International Journal for Innovative Engineering and Management Research

PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL

www.ijiemr.org

IJIEMR Transactions, online available on 29th Mar 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 03

10.48047/IJIEMR/V12/ISSUE 03/52

Title **FINE GRAINED CONTROL OF ACCESS TO CLOUD STORAGE USING CP-ABE ENCRYPTION TECHNIQUE**

Volume 12, ISSUE 03, Pages: 365-373

Paper Authors

PINNINTI SAI PREETHI, NANAM PREETHI, AMARTHALURI CHANDRIKA,RAKSHITHA OKALI

International Journal for Innovative Engineering and Management Research

PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL

www.ijiemr.org

FINE GRAINED CONTROL OF ACCESS TO CLOUD STORAGE USING CP-ABE ENCRYPTION TECHNIQUE

[1]PINNINTI SAI PREETHI, [2]NANAM PREETHI, [3]AMARTHALURI CHANDRIKA, [4]RAKSHITHA OKALI

[1,2,3]B. Tech Students, Dept. of CSE, CMR Technical Campus, Medchal, Hyderabad, Telangana, India.

[1]pinnintisaipreethi@gmail.com, [2]nanampreethi@gmail.com, [3]amarthaluri.chandrika@gmail.com

[4]Assistant Professor, Dept. of CSE, CMR Technical Campus, Medchal, Hyderabad, Telangana, India.

[4]rakshitaokali1997@gmail.com

ABSTRACT: Cloud computing has become a popular way to store data, but many people are concerned about entrusting sensitive information to cloud providers who may not provide enough user control. With the development of cloud storage system and its application in complex environment, its data security has been more and more attention. However, previous schemes have not adequately protected against Economic Denial of Sustainability (EDoS) attacks, where attackers can consume cloud resources and cost the payer a great deal of money. This lack of transparency and accountability is a major concern for data owners. In order to solve these issues, Fine grained control of access to Cloud Storage using CP-ABE Encryption Technique. The main aim is to secure encrypted cloud storage from EDoS attacks and provide resource consumption accountability by using CP-ABE schemes in a black-box manner that complies with the arbitrary access policies of CP-ABE. Many data owners choose to outsource encrypted data using Ciphertext-Policy Attribute-based Encryption (CP-ABE) for fine-grained access control. Two protocols are described for different settings and conducted performance. Security is analyzed to demonstrate the effectiveness and efficiency of the presented solution.

KEYWORDS: Cloud Computing, data storage, Security, Ciphertext-Policy Attribute-based Encryption, Access Control

.

I. INTRODUCTION

Cloud computing is an emergent technology in data analytics, which is used to retrieve, store and share big data in a distributed environment. Each day individuals and enterprises are storing their data in the server of the Cloud. The authorities of enterprises and individuals are starting to worry about the safety of big data in the Cloud.

The Cloud provides three types of services such as software, infrastructure and platform, but delivering the security to big data in the Cloud is the most difficult issue [1]. Generally, the government data, medical data and military data include sensitive details that need to be stored in the environment of the Cloud, but users are not sure about the security given by the service providers.

Cloud computing is a unique network or environment where access, maintenance and process can be done from any part of the world. It is a customized internet-based computer server. It is a current trend of modern technology. For the massive computational power, it is the best option for storing data. There is no uncertainty that Cloud Data Server offers quick and solid types of assistance to its customers. When data is storing in the cloud storage the most important thing comes is the security of data. So, in recent years, cloud security is so much important issue because of the increasing of data [4].

Every day, the number of people using cloud computing services increases, and lots of data have been stored in cloud computing environments. Cloud computing has giant blessings that consist of remote storage, mobility, information sharing, value financial savings in hardware and software, etc [3]. The Cloud includes many advantages but still it lacks the security to store data. It is less popular to store the data in a single Cloud because of the failure of resource availability and also it includes some conditions where the inside malicious attackers will steal the data from a single Cloud. Data leakage to cloud services is also increasing every year because of attackers who are always trying to exploit the security vulnerabilities of cloud. Engineers and researchers try to identify the possible cloud threats and attacks in order to implement better security mechanisms to protect sensitive data and cloud computing environments [2].

Cryptography is the way to take care of the security worries of both users and service providers. Cryptography is the technique of encoding users' data to make it incomprehensible and impenetrable during storage or transmission. The very basic security threat that users face, while signing up for a cloud service, is giving open access to a service provider to their personal data. The second threat comes from other users in a shared virtual environment and the third security hazard is privileged access abuse from an outside source. Most cloud computing security solutions are related to cryptography of user's data on service provider's end so that no shared user or outside source can violate a particular user's personal data access rights.

Cryptography is the art of encoding secret information in illegible hidden format using an encryption key. The data is retrieved in its actual form on receiver end by decryption using the same secret key. Only the person with the secret key knowledge has access to the encrypted data and the right to decrypt it. The main ingredients of any cryptography process are: plain data, secret key, encryption algorithm, cipher data and decryption algorithm. Cryptography has two main types: symmetric or private or single key type cryptography and asymmetric or public key type cryptography [5].

Symmetric key cryptography algorithms are AES (Advanced Encryption Standard DES (Data Encryption Standard) 3DES (Triple Data Encryption Standard) IDEA and blowfish. The main issue is deliver the key to receiver into multi user application. These algorithm require low delay for data encode decode but provides low security. Public key cryptography algorithm is RSA and ECC (Elliptic Curve Cryptography) algorithm. Public and private keys are manipulated into public key cryptography algorithms. These algorithms accomplished high level security but increase delay for data encode and decode.

To solve these issues, Fine grained control of access to cloud storage using CP-ABE encryption technique. This technique involves encrypting the data and providing access to authorized users who can decrypt it using the access provided by the data owner. This approach will enable the fine granular access control and ensure security of the shared information. The rest of the work is organized as follows: The section

II describes the literature survey. The section III demonstrates the Fine grained control of access to cloud storage using CP-ABE encryption technique. The section IV evaluates the result analysis of presented technique. Finally the section V ends with conclusion.

II. LITERATURE SURVEY

R.Nivedhaa and J.Jean Justus et. al., [6] describes A Secure Erasure Cloud Storage system using Advanced Encryption Standard algorithm and Proxy Re-encryption. Proxy re-encryption scheme is suggested and combined with a distributed erasure code such that a secure and strong data storage and retrieval, but also lets a user to share his information on the cloud with a different user in the encrypted format itself. This work facilitates the use of encoding the encrypted files and sharing files in the encrypted format itself. This work uses the techniques of both encrypting and sharing the data. Erasure encoding supports sharing encrypted files and is valid in decentralized distributed system. A distributed erasure code is used to authorize the data safety in the dispersed cloud storage.

Rongzhi Wang et. al., [7] presents research on data security technology based on cloud storage. It introduces the implementation of DSBT (data secure storage scheme based on Tornado codes) system based on trusted log and research on data retrieval system as the core of the cloud storage prototype system. The system uses a simple three party security model, with Cassandra as the underlying distributed storage platform; the subsystem needs to carry out the logic module. The key part of this paper also gives a detailed flow chart and interface diagram. System performance test is also put in this part, first introduced the test parameters and the environment, and then for each function of the program design test case, the final result analysis.

Lalitha V.P, Sagar M.Y, Sharanappa S, Shredar Hanji, Swarup R et. al., [8] describes Data Security in Cloud. In this current work the data is stored in the server in encrypted fashion and only the admin is given the writes to decrypt the data. If an unauthorized user is trying to access any file or data from the cloud the admin can block the users IP address from accessing the data so that the security for data is given.

Keke Gai, Meikang Qiu, Hui Zhao et. al., [9] describes Security-Aware Efficient Mass Distributed Storage Approach for Cloud Systems in Big Data. a novel approach is presented that can efficiently split the file and separately store the data in the distributed cloud servers, in which the data cannot be directly reached by cloud service operators. The proposed scheme is entitled as Security-Aware Efficient Distributed Storage (SAEDS) model, which is mainly supported by the presented algorithms, named Secure Efficient Data Distributions (SED2) Algorithm and Efficient Data Conflation (EDCon) Algorithm. the experimental evaluations have assessed both security and efficiency performances.

Yibin Li, Keke Gai, Longfei Qiu, Meikang Qiu, Hui Zhao et. al., [10] describes Intelligent cryptography approach for secure distributed big data storage in cloud computing. This scheme is entitled Security-Aware Efficient Dis- tributed Storage (SA-EDS) model, which is mainly supported by our proposed algorithms, including Alternative Data Distribution (AD2) Algorithm , Secure Efficient Data Distributions (SED2) Algorithm and Efficient Data Conflation (EDCon) Algorithm. The experimental evaluations have assessed both security and efficiency performances and the experimental results depict that our approach can effectively defend main threats from clouds and requires with an acceptable computation time.

III. FINE GRAINED CONTROL OF ACCESS TO CLOUD STORAGE

In this section, Fine grained control of access to cloud storage using CP-ABE encryption technique is presented. The Fig. 1 shows the architecture of presented Fine grained access control to cloud storage using CP-ABE encryption technique. The main objective of this project is to enhance the security of encrypted cloud storage by preventing attacks and ensuring accountability for resource consumption. The system will enable access to data only by authorized users, rather than making it available to everyone.

Data owners: In this module, Data owners are the owner and publisher of files and pay for the resource consumption on file sharing. As the payers for cloud services, the data owners want the transparency of resource consumption to ensure fair billing. The data owners require the cloud provider to justify the resource usage. In our system, the data owner is not always online.

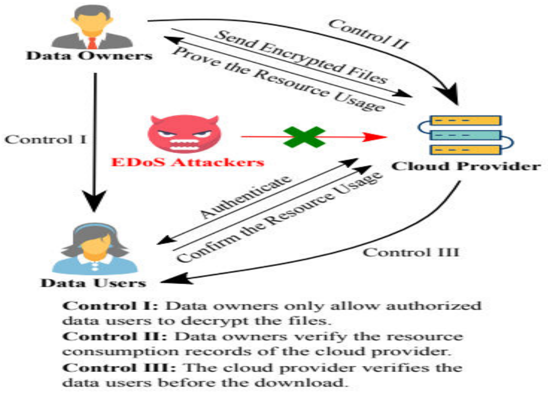

Data Owners
Control II
Send Encrypted Files
Prove the Resource Usage
Control I
EDoS Attackers
Cloud Provider
Authenticate
Confirm the Resource Usage
Control III
Data Users
Control I: Data owners only allow authorized data users to decrypt the files.
Control II: Data owners verify the resource consumption records of the cloud provider.
Control III: The cloud provider verifies the data users before the download.

Fig. 1: The Architecture of Fine grained control of access to cloud storage using CP-ABE encryption technique

Data users: In this module users want to obtain some files from the cloud provider stored on the cloud storage. They need to be authenticated by the cloud provider before the download (to thwart EDoS attacks). The authorized users then confirm (and sign for) the resource consumption for this download to the cloud provider.

Cloud provider: Cloud provider hosts the encrypted storage and is always online. It records the resource consumption and charges data owners based on that record. The cloud is not public-accessible in our system as it has an authentication based access control. Only data users satisfying the access policy can download the corresponding files. The cloud provider also collects the proof of the resource consumption to justify the billing.

Security against EDoS Attacks: EDoS attackers are those that do not satisfy the access policy (i.e., unauthorized users) but want to trigger the cloud provider to send something through the network, as a result the resource consumption increases. To thwart such attacks, the cloud provider uses authentication. The protocols only send a constant amount of bytes to the data user before it passes the cloud-side access control. To succeed a EDoS attack in our definition, the attacker has to first pass the cloud-side access control.

The main focus of this work is to implement Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to enable fine-grained and owner-centric access control for sharing encrypted files with other users. The project utilizes Partially Outsourced Protocols (POP) and Fully Outsourced Protocols (FOP) to ensure accountability for resource consumption.

Attribute-based encryption (ABE) is a type of encryption that allows for access control based on attributes like user characteristics or data properties. This is different from traditional access control methods, such as user names or roles. ABE can provide greater confidentiality compared to other methods, due to its ability to offer fine-grained control over who can access encrypted data. ABE is highly flexible and efficient, making it applicable to various domains and applications. There are several types of ABE schemes, including key-policy ABE. ABE is making crucial advances in solving problems related to confidentiality, and its versatility and efficiency make it an attractive solution for many use cases.

The security requirements of the system are achieved through two key components: 1. A cloud-side access control mechanism that blocks users whose attribute set does not meet the access policy A; 2. A proof-collecting subsystem that allows the cloud provider to collect proofs of resource consumption from users and present them to the data owner later.

Real-world scenarios often involve specifying a maximum expected download time, and data owners can remain offline unless they choose to increase this value. The first protocol, Partially Outsourced Protocol (POP), is designed to address such scenarios. In cases where the data owner cannot set expectations for download times or would be offline for an extended period, the Fully Outsourced Protocol (FOP) can be utilized, allowing the data owner to delegate control to the cloud.

The Partially Outsourced Protocol (POP) involves encrypting an ephemeral key in CP-ABE by the data owner. This key is then used for both message encryption/decryption and cloud-side access control. The data owner provides the cloud provider with a set of N challenge cipher texts $\{enchali\}\in[N]$ and the corresponding hashed challenges $\{hashi\}i\in[N]$.

To prove legitimacy to the cloud provider, the user must show that the decryption result $chalj$ of a randomly selected unused challenge ciphertext $enchalj$ is a pre-image of $hash$. If the user's response is valid, the cloud provider stores the response for further resource consumption accounting. To reduce storage space and improve efficiency, a bloom filter can be introduced for data owners to store their challenge plaintexts. This bloom filter can be stored locally or remotely on the cloud server. As the challenge update process cannot be outsourced to the cloud and must be implemented on demand or periodically by the data owner, the scheme is referred to as the Partially Outsourced Protocol (POP).

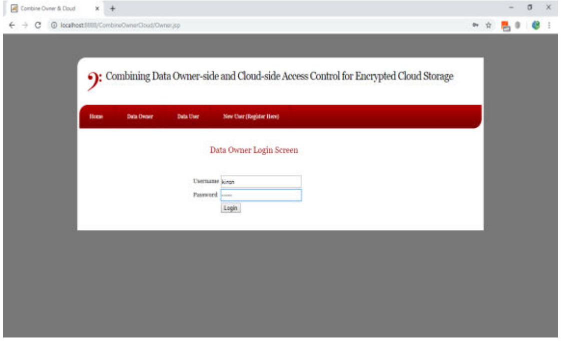
The procedure of POP is done in 4 phases which are as follows: i) Encrypt and Upload (POP-EU): This operation is implemented by an individual data owner independently. ii) Cloud-side Access Control: POP-CR. POP-CR-1: The cloud provider selects one of the unused challenge and sends the following tuple to the user. iii) Challenge update (POP-SU): The scheme allows for on-demand or periodic challenge updates by the data owner, as long as the specified upper bound of download times (N) has not yet been reached. If the data owner wishes to provide additional challenges, they can do so by being online for a short period. The update process is similar to that in the POP-EU-2 phase, using the same key k. The data owner is assumed to keep a record of session keys either in local storage or encrypted form outsourced to the cloud. As the plaintext space for challenges is sufficiently large, it is assumed that no duplicated challenge plaintexts are generated. If a bloom filter is used (and its encrypted form), it will need to be reconstructed in this case. iv) Resource Accounting (POP-RA): Data owners and the cloud interactively implement this operation

The Fully Outsourced Protocol (FOP) is a protocol that allows for outsourced challenge generation and update, as well as resource accounting, without relying on an external PKI. It is based on the signature algorithm and offers two key differences when compared to the Proof of Possession (POP) protocol. Firstly, in FOP, the cloud provider generates the challenges { 〖enchal〗 i }(i∈[N]) instead of the data owners. Secondly, the data owners generate a pair of signature keys (vk, sk) for each file, which users can use to sign a confirmation to prove resource consumption.

The FOP procedure involves four steps: i) Encrypt and Upload (FOP-EU): The data owner encrypts the file using a symmetric key and uploads it to the cloud. The data owner also generates a pair of signature keys (vk, sk) for the file. ii) Outsourced Challenge Generation (FOP-CG): The cloud provider generates the challenges { 〖enchal〗 i }(i∈[N]) for the file, which are then sent to the data owner. This step can be done in advance or on demand. iii)Challenge-Response (FOP-CR): In this step, the data owners and the cloud run the operation. The data owner calculates a response to the challenges sent by the cloud and sends them back. iv) Resource Accounting (FOP-RA): Legitimate users can sign a confirmation using the signature keys (vk,sk) to prove resource consumption. This operation is interactively implemented. Overall, FOP provides a secure and efficient solution for outsourced challenges generation/update and resource accounting, without relying on an external PKI (Public Key Infrastructure.

IV. RESULT ANALYSIS

In this section, Fine grained control of access to cloud storage using CP-ABE encryption technique is implemented. The Fig. 2 shows the login page of presented approach.



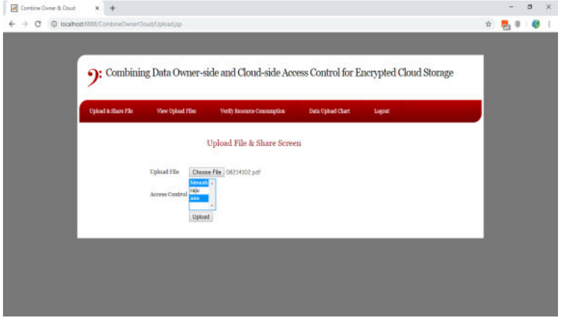
Combining Data Owner-side and Cloud-side Access Control for Encrypted Cloud Storage

Data Owner Login Screen

Username kiran
Password ······

Fig. 2: Log-in Page

After the login the data owner will get access to upload the files in cloud storage. The Fig. 3 shows the files uploading page.



Combining Data Owner-side and Cloud-side Access Control for Encrypted Cloud Storage

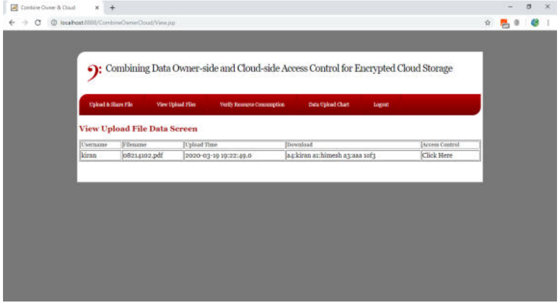
Upload File & Share Screen

Upload File 08214102.pdf

Access Control

Fig. 3: Uploading files to cloud storage

The fig. 4 shows the data file screen.



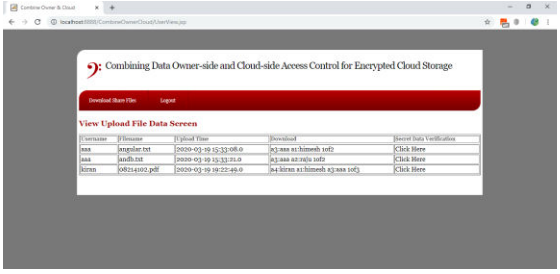
Combining Data Owner-side and Cloud-side Access Control for Encrypted Cloud Storage

View Upload File Data Screen

Username	Filename	Upload Time	Download	Access Control
kiran	08214102.pdf	2020-03-19 19:22:49.0	a4:kiran a1:himesh a3:aaa 1of3	Click Here

Fig. 4: Data File Screen

All uploaded files store in encrypted format inside "WEB-INF/user" folder. In above screen we can see ACCESS POLICY also generated by data owner. Now click on 'View Resource Consumption' link to request cloud to give proof on resource consumption which means how many users access this data owner's file. By using this option we can prevent cloud from cheating or applying fraud resource consumption cost. The Fig. 5 shows the file requesting page.



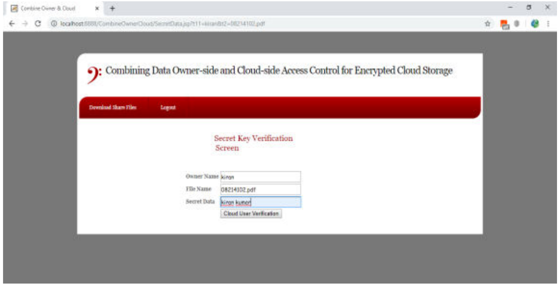
Combining Data Owner-side and Cloud-side Access Control for Encrypted Cloud Storage

View Upload File Data Screen

Username	Filename	Upload Time	Download	Secret Data Verification
aaa	angular.txt	2020-03-19 15:33:08.0	a3:aaa a1:himesh 1of2	Click Here
aaa	andb.txt	2020-03-19 15:33:21.0	a3:aaa a2:raju 1of2	Click Here
kiran	08214102.pdf	2020-03-19 19:22:49.0	a4:kiran a1:himesh a3:aaa 1of3	Click Here

Fig. 5: File requesting page

In above screen data user can see all files from all data owners shared with him. By clicking on 'Click Here' link user can request cloud for file download and will get below screen.


Combine Owner & Cloud
localhost:8888/CombineOwnerCloud/SecretData.jsp?t1=kiran&t2=08214102.pdf
Download Share Files
Logout
Cloud User Verification

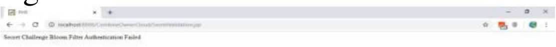
Combining Data Owner-side and Cloud-side Access Control for Encrypted Cloud Storage

Secret Key Verification Screen

Owner Name kiran
File Name 08214102.pdf
Secret Data kiran kumar

Fig. 6: Secret Challenge Page

In above screen cloud is asking data user for secret data challenge and if user give correct data owner secret data then only file will be downloaded otherwise not. If the user enters wrong data then the verification is failed which is shown in Fig. 7.



Secret Challenge Bloom Filter Authentication Failed

Fig. 7: Verification Failed

From Fig. 7 it is clear that secret data verification failed at cloud side and cloud will not allow user to download file if wrong data is entered.

V. CONCLUSION

In this work, Fine grained control of access to cloud storage using CP-ABE encryption technique is presented. The main aim is to enhance the security of encrypted cloud storage by combining access control measures both at the cloud and data owner sides. This approach is designed to resist Distributed Denial of Service (DDoS) and Extreme Denial of Service (EDoS) attacks while also providing resource consumption accounting. This system supports arbitrary Conjunctional Policy Attribute-Based Encryption (CP-ABE) constructions, which are secure against malicious data users and covert cloud providers. We have relaxed the security requirements for the cloud provider to accommodate covert adversaries, a more practical and relaxed notion compared to semi-honest adversaries. To optimize resource consumption accounting and reduce overhead, we utilize bloom filters and probabilistic checks. From the result analysis, it is observed that this approach offers very less overhead compared to existing systems.

VI. ACKNOWLEDGEMENT

We thank CMR Technical Campus for supporting this paper titled "Fine Grained Control of access to cloud storage using CP-abe Encryption Technique", which provided good facilities and support to accomplish our work. Sincerely thank our Chairman, Director, Deans, Head Of the Department, Department Of Computer Science and Engineering, Guide and Teaching and Non- Teaching faculty members for giving valuable suggestions and guidance in every aspect of our work

VII. REFERENCES

[1] Mohan Naik Ramachandra, Madala Srinivasa Rao, Wen Cheng Lai, Bidare Divakarachari Parameshachari,

Jayachandra Ananda Babu and Kivudujogappa Lingappa Hemalatha, “An Efficient and Secure Big Data Storage in Cloud Environment by Using Triple Data Encryption Standard”, Big Data Cogn. Comput. 2022, 6, 101, doi:10.3390/bdcc6040101

[2] Amr M. Sauber Passent M. El-Kafrawy, Amr F. Shawish , Mohamed A. Amin, and Ismail M. Hagag, “A New Secure Model for Data Protection over Cloud Computing”, Hindawi Computational Intelligence and Neuroscience Volume 2021, Article ID 8113253, 11 pages, doi:10.1155/2021/8113253

[3] Mrs. Anjali Sharma, Dr. Garima Sinha, “An Efficient Approach on Data Security with Cloud Computing Environment: A Comprehensive Research”, Turkish Journal of Computer and Mathematics Education Vol.12 No.14 (2021), 1372 – 1382

[4] Md. Alamgir Hossain & Md. Abdullah Al Hasan, “Improving cloud data security through hybrid verification technique based on biometrics and encryption system”, International Journal of Computers and Applications, 2020, DOI: 10.1080/1206212X.2020.1809177

[5] Sameer A. Nooh, “Cloud Cryptography: User End Encryption”, 2020 International Conference on Computing and Information Technology, University of Tabuk, Kingdom of Saudi Arabia. Volume: 01, Issue: ICCIT- 1441, Page No.: 397 - 400, 9th & 10th Sep. 2020

[6] R.Nivedhaa and J.Jean Justus, “A Secure Erasure Cloud Storage system using Advanced Encryption Standard algorithm and Proxy Re-encryption”, International Conference on Communication and Signal Processing, April 3-5, 2018, India

[7] Rongzhi Wang, Research on data security technology based on cloud storage”, 13th Global Congress on Manufacturing and Management, GCMM 2017, Elsevier, doi: 10.1016/j.proeng.2017.01.286

[8] Lalitha V.P, Sagar M.Y, Sharanappa S, Shredar Hanji, Swarup R, “Data Security in Cloud”, International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017)

[9] Keke Gai, Meikang Qiu, Hui Zhao, “Security-Aware Efficient Mass Distributed Storage Approach for Cloud Systems in Big Data”, 2016 IEEE 2nd International Conference on Big Data Security on Cloud, IEEE International Conference on High Performance and Smart Computing, 978-1-5090-2403-2/16, DOI 10.1109/Big Data Security

[10] Yibin Li, Keke Gai, Longfei Qiu, Meikang Qiu, Hui Zhao, “Intelligent cryptography approach for secure distributed big data storage in cloud computing”, Information Sciences 0 0 0 (2016) 1–13, doi:10.1016/j.ins.2016.09.005

Sai Preethi is currently pursuing B. Tech final year in the stream of Computer Science and Engineering in CMR Technical Campus, Medchal, Hyderabad, Telangana, India.

Preethi is currently pursuing B. Tech final year in the stream of Computer Science and Engineering in CMR Technical Campus, Medchal, Hyderabad, Telangana, India.

Chandrika is currently pursuing B. Tech final year in the stream of Computer Science and Engineering in CMR Technical Campus, Medchal, Hyderabad, Telangana, India.

Ms. Rakshitha Okali is working as an Assistant professor in the Department of Computer science and Engineering, CMR Technical Campus, Medchal, Hyderabad. She is having one year of Teaching Experience.