International Journal of Gender, Science and Technology
..ISSN: 2040-0748

UGC Care Group I Journal
Vol-13 Issue-01 June 2024

Enhanced Security For Cloud Data Sharing And Outsourcing Through User-Side Encrypted File System

Mrs.HARIKA.K[1], Ms.KRISHNAPRIYA.U[2]

#1 Assistant professor in the department of DCA at DVR & DR. HS MIC College of Technology (Autonomous), Kanchikacherla, NTR District.

#2 MCA student in the Department of Computer Applications (DCA) at DVR & DR. HS MIC COLLEGE OF TECHNOLOGY, Kanchikacherla, NTR District

ABSTRACT_ The goal of cloud computing, an emerging paradigm, is to offer flexible data sharing services, large data storage capacity, and computer resources.Businesses and individuals are persuaded to outsource their data to cloud storage systems due to the cloud's top benefits and the exponential rise of data produced.But increasingly, there are concerns about the integrity and confidentiality of sensitive data that is outsourced and stored on distant cloud servers. Before data is stored in the potentially unreliable cloud, it must be encrypted. Data owners are burdened with a significant amount of file management and encryption activities by existing standard encryption methods. They have significant problems with usability, security, and efficiency, and some of the schemes aren't suitable for safeguarding cloud data. We provide OutFS, a user-side encrypted file system, in this work with the goal of transparently encrypting shared and stored external data.

1.INTRODUCTION

Cloud computing is an emerging as the most suitable paradigm for individuals and organizations to access inexpensive,scalable,ubiquitous,and on-demand computing resources,applications,and data storage services.cloud storage systems,such as Dropbox,Google Drive,Apple's iCloud,Microsoft oneDrive,ect..,enable users to remotely store a large volume of data that can be accessed and shared among users,regardless of time and location constraints. with the growing popularity of cloud computing.the number of enterprises and individuals shifting toward the use of cloud has increased rapidly.as a result,a vast amount of important personal information and critical organization data.such as personal health records,government documents,and

company finance data,ect..are transmitted across the internet and stored in cloud servers.however,outsourcing sensitive data suffers from critical security threats,privacy,and access control problems.these are common concerns of organizations and individuals using cloud services.when data owners migrate their sensitive data to the cloud,they lose an element of control over their data .cloud users have no guarantee about the way these sensitive data will be treated and protected by cloud provider.although the cloud provides users with convenience of data access across multiple devices,by using cloud services,user data are vulnerable to a verity of malicious attacks and threats.security incidents occur frequently.even worse,cloud service provider may leak user data to unauthorized entities for illegal profit.

However,the involvement of data owners in performing multiple encryption and decryption operations is cumbersome and time consuming.also,it is difficult for users to manage more than a few keys,and if the keys are leaked or otherwise compromised,security will be threatened.encryption applications are designed to be bandwidth-hungry and latency-sensitive,in which the increased number of outsourced files requiring encryption would significantly affect the system performance and data access response time.we have proposed a user-side encrypted file system named outFS that utilizes the FUSE technology for Linux platforms.moreover we propose a hybrid cryptographic scheme that combines symmetric and public key encryption algorithms in order to improve the security and performance of the personal and shared files that are outsourced

2.LITERATURE SURVEY

2.1 DaSCE: Data Security for Cloud Environment with Semi-Trusted Third Party AUTHORS: Ali, M., Malik, S. and Khan, S.,

Off-site information capacity is a utilization of cloud that alleviates the clients from zeroing in on information capacity framework. However, there are serious security concerns associated with outsourcing data to a third-party administrative control. Attacks by other cloud users and machines may result in data leakage. Discount of information by cloud specialist co-op is one more
issue that is looked in the cloud climate. Thusly, elevated degree of safety measures is required. In this paper, we propose Information Security for Cloud Climate with
Semi-Confided in Outsider (DaSCE), an

information security framework that gives

(a) key administration (b) access control, and (c) record guaranteed erasure. To manage the keys, the DaSCE employs Shamir's (k, n) threshold scheme, in which k shares out of n are required to generate the key.

We utilize numerous key supervisors, each facilitating one portion of key. Multiple key managers keep the cryptographic keys safe from a single point of failure. We

(a) execute a functioning model of DaSCE and assess its presentation in light of the time consumed during different activities, (b) officially model and investigate the working of DaSCE utilizing Undeniable Level Petri nets (HLPN), also (c) confirm the working of DaSCE utilizing Satisfiability Modulo Hypotheses Library (SMT-Lib) also, Z3 solver. Key management, access control, and file assured deletion are all features of DaSCE that can be used effectively to protect outsourced data, as demonstrated by the findings.

2.2 Control Cloud Information Access Honor and Namelessness With Completely Mysterious Trait Based Encryption

Creators: Wan, Z., Wan, M., Jung, T., Li, X. Y., and Wan, Z. Cloud computing is a new computing paradigm that lets you use computing resources in a flexible,

on-demand, and inexpensive way. However, some cloud servers store data, which raises a number of privacy issues. To protect cloud storage, a number of approaches based on attribute-based encryption have been proposed. Anony Control, a semi-anonymous privilege control method, is presented in this paper to address both user identity privacy and data privacy concerns in existing access control methods. In order to prevent identity theft, Anony Control decentralized authority, resulting in semi-anonymity.

In addition, it extends file access control to privilege control, making it possible to fine-tune privilege management for all cloud data operations.

2.3 Web-Based Cloud Computing Services: Fine-Grained Two-Factor Access Control This paper presents a new, fine-grained two-factor authentication (2FA) access control system for web-based cloud computing services by Liu, J. K., Au, M. H., Huang, X., Lu, R., and Li, J.

In particular, an attribute-based access control mechanism is used in our 2FA access control system, requiring a user

secret key and a lightweight security device. The mechanism can improve system security, especially in situations where multiple users share a computer for web-based cloud services because a user cannot access the system without both.

Furthermore, property based control in the framework likewise empowers the cloud server to confine the admittance to those clients with similar arrangement of traits while saving client security, i.e., the

cloud server just realizes that the client satisfies the necessary predicate, however has no clue on the definite character of the client. Last but not least, we perform a simulation to demonstrate the viability of our 2FA system.

3.EXISTING SYSTEM

Existing traditional encryption systems impose a heavy burden of managing files and encryption operations on data owners. They suffer from serious security, efficiency, and usability issues, and some schemes are inappropriate for protecting cloud data.

3.2 PROPOSED SYSTEM

The goal of the suggested file system is to protect files shared or synchronised on open cloud storage platforms.Using robust and dependable encryption, integrity, and key management procedures, all outsourced files are transparently encrypted before being stored on the cloud server.

3.21 IMPLEMENTAION

Data Provider:-

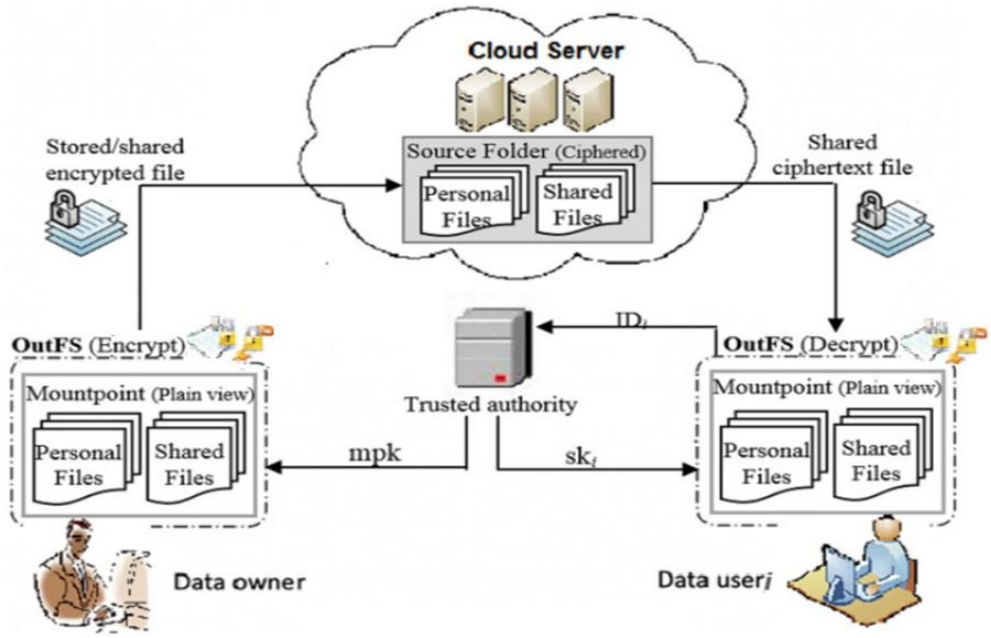
Data provider uploading file to cloud with tag , label and security key , the proposed scheme guarantees data integrity against any tag inconsistency attack. Thus, security is enhanced in the proposed scheme.

Cloud Storage:-

Secure Deduplication with the goal of saving storage space for cloud storage services, Douceur et al the first solution for balancing confidentiality and efficiency in performing deduplication called convergent encryption, where a message is encrypted under a message-derived key so that identical plaintexts are encrypted to the same ciphertexts.

In this case, if two users upload the same file, the cloud server can discern the equal ciphertexts and store only one copy of them. which may violate the privacy of the data if the cloud server cannot be fully trusted .

This is a client who owns data, and wishes to upload it into the cloud storage to save costs. A data owner encrypts the data and outsources it to the cloud storage with its index information, that is, a tag.



Data User : A data user is an individual or organization that utilizes data in various forms for analysis, decision-making, research, or other purposes. Data users may extract, process, interpret, visualize, and present data to derive insights, inform strategies, or solve problems. They may work in fields such as market research, business intelligence, data science, academia, healthcare, government, and more. Data users often rely on databases, spreadsheets, statistical software, and other tools to access, manipulate, and analyze data in order to make informed decisions or generate new knowledge.

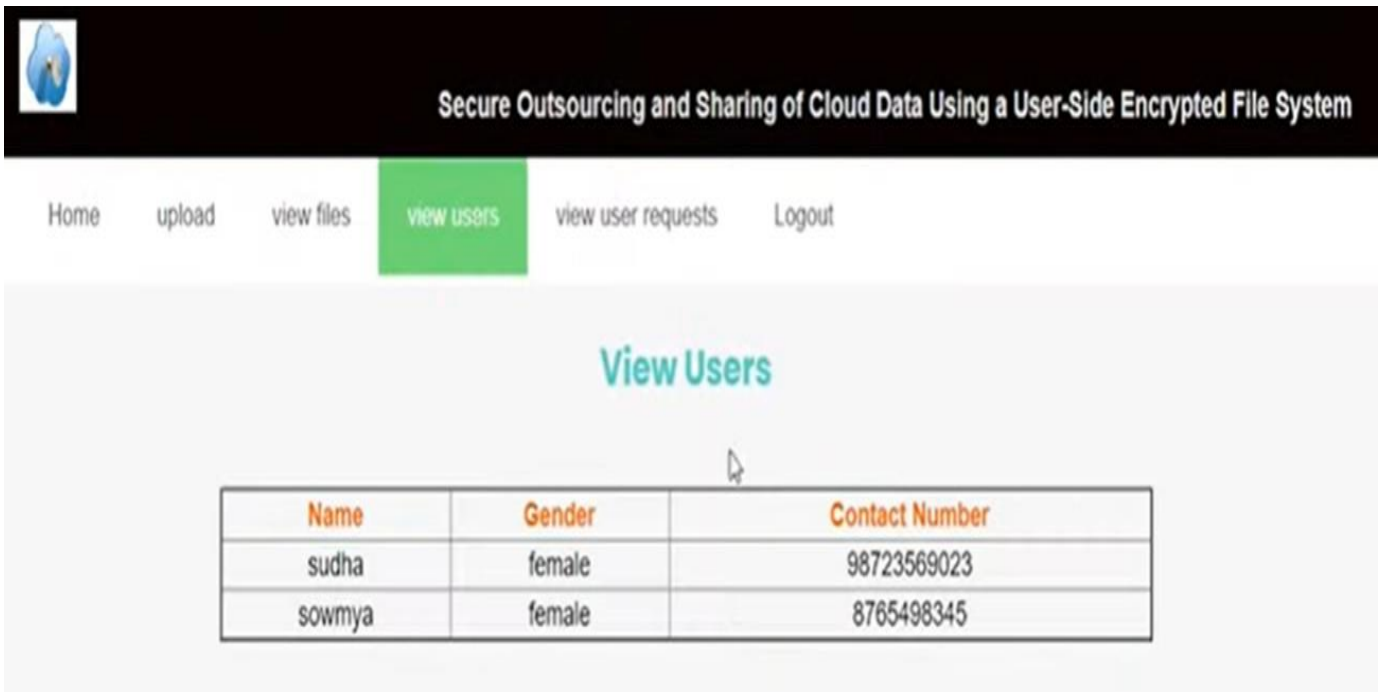
The role of a data user is to collect, manipulate, analyze, and interpret data in order to make informed decisions and drive business growth. Data users are responsible for gathering data from various sources, ensuring its accuracy and validity, and organizing it in a way that makes it useful and actionable. They may use data analytics tools and techniques to uncover trends, insights, and patterns that can help their organization improve operations, identify opportunities, and mitigate risks. Data users also collaborate with other stakeholders within the organization to communicate findings and recommendations, ultimately influencing strategic decision-making.

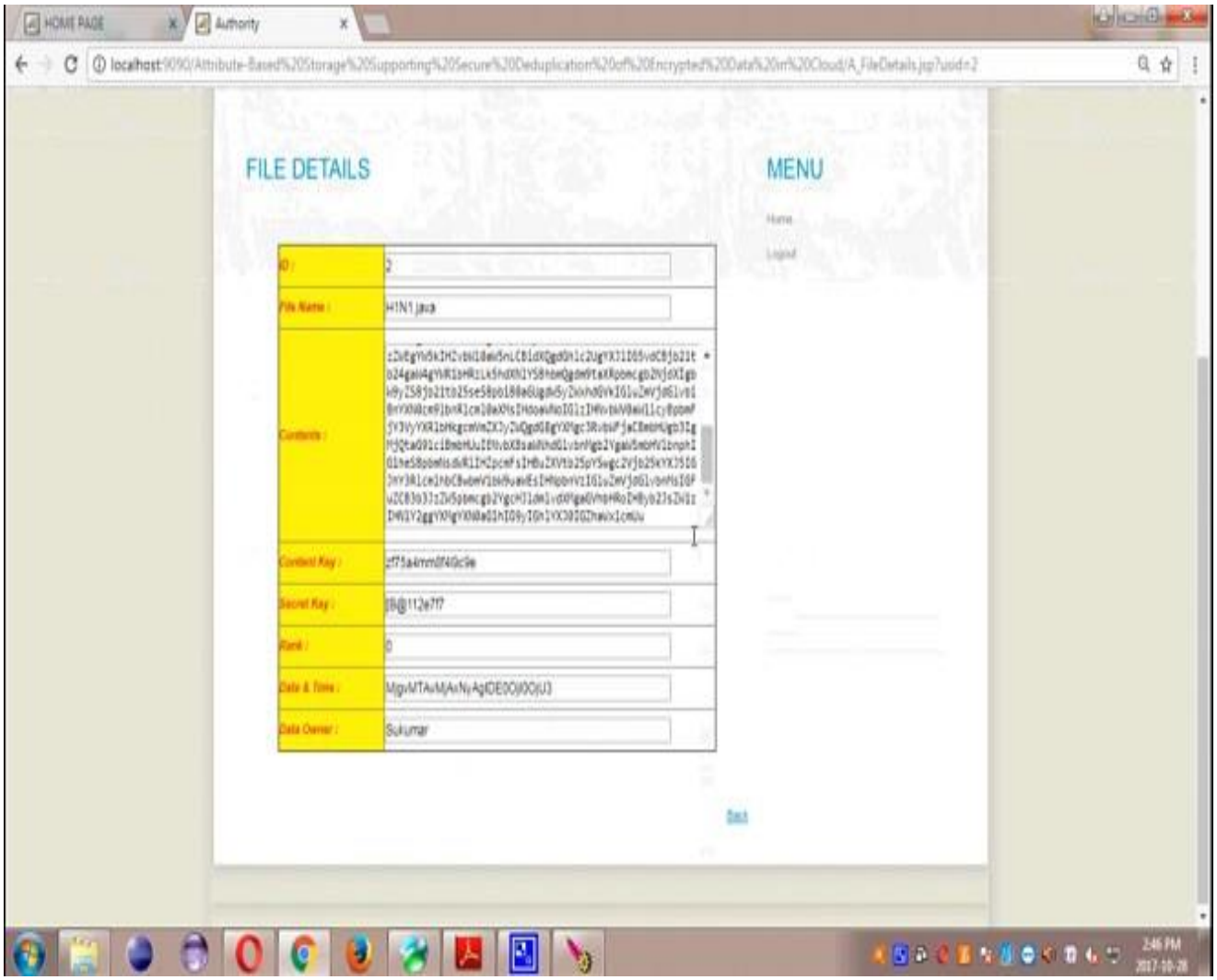
Authority:

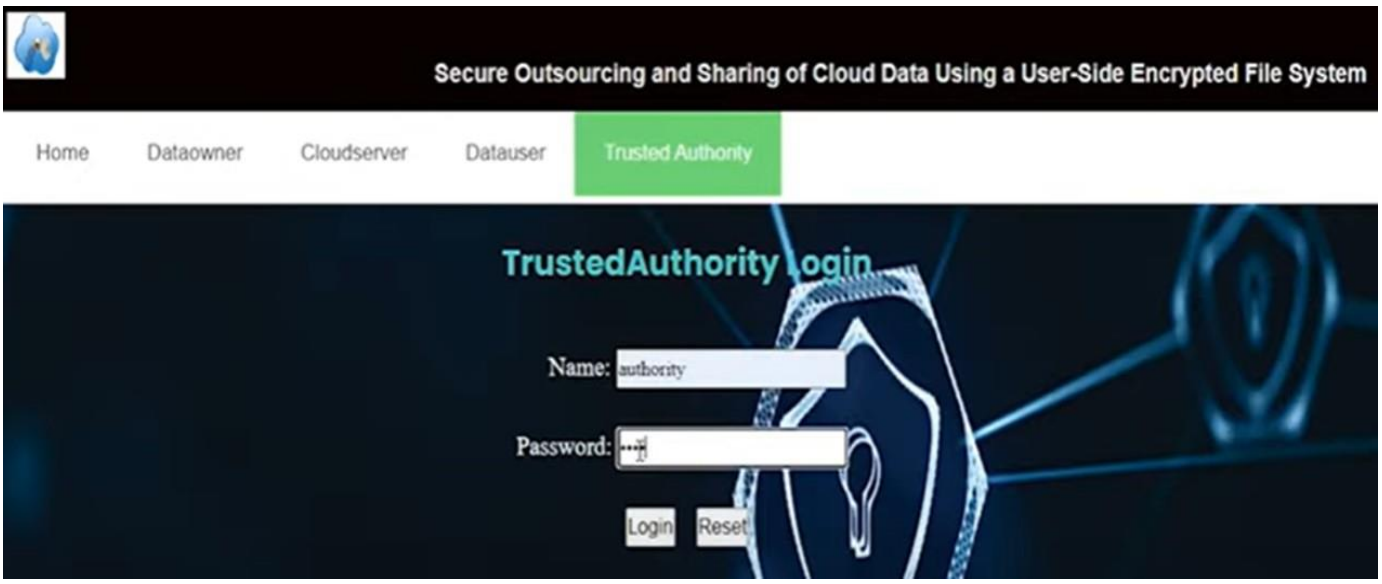
The AA issues every user a decryption key associated with the user set of attributes At the user side, each user can download an item, and decrypt the ciphertext with the attribute-based private key generated by the AA if this user's attribute set satisfies the access structure.

Fig 1:Architecture

4.RESULTS AND DISCUSSION




HOME PAGE
Authority
FILE DETAILS
MENU
Home
Logout
ID :
2
File Name :
H1N1.java
Contents :
Content Key :
Secret Key :
Rank :
Date & Time :
Data Owner :
Sukumar
Back


Secure Outsourcing and Sharing of Cloud Data Using a User-Side Encrypted File System
Home
Dataowner
Cloudserver
Datauser
Trusted Authority
TrustedAuthority Login
Name:
authority
Password:
Login
Reset

MASTER SECRET KEY(MSK) USER REQUESTS

ID	User Name	Owner Name	File Name	Secret Key
1	Rajesh	Sukumar	Dengue.txt	Permitted
2	tmksmanju	Manjunath	Malaria.txt	Permitted
3	tmksmanju	Sukumar	Dengue.txt	Permitted
4	sairam	sai	java.txt	Permitted
5	mba	mca	mca.txt	Permitted
6	projectss	projects	projects.txt	Give Permission

5.CONCLUSION

OutFS is a user-side encrypted file system that is implemented based on FUSE to secure outsourced files to cloud storage systems. It can enforce a secure file system mount over the cloud synchronized directory to perform a transparent encryption on per-file basis using per- file keys. OutFS does not introduce dependencies to the asymmetric encryption ciphers, but rather proposes a hybrid encryption scheme that combines symmetric and asymmetric methods used to encrypt files and file keys, respectively, for the outsourced personal and shared files.

REFERENCES

[1] A Sanchez-Gomez, J. Diaz, L. Hernandez-Encinas, and D. Arroyo, ‘‘Review of the main security threats and challenges in free-access public cloud storage servers,’’ in Computer and Network Security Essentials. Cham, Switzerland: Springer, 2018, pp. 263–281.

[2] J. Domingo-Ferrer, O. Farràs, J. Ribes-González, and D. Sánchez, ‘‘Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges,’’ Comput. Commun., vols. 140–141, pp. 38–60, May 2019.

[3] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, ‘‘A survey on IoT security: Application areas, security threats, and solution architectures,’’ IEEE Access, vol. 7, pp. 82721–82743,2019.

[4] Y.-H. Chang, J. Hu, M. B. Tahoori, and R. F. DeMara, ‘‘Guest editorial: IEEE transactions on computers special section on emerging non-volatile memory technologies: From devices to architectures and systems,’’ IEEE Trans. Comput., vol. 68, no. 8, pp. 1111–1113,Aug. 2019.

[5] A. Khashan and M. AlShaikh, ‘‘Edge-based lightweight selective encryption scheme for digital medical images,’’ Multimedia Tools Appl., vol. 79, pp. 26369–26388, Jul. 2020.

[6] Shucheng Yu, Cong Wang, Kui Ren, and Weijing Lou, “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing,” Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,” Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006

[8] R. Lu, X. Lin, X. Liang, and X. Shen, “Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing,” Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[9] B. Waters, “Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,” Proc. Int’l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008

[10] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yang, “Mona: Secure Multi-Owner Data Sharing for

Dynamic Groups in the Cloud," IEEE Transactions on

AUTHOR PROFILES

Mrs.HARIKA.KONDETI completed her degree Bachelor of Science (BSC) in S.R.S.V.R.G.N.R Degree college. she Completed her Master of Computer Applications(MCA) in Nova College Of Engineering and Technology for Women. Currently working as an Assistant Professor in the department of DCA at DVR & DR HS MIC COLLEGE OF TECHNOLOGY(Autonomous), Kanchikacherla, NTR(Dist), AP. Her areas of interest are Computer Networks , Date base Management system ,Java

Ms. KRISHNAPRIYA.U as MCA Student in the Department of DCA at DVR &DR.HS MIC COLLEGE OF TECHNOLOGY, Kanchikacherla, NTR(DT).She completed her BSC(MPCS) SreeNidhi Degree college(Affiliated to Kakatiya University), Madhira, Khammam District.Her areas of interests are computer Networks, Cloud Computing and security,java.