International Journal of Research in Information Technology

(IJRIT)

www.ijrit.com ISSN 2001-5569

Enabling Fine Grained Multi-Keyword Search Encrypted Cloud Data.

G. Sravan kumar[1], R.Ravali[2]

[1]Assistant Professor, Computer Science and Engineering, Sreyas Institute of Engineering & Technology , JNTU Hyderabad, India.

sravanreddy.golamari@gmail.com[1]

[2] Student, Computer Science and Engineering, Sreyas Institute of Engineering & Technology, JNTU Hyderabad, India.

Ravali.jnu@gmail.com[2]

Abstract

Performing efficient search operations on outsourced cloud data is very important as the cloud operations need to be flexible. There will be ranked keyword search that can help users to have search operations on encrypted cloud data. The ranked search on the outsourced and encrypted cloud data is very important for users of cloud. Many schemes came into existence to support search operations in encrypted cloud data. In this paper we proposed a scheme that supports fine-grained multi-keyword search. In order to achieve this, classified sub-directories are used in order to have fine grained search. The proposed scheme is meant for improving flexible operations on the outsourced data. We built a prototype application to demonstrate the proof of concept. The empirical results revealed that the proposed scheme is useful to have multi-keyword ranked search. This can be used in real world applications where cloud data is accessed by users through searching.

Index Terms – *Cloud computing, keyword search, searchable encryption*

I.INTRODUCTION

Cloud computing has become a reality and organizations are outsourcing their data to cloud for having different services. When data is outsourced it may be subjected to theft or any attack. Therefore the owners of the data are supposed to encrypt data before outsourcing it. This approach can protect data from attacks. However, the search operations become difficult as the data is encrypted and stored. Therefore it is essential to have mechanism for having multi-keyword ranked search. The conceptual overview of the approach is shown in Figure 1.

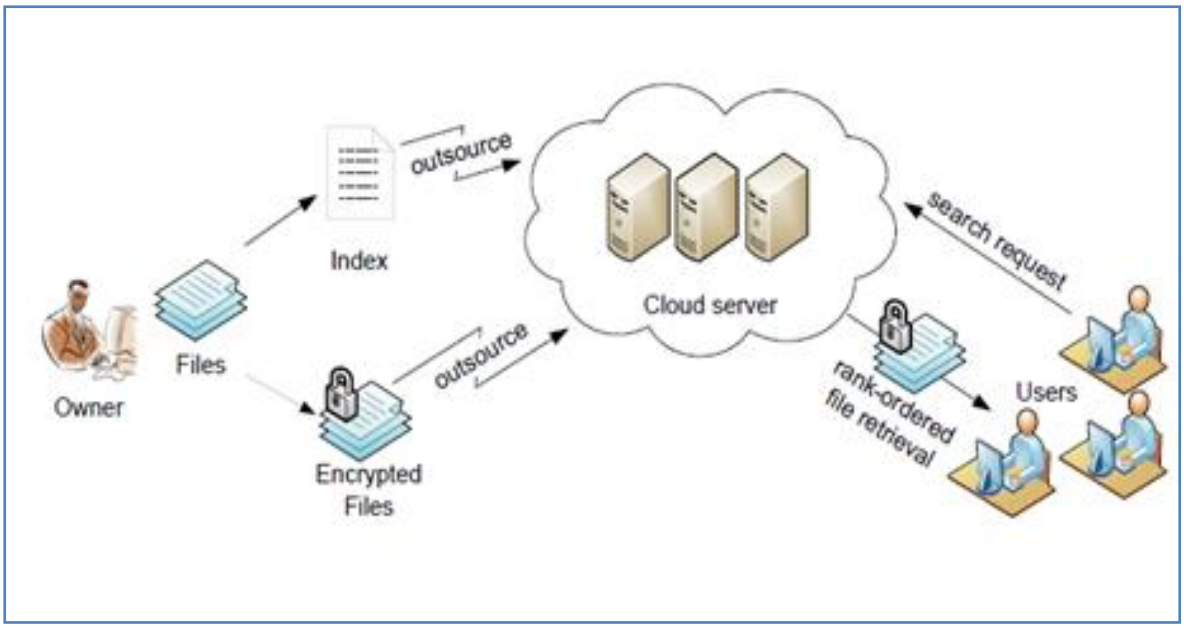

Figure 1: Overview of Search on Encrypted Data

As shown in Figure 1, it is evident that the outsourced data is encrypted and stored in cloud servers. The data is indexed and the encrypted files are saved in cloud. The users can make search request and gain ranked results. In this paper we proposed a multi-keyword ranked search fine grained approach for efficient query processing.
Many schemes came into existence as found in literature. When cloud data is outsourced, it is encrypted before sending to cloud for security reasons. There are two ways in which searchable encryption is made. They are known as Searchable Symmetric Encryption (SSE) and Searchable Public-Key Encryption (SPE). Schemes explored in [1]-[6] are related to the latter while the schemes discussed in [8]-[12] are related to the former technique. The remainder of the paper is structured as follows. Section II provides review of literature. Section III presents the proposed system in detail. Section IV presents experimental results while section V concludes the paper.

II.RELATED WORK

When cloud data is outsourced, it is encrypted before sending to cloud for security reasons. There are two ways in which searchable encryption is made. They are known as Searchable Symmetric Encryption (SSE) and Searchable Public-Key Encryption (SPE).

Searchable Public Key Encryption

The SPE technical was first proposed by Boneh et al. [1] that were supporting searching on encrypted data using single keyword search. However, it was causing heavy overhead. Later on Boneh et al. [2] made a framework for improving it and supported range queries on the outsourced encrypted data. Hwang et al. [3] proposed a multi-keyword search mechanism with conjunctive keyword concept. Zhang et al. [4] explored public key encryption with conjunctive keyword search. The problem with these schemes is that they can return results only when all keywords are matched. Matrix based query scheme proposed by Qin et al. [5] achieved cost-effective solution while multi-keyword top-k scheme proposed by Yu et al. [6] made it highly secure with the help of homomorphic encryption. The concept of expressive queries is more in SPE when compared with that of SSE [7].

Searchable Symmetric Encryption

This scheme was first introduced in [8]. Later on ranked keyword search scheme was proposed in [9] for relevance score of a keyword. However these schemes were not able to provide multi-keyword search efficiently. Multi-Keyword Ranked Search (MRSE) is used in [10] for returning ranked results. K-Nearest

Neighbour (KNN) and relevance score are explored in the multi-keyword search in [11] for accuracy. It improved search efficiency. In [12] authorized and ranked multi-keyword search scheme (ARMS) is proposed for improving search on encrypted cloud data. In this paper we proposed a framework that supports multi-keyword ranked search.

III. IMPLEMENTATION AND RESULTS

We built a prototype application using Java programming language and Java technologies. The proposed system supports multi-keyword ranked search on encrypted cloud data. The application has functionalities that are associated with two roles namely cloud service provider and user. The activities of both the users are shown in Figure 2.

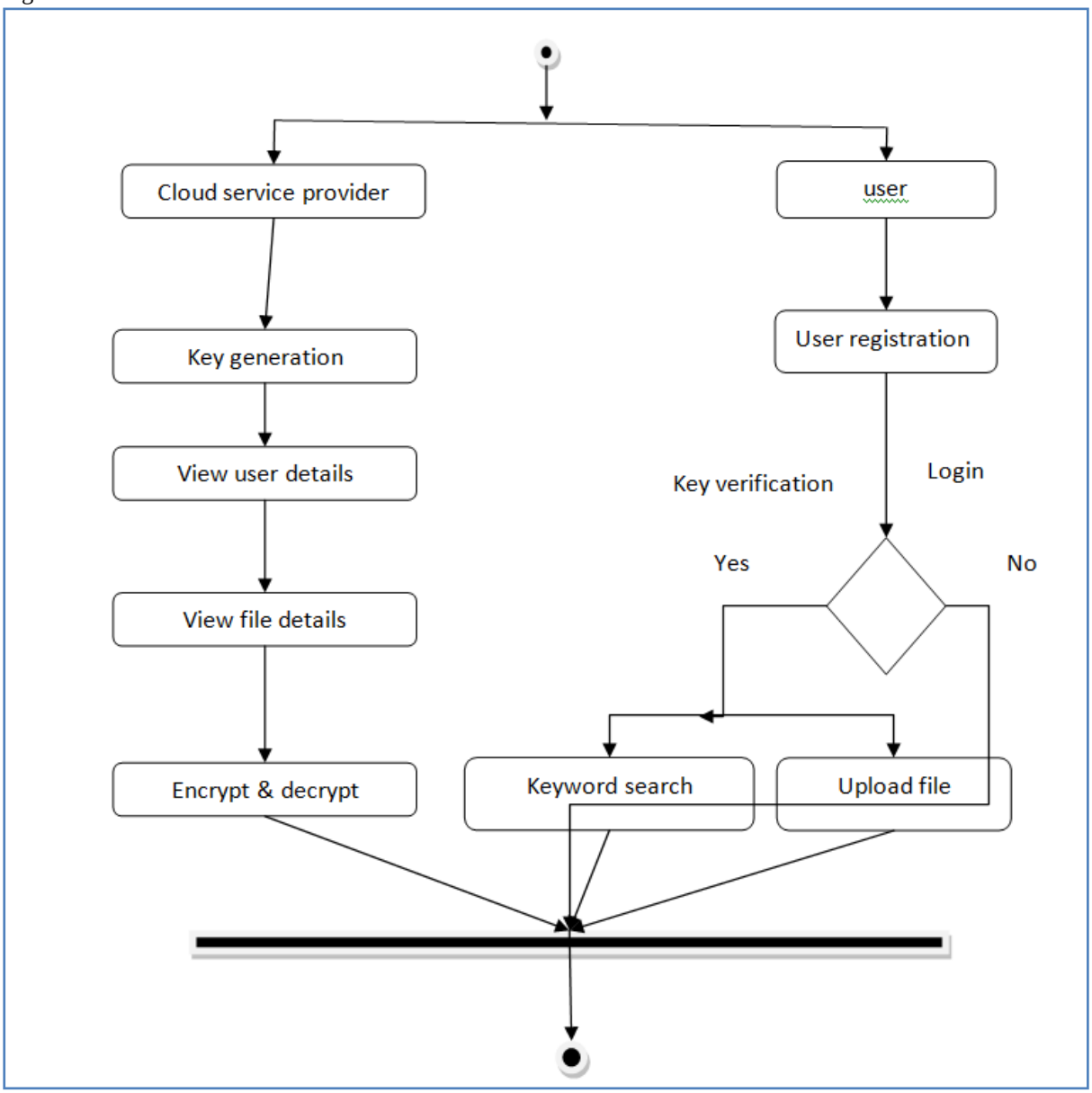

Figure 2: Shows Activities of the Two Roles

As shown in Figure 2, the user can have registration, authentication, uploading data and making multi-keyword ranked search. The cloud service provider can have access to system functionalities such as key generation; viewing user details viewing file details, and performing encryption and decryption.

Experimental Results

Size of dictionary	Existing	Proposed
2000	0	0
4000	100	0
6000	400	20
8000	900	40
10000	1500	100

Table 1: Shows Size of Dictionary and Time Taken

As shown in Table 1, the size of dictionary and the time taken for search are presented. As dictionary size is increased, the time taken is increased for both the systems. However, the proposed system outperforms the existing system in performance.

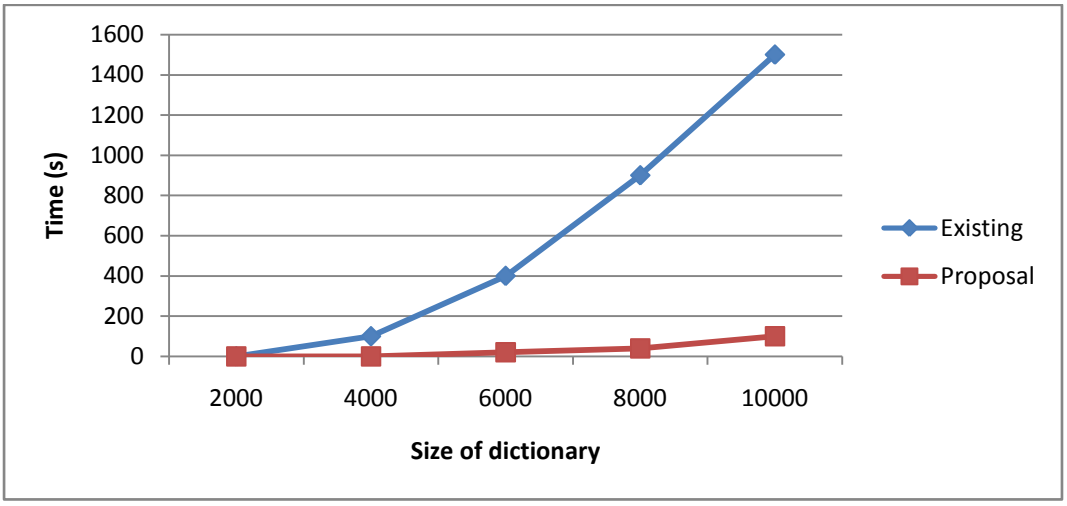

Figure 3: Size of Dictionary vs. Time Taken for Search

As shown in Figure 3, the size of dictionary and the time taken for search are presented. As dictionary size is increased, the time taken is increased for both the systems. However, the proposed system outperforms the existing system in performance.

Number of documents	Existing	Proposed
2000	50	0
4000	100	20
6000	180	30
8000	200	40
10000	350	50

Table 2: Number of Documents and Time Taken

As shown in Table 2, the number of documents and the time taken for search are presented. As number of documents is increased, the time taken is increased for both the systems. However, the proposed system outperforms the existing system in performance.

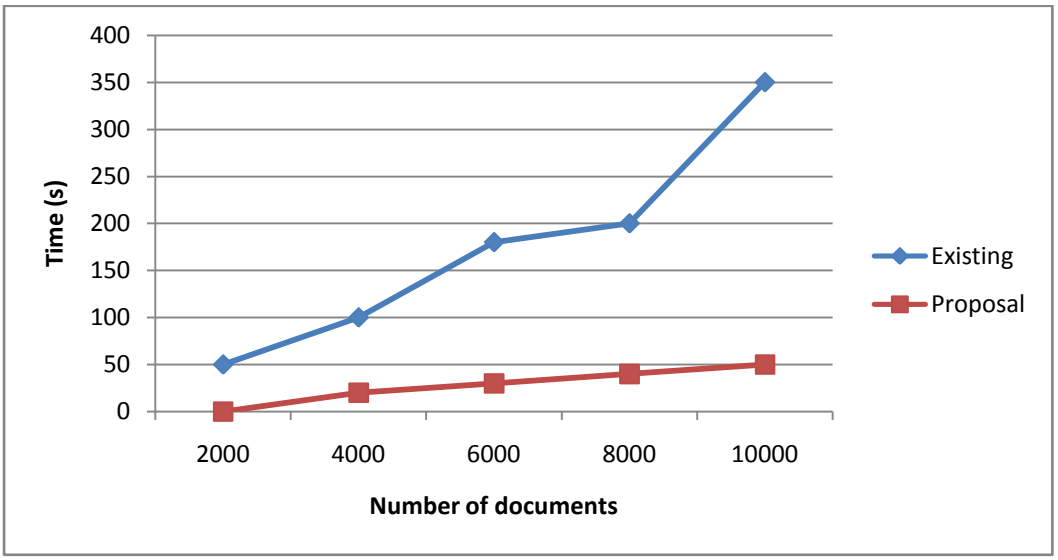

Figure 4: Number of Documents vs. Time Taken

As shown in Figure 4, the number of documents and the time taken for search are presented. As number of documents is increased, the time taken is increased for both the systems. However, the proposed system outperforms the existing system in performance.

Size of dictionary	Existing	Proposed
2000	0	0
4000	180	10
6000	250	20
8000	400	30
10000	450	40

Table 3: Dictionary Size and Time Taken

As shown in Table 3, the size of dictionary and the time taken for search are presented. As dictionary size is increased, the time taken is increased for both the systems. However, the proposed system outperforms the existing system in performance.

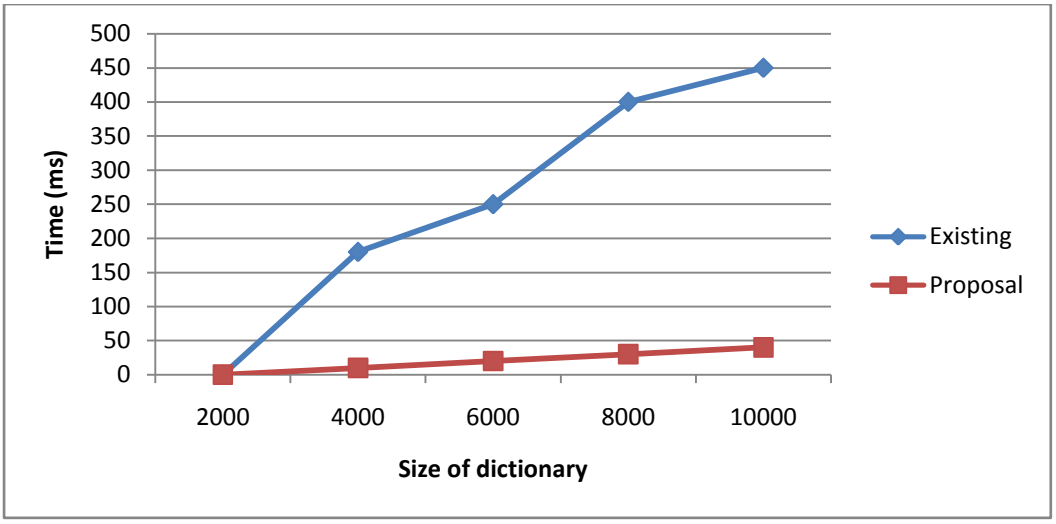

Figure 5: Size of Dictionary vs. Time Taken

As shown in Figure 5, the size of dictionary and the time taken for search are presented. As dictionary size is increased, the time taken is increased for both the systems. However, the proposed system outperforms the existing system in performance.

Number of query keywords	**Existing**	**Proposed**
2000	170	20
4000	160	20
6000	170	10
8000	160	10
10000	170	20

Table 7: Number of Keywords and Time Taken

As shown in Table 7, the number of keywords and the time taken for search are presented. As number of keywords is increased, the time taken is taken differently. However, the proposed system outperforms the existing system in performance.

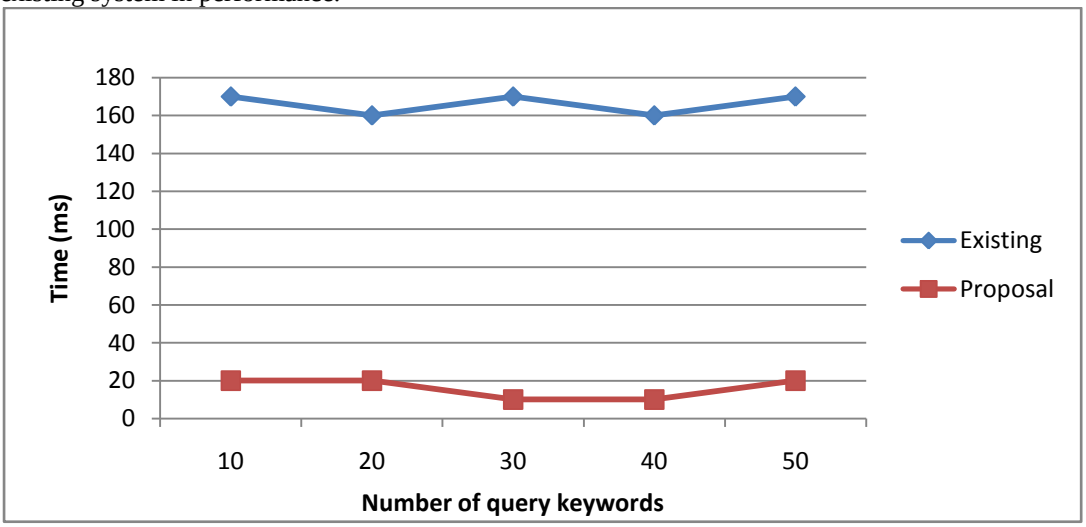

Figure 8: Number of Query Keywords vs. Time Taken

As shown in Figure 8, the number of keywords and the time taken for search are presented. As number of keywords is increased, the time taken is taken differently. However, the proposed system outperforms the existing system in performance.

IV. CONCLUSIONS FOR FUTURE WORK

Cloud computing is widely used in the real world for storing data and managing it easily. The data outsourced to cloud needs to be protected and accessed. It is essential to have search operations on the encrypted data. When encrypted data is searched, it is important to have the mechanism to perform search operations. The ranked search on the outsourced and encrypted cloud data is very important for users of cloud. Many schemes came into existence to support search operations in encrypted cloud data. In this paper we proposed a scheme that supports fine-grained multi-keyword search. In order to achieve this, classified sub-directories are used in order to have fine grained search. The proposed scheme is meant for improving flexible operations on the outsourced data. We built a prototype application to demonstrate the proof of concept. The empirical results revealed that the proposed scheme is useful to have multi-keyword ranked search. We extend this work by using different techniques for more fine-grained search in future.

REFERENCES

[1] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Advances in Cryptology–Eurocrypt*. Springer, 2004, pp. 506–522.

[2] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in *Theory of cryptography*. Springer, 2007, pp. 535– 554.

[3] Y. Hwang and P. Lee, "Zpublic key encryption with conjunctive keyword search and its extension to a multi-user system," in *Proceeding of Pairing*. Springer, 2007, pp. 2–22.

[4] B. Zhang and F. Zhang, "An efficient public key encryption with conjunctive-subset keywords search," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 262–267, 2011.

[5] Q. Liu, C. C. Tan, J. Wu, and G. Wang, "Efficient information retrieval for ranked queries in cost-effective cloud environments," in *Proceedings of INFOCOM*. IEEE, 2012, pp. 2581–2585.

[6] J. Yu, P. Lu, Y. Zhu, G. Xue, and M. Li, "Towards secure multikeyword top-k retrieval over encrypted cloud data," *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 4, pp. 239–250, 2013.

[7] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," *IEEE Transactions on Parallel and Distributed Systems*, vol. DOI: 10.1109/TPDS.2013.282, 2013.

[8] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proceedings of S&P*. IEEE, 2000, pp. 44–55.

[9] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 8, pp. 1467–1479, 2012.

[10] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multikeyword ranked search over encrypted cloud data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 1, pp. 222 233, 2014.

[11] H. Li, D. Liu, Y. Dai, T. H. Luan, and X. Shen, "Enabling efficient multi-keyword ranked search over encrypted cloud data through blind storage," *IEEE Transactions on Emerging Topics in Computing*, 2014, DOI10.1109/TETC.2014.2371239.

[12] H. Li, D. Liu, K. Jia, and X. Lin, "Achieving authorized and ranked multi-keyword search over encrypted cloud data," in *Proceedings of ICC*. IEEE, 2015, to appear.

G. Sravan Kumar Currently working as Assistant Professor in Sreyas Institute of Engineering and Technology, Hyderabad. pursued her B.Tech.and M.Tech. in Computer Science and Engineering from JNTUH.