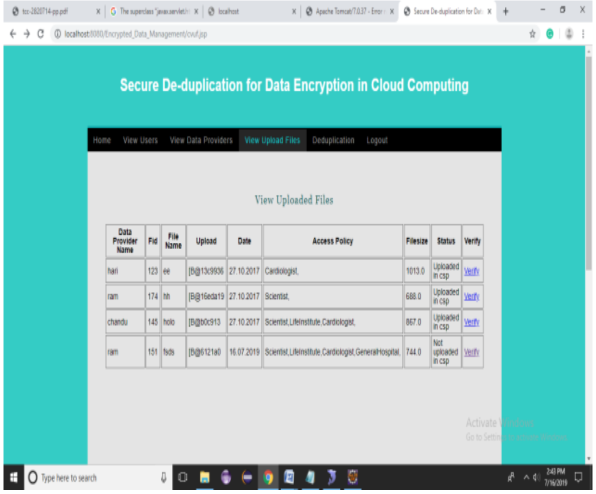
Id:	137
File Name:	testing
Access Policy:	
☑	Scientist
☑	LifeInstitute
☑	Cardiologist
☑	GeneralHospital
Date:	16.07.2019

Fig. 1 Here data provider can login and select any text files and uploads the data means plain data.


Attribute-based encryption for fine-grained access control of encrypted data in Cloud
Home View Profile Upload Files View Files View Deduplication Files Logout
Upload File
Upload File
Reset

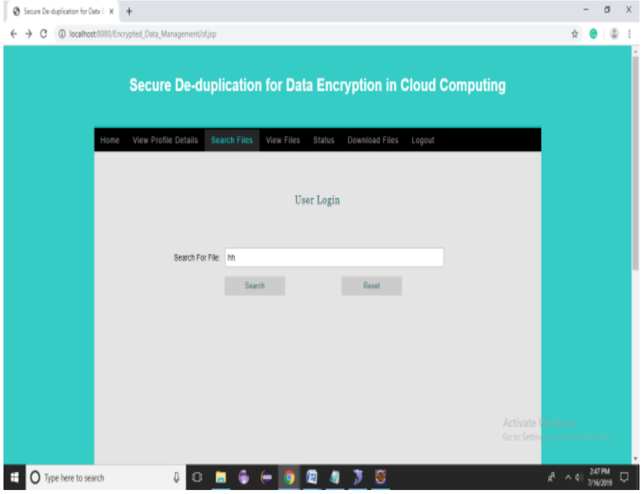
Id:	174
Name:	sai
Date:	09.07.2019
Access Policies:	LifeInstitute,
Upload File:	Choose File 17241-200.png

Fig. 2 And upload a file into the cloud. Then private cloud can be verify the uploaded file


Secure De-duplication for Data Encryption in Cloud Computing
Home View Users View Data Providers View Upload Files Deduplication Logout
View Uploaded Files

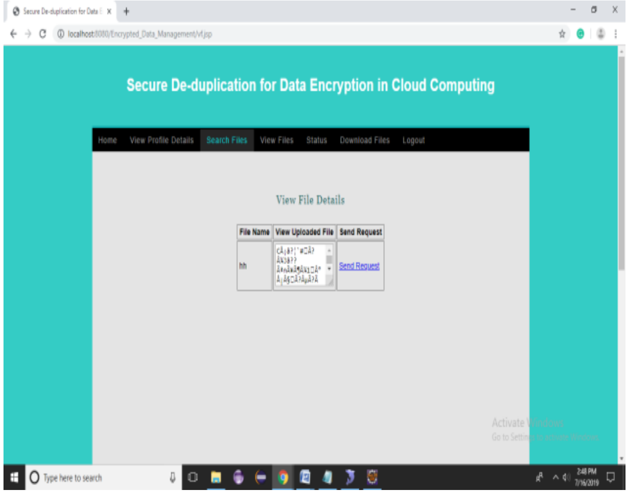
Data Provider Name	Fid	File Name	Upload	Date	Access Policy	Filesize	Status	Verify
hari	123	ee	[B@13c9936	27.10.2017	Cardiologist,	1013.0	Uploaded in csp	Verify
ram	174	hh	[B@16eda19	27.10.2017	Scientist,	688.0	Uploaded in csp	Verify
chandu	145	holo	[B@b0c913	27.10.2017	Scientist,LifeInstitute,Cardiologist,	867.0	Uploaded in csp	Verify
ram	151	fsds	[B@6121a0	16.07.2019	Scientist,LifeInstitute,Cardiologist,GeneralHospital,	744.0	Not uploaded in csp	Verify

Fig. 3


Secure De-duplication for Data Encryption in Cloud Computing
Home View Profile Details Search Files View Files Status Download Files Logout
User Login
Search
Reset

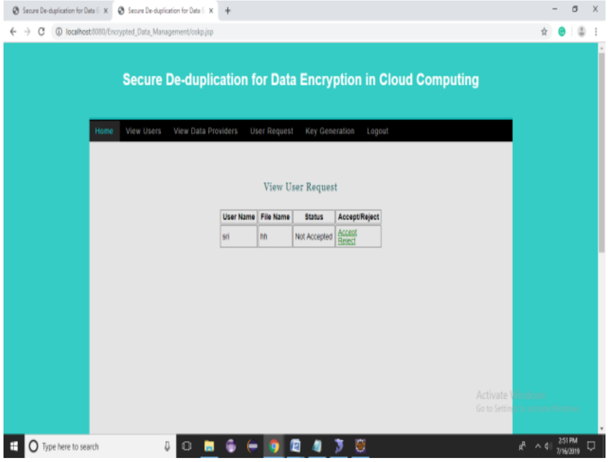
Search For File: hh

Fig. 4 Here user search the files, based on file name


Secure De-duplication for Data Encryption in Cloud Computing
Home View Profile Details Search Files View Files Status Download Files Logout
View File Details

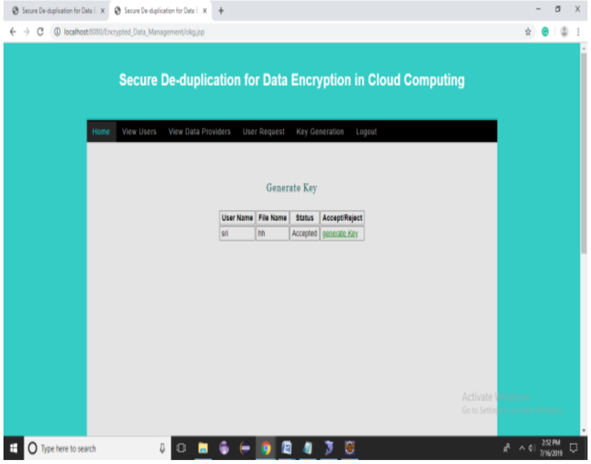
File Name	View Uploaded File	Send Request
hh	[illegible]	Send Request

Fig. 5 Get the results of the searched file name, and then send request that can be forwarded to authority person.


Secure De-duplication for Data Encryption in Cloud Computing
Home View Users View Data Providers User Request Key Generation Logout
View User Request

User Name	File Name	Status	Accept/Reject
sri	hh	Not Accepted	Accept Reject

Fig. 6 The user forwarded request can be viewed by the authority, where authorities accept or reject the request.

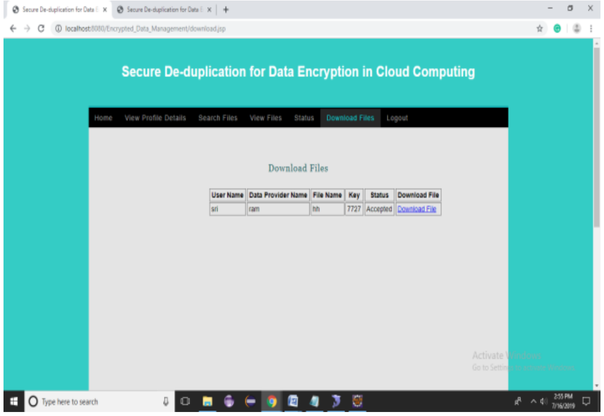


Secure De-duplication for Data Encryption in Cloud Computing

Generate Key

User Name	File Name	Status	Accept/Reject
sri	hh	Accepted	generate Key

Fig. 7 After accepting the request Authority can generate key for file downloading.

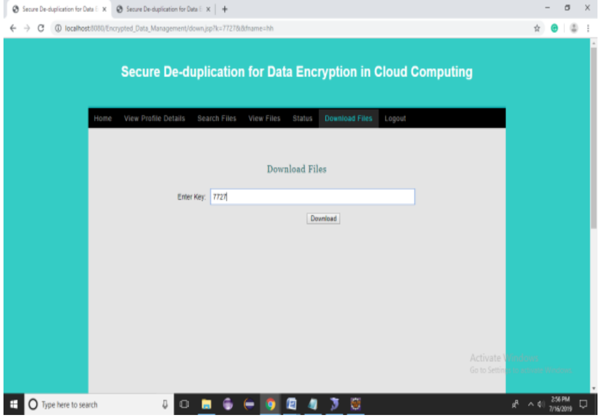


Secure De-duplication for Data Encryption in Cloud Computing

Download Files

User Name	Data Provider Name	File Name	Key	Status	Download File
sri	ram	hh	7727	Accepted	Download File

Fig. 8 Here user view the authority generated key.



Secure De-duplication for Data Encryption in Cloud Computing

Download Files

Enter Key: 7727

Fig. 9 Finally download the file using key

V. Conclusion and Future Scope

Attribute based encryption (ABE) is the most commonly used in registering dispersed data in which the data providers follow the mechanism of redistribution of their data to the cloud after that it can distribute and present the data to customers having demonstrated accreditations. On the other hand, deduplication is a critical method to save the additional room and framework transmission limit, which gets rid of duplicate copies of vague data. In any case, the standard ABE structures don't support secure deduplication, which makes them costly to be associated in some business amassing organizations. In this paper, we acquainted novel route approach, with arrangement of comprehending an attribute based limit system which supports secure deduplication. Our ability system is worked under a cloud designing especially for sorting out the data, where a private cloud monitors and manages the estimation and an open cloud manages the limit. After that, private cloud is assigned with a trapdoor key related with the contrasting figure content, with which it can move the figure message more than single access technique into figure works of the equal plaintext underneath some marvellous access procedures without observing the central plaintext. In the wake of getting a limit request, the private cloud first checks the authenticity of the moved thing through the added proof. If the affirmation is authentic, the private cloud runs a name planning count to see whether comparable data fundamental the figure substance has been secured.

References

[1] D. Quick, B. Martini, and K. R. Choo, Cloud Storage Forensics. Syngress Publishing / Elsevier, 2014. [Online]. Available: http://www.elsevier.com/books/cloud-storageforensics/quick/978-0-12-419970-5

[2] K. R. Choo, J. Domingo-Ferrer, and L. Zhang, "Cloud cryptography:Theory, practice and future research directions," Future Generation Comp. Syst., vol. 62, pp. 51–53, 2016.

[3] K. R. Choo, M. Herman, M. Iorga, and B. Martini, "Cloud forensics:State-of-the-art and future directions," Digital Investigation,vol. 18, pp. 77–78, 2016.

[4] Y. Yang, H. Zhu, H. Lu, J.Weng, Y. Zhang, and K. R. Choo, "Cloud Based data sharing with fine-grained proxy re-encryption," Pervasive And Mobile Computing, vol. 28, pp. 122–134, 2016.

[5] D. Quick and K. R. Choo, "Google drive: Forensic analysis of data remnants," J. Network and Computer Applications, vol. 40, pp. 179–193, 2014.

[6] Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings, ser. Lecture Notes in Computer Science, vol. 3494. Springer, 2005, pp. 457–473.

[7] B.Zhu, K. Li, and R. H. Patterson, "Avoiding the disk bottleneck in the data domain deduplication file system," in 6th USENIXConference on File and Storage Technologies, FAST 2008, February 26-29, 2008, San Jose, CA, USA. USENIX, 2008, pp. 269–282.

[8] M. Bellare, S. Keelveedhi, and T. Ristenpart, "Message-locked encryption and secure deduplication," in Advances in Cryptology-EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings, ser. Lecture Notes in Computer Science, vol. 7881. Springer, 2013, pp. 296–312.

[9] M. Abadi, D. Boneh, I. Mironov, A. Raghunathan, and G. Segev,"Message-locked encryption for lock-dependent messages," in Advances in Cryptology - CRYPTO 2013 - 33rd Annual

Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I, ser. Lecture Notes in Computer Science, vol. 8042. Springer, 2013, pp. 374–391.

[10] S. Keelveedhi, M. Bellare, and T. Ristenpart, “Dupless: Serveraided encryption for DEduplicated storage,” in Proceedings of the22th USENIX Security Symposium, Washington, DC, USA, August14-16, 2013. USENIX Association, 2013, pp. 179–194.

[11] M. Bellare and S. Keelveedhi, “Interactive message-locked encryption and secure deduplication,” in Public-Key Cryptography - PKC2015 - 18th IACR International Conference on Practice and Theory in Public KeyCryptography,Gaithersburg, MD, USA, March 30 - April1, 2015, Proceedings, ser. Lecture Notes in Computer Science, vol.9020. Springer, 2015, pp. 516–538.

[12] S. Bugiel, S. N¨ urnberger, A. Sadeghi, and T. Schneider, “Twinclouds: Secure cloud computing with low latency - (full version),”in Communications and Multimedia Security, 12th IFIP TC 6 / TC11 International Conference, CMS 2011, Ghent, Belgium, October 19-21,2011. Proceedings, ser. Lecture Notes in Computer Science, vol.7025. Springer, 2011, pp. 32–44.

Authors Profile

Mr. A Prasannakumar Reddy pursed Bachelor of Sciences from Annamacharya Institute of Sciences and Technology, Tirupati in the year 2015. He is currently pursuing Master of Science in Sri Venkateswara College of Engineering, Tirupati. His research interests are Cloud Computing, Network Security and Cryptography.

Mr. M. Vikram currently working as an Associate Professor in Sri Venkateswara College of Engineering, Tirupati and he pursuing his Doctorate with the specialization of Data Mining in JNTUA University Ananthapuram. His research interests are Web Data Mining, Data Analytical, Big Data and Cloud Computing.

Dr. N Sudhakar Reddy, currently working as a principal in Sri Venkateswara College of Engineering, Tirupati and he completed his B.E from College of Engineering, GITAM, Visakhapatnam, M.Tech (Computer Science) from College of Engineering JNTU, Anantapur and Ph.D from JNTUA Anantapur in Data mining Specialization. He has been awarded the CMI Level 5 Certificate in Management and Leadership. He has 20 years of Teaching and Research Experience. He worked at various engineering colleges in different positions like Professor, Training and Placement Officer, Head of the Department and Vice Principal.