iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VI **Month of publication:** June 2021

DOI: https://doi.org/10.22214/ijraset.2021.36131

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI June 2021- Available at www.ijraset.com

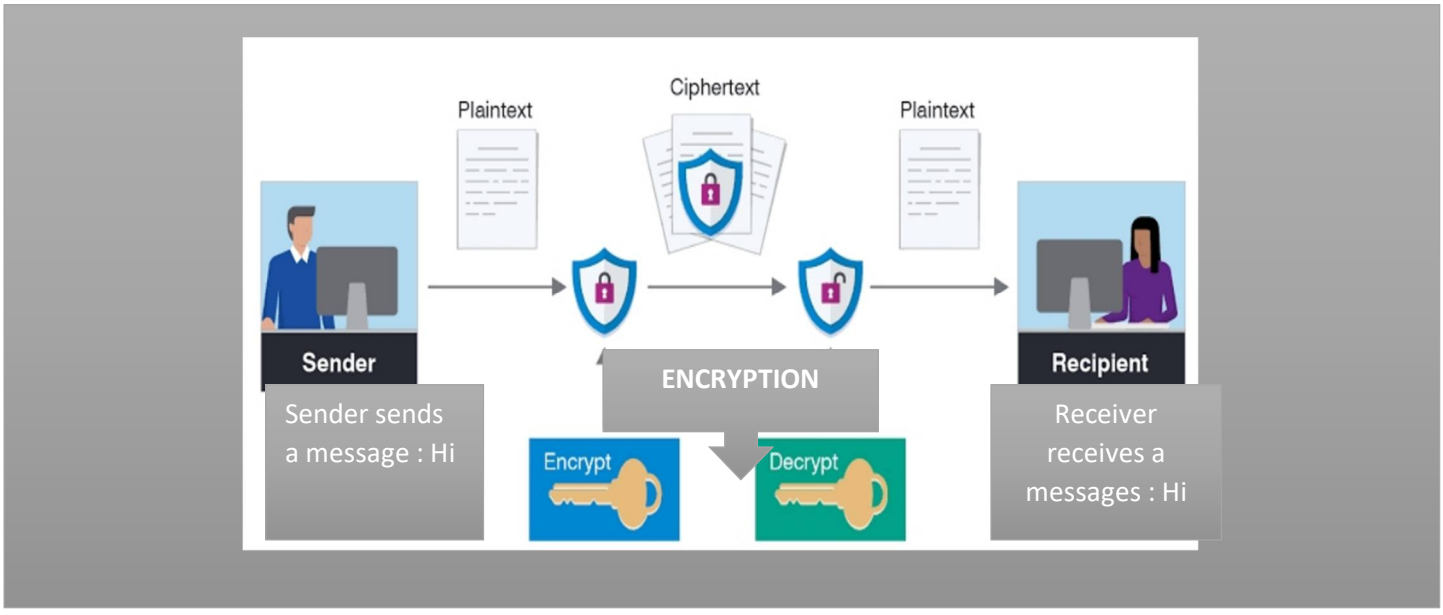
Secure File Storage and Deduplication in Cloud Server Using Cryptography

Somya Das[1], Shubham Kumar[2], Ritik Verma[3], Prof. Swati Tyagi[4]
[1, 2, 3]*Engineering Student, Dronacharya Group of Institutions, Greater Noida*
[4]*Prof. CSE Dept. , Dronacharya Group of Institutions, Greater Noida*

Abstract: ***The security is uppermost issue of any organisation. There are multiple alternatives for assuring the security. We have focussed on a security system and requirements of data centre of cloud using the technique hybrid cryptography. The system includes the encryption and decryption of data using various algorithms like AES, DES, etc. and Client Server Architecture. In addition, there is a technique called Deduplication is a technique for eliminating duplicate copies of repeating data. Deduplication of encrypted data is very useful in order to make a cloud service successful.***
Keywords: Encryption, Decryption, AES, DES, Deduplication.

I. INTRODUCTION

The system is based on the security system and requirements of data centre of cloud using the technique hybrid cryptography. The system includes the encryption and decryption of data using various processes. Blowfish used for the encryption of file slices takes minimum time and has maximum throughput for encryption and decryption from other symmetric algorithms.
In the process of encryption, the system will divide a message into three separate messages and store them into three separate files and all the files will be encrypted using AES, DES algorithm and uses key to encrypt the messages. The key is also stored through the image steganography process to secure the key and also attached the image to the user via e-mail. In the process of decryption, when the user wants to decrypt the files, the user logs into the mail account and the key via mail embedded in the image using image steganography technique. The receiver will receive the key and decrypt the three files that the receiver has using AES, DES. After decryption, the original message can be viewed by the receiver. For the file decryption purpose, reverse process of encryption is applied in order to get the original message back after combining the messages from the files with a secure key. The system has the high level of security to secure the data in between sender and the receiver. The idea of splitting and merging adds on to met the principle of data security. The hybrid approach, when deployed in cloud environment makes the remote server more secure and thus, helps the cloud providers to fetch more trust of their users.



II. PROPOSED METHODOLOGY AND ALGORITHM

The main components of the proposed system are:

a) Data owner: the interface used by the client to use the cloud storage service.

b) Cloud: The server of the cloud service provider (CSP) where operations such as deduplication check using hashing is carried out and the data is stored.

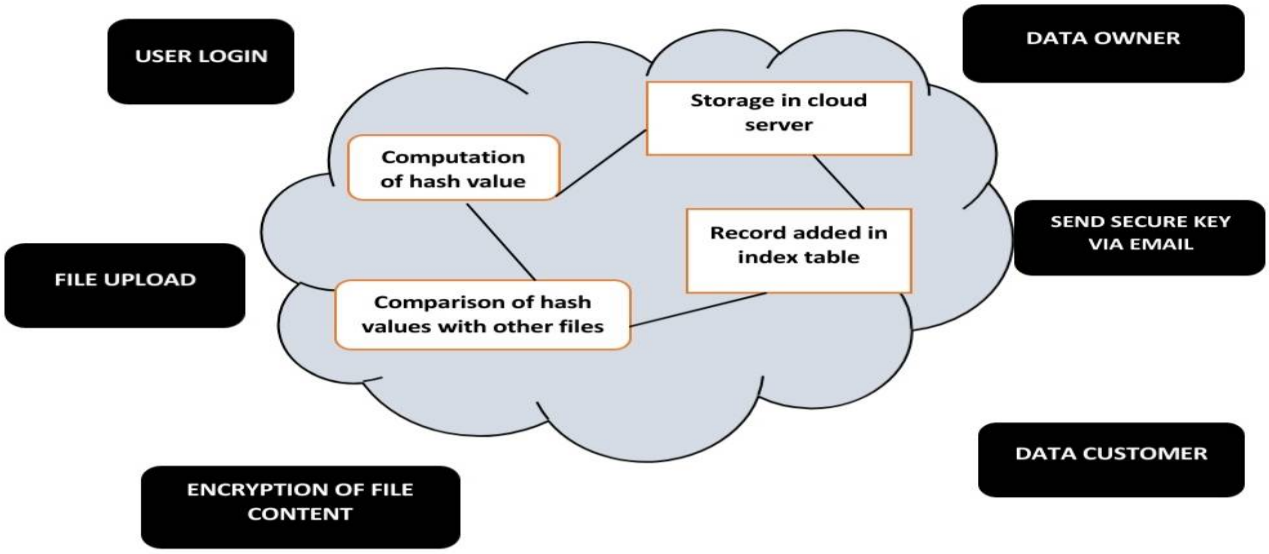
The end user after using the credentials logs into the interface on the CSP webpage. The data is uploaded into the cloud from the client machine by the end user of the CSP and once the data is encrypted and then the data is sent to the CSP server and deduplication is performed. Then, the data owners can view or edit the data but the data customers can only request permission to view the data through the privilege grant module the random access key provided to them by the CSP, once their request to view the document is accepted by the data owner.

A. Alogorithm

1) Data Owner 'ui' login to the CSP interface using his credentials.
2) Data Owner 'ui' chooses his file 'm' in the upload interface.
3) Once user clicks the upload button the machine starts encryption of the file 'm' and generates E (m).
4) This E (m) gets passed on the CSP servers using secure connections.
5) The cipher file E (m) is then computed for its hash value H (E (m)) and is compared with all other files already stored in the cloud. H (E (mj)) where j= no. of files ∈ (1…N).
6) If H (E (m)) = H (E (mj)), then the file is duplicate and, the file is discarded.

The proposed algorithm implement a secure approach to data deduplication. The CSP computes Hash value of cipher text. CSP and Users while functioning, without collusion guarantees that data is never compromised at the cloud storage. The system still has a scope of using a Secure Hashing Algorithm (SHA).

The data to be uploaded needs to be encrypted before sending it to the server of CSP. This is to ensure that data integrity and privacy of user is maintained. This system cloud is used in other web services such as messaging services, web hosting, etc. to make them system more efficient and handle more data volumes.



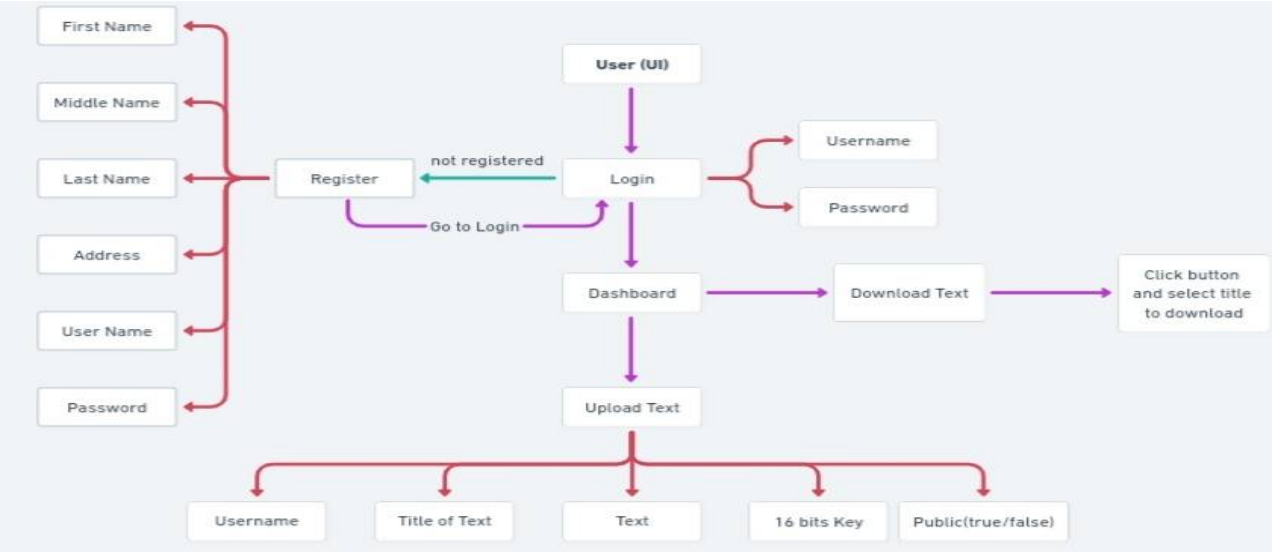
The encryption key attach with the user mail after embedding into an image using the process of steganography (technique for hiding the data) for the receiver to receive the message after the decryption of the message with highly secure and robust algorithm. Cryptography technique translates the original data into unreadable form. It is divided into symmetric key cryptography and public key cryptography. So, only authorised person can access the data from the cloud server

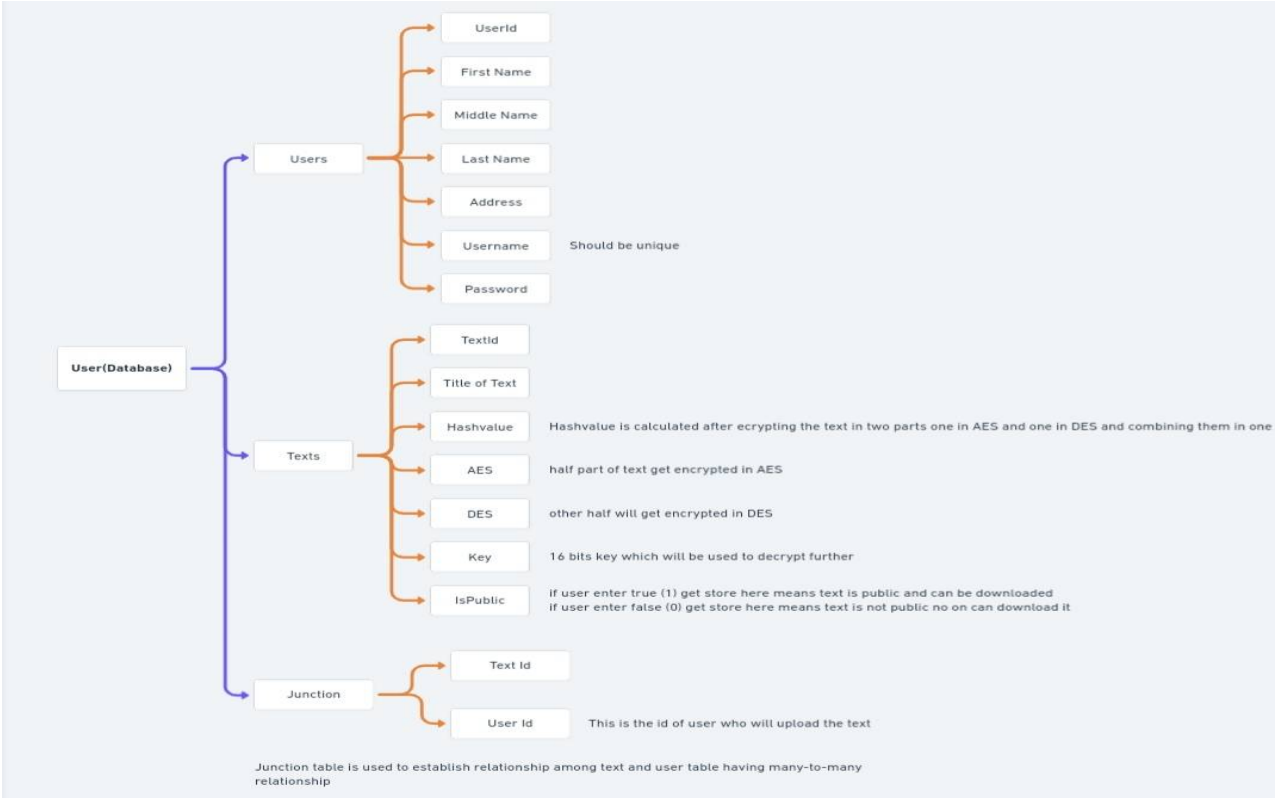
B. Deduplication

Deduplication is a technique for eliminating duplicate copies of repeating data.

Deduplication of encrypted data is very useful in order to make a cloud service successful. In case of big data analytics and other industries where file sizes are huge; the system will bring out simplicity in carrying of these operations. The actual process of data deduplication can be implemented in a number of different ways. We can eliminate duplicate data by simply comparing two files and making the decision to delete one that is older or no longer needed. Deduplication has proved to achieve high cost savings, e.g., reducing up to 90-95% storage needs for backup applications.

There Is A Flow Of Ui Through Which The Process Will Start And Completes





III. SOFTWARE/HARDWARE REQUIREMENTS:

A. Windows 7 or above
B. Wamp server
C. PHP MyAdmin
D. Java NetBeans 8.2
E. Memory – 2 GB
F. Processor – core i3

IV. ADVANTAGES

A. The stored image file is completely secured, as the file is being encrypted by three encryption algorithms.
B. The key is also safe as it embeds the key in image using LSB.
C. The system is very secure and robust in nature.
D. Data is kept secured on cloud server which avoids unauthorised access.

V. CONCLUSION

The entire system has main emphasis on encryption of data and data deduplication using various algorithms. In encryption, there are the algorithms like AES, DES used. Also Hashing algorithms used in the model. The reverse process of encryption is called Decryption which is used to decrypt the message in the system which the receiver receives.

The resolved system is efficient in implementing de duplication in big data files too. The hashing algorithm can be taken of greater bits like SHA1 and SHA2 in order to regulate collision resistance.

This factor defines probability of finding same hash values for different data in files. The process that is put forth follows a very simple to understand and implement approach.

REFERENCES

[1] Vaishnavi Moorthy, Arpit Parwal and Udit Rout, ARPN Journal of Engineering and Applied Sciences VOL. 13, NO. 5, 2018. (DEDUPLICATION IN CLOUD STORAGE USING HASHING TECHNIQUE FOR ENCRYPTED DATA)
[2] Aditya Poduval, Abhijeet Doke, Hitesh Nemade, Rohan Nikam, International Journal of Computer Sciences and Engineering , Vol.-7, Issue-1, Jan 2019. (Secure File Storage on Cloud using Hybrid Cryptography)
[3] Prof. B.A. Jadhawar, Komal A. Bhosale, IARJSET, Vol. 4, Special Issue 4, January 2017**,** Java Interactional Development Environment Programming Tool.
[4] Ako mohammad Abdullah, Dept of Applied maths & CS, published on: 16 june 2017, (AES algorithm to encrypt and decrypt data.

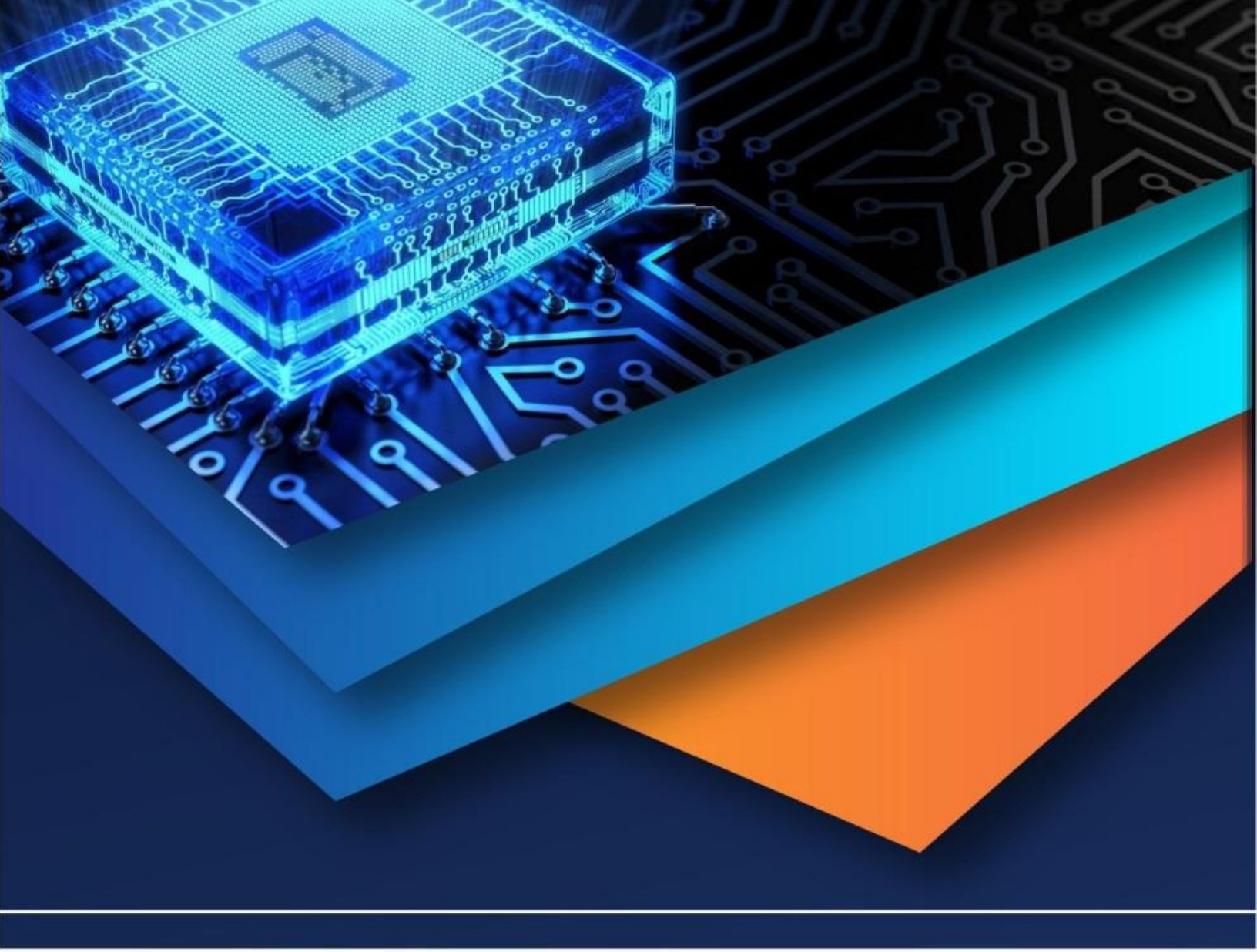
AUTHOR

Somya Das is currently pursuing B.Tech in Computer Science & Engineering from Dr. APJ Abdul Kalam Technical University, Lucknow(Uttar Pradesh). She has wide knowledge of Java Programming, Database Management Systems, SQL, MySQL, PostgreSQL, Cryptography and Web Development.

Shubham Kumar is currently pursuing B.Tech in Computer Science & Engineering from Dr. APJ Abdul Kalam Technical University, Lucknow(Uttar Pradesh). He has wide knowledge of C++ Programming, Data Analytics, Database Management Systems, MySQL and Cloud Computing.

Swati Tyagi has a working experience of 7+ years in academics and currently leading students as Assistant professor of Computer Science & Engineering at Dronacharya Group of Institutions, Greater Noida. She is specialized in Data Structures, Database Management Systems and Problem Solving.

Ritik Verma is currently pursuing B.Tech in Computer Science & Engineering from Dr. APJ Abdul Kalam Technical University, Lucknow(Uttar Pradesh). He has wide knowledge of C++, Database Management Systems, MySQL, and Software Engineering.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY