Industrial Engineering Journal
ISSN: 0970-2555

Volume : 52, Issue 7, July : 2023

# Cloud Storage Using the CP-ABE Scheme with Shared Decryption

**Mr. K.Ravichand[1], Miss. Momidi Suvarna [2]**

#1 Associate Professor in Department of CSE, Visvodaya Engineering College, Kavali.

#2M.Tech student in the department of CSE at Visvodaya Engineering College, Kavali, SPSR Nellore (DT).

**ABSTRACT_** A preferred method for controlling access to cloud server data is attribute-based encryption (ABE). However, the authorized decryption user may not always be able to decrypt the ciphertext in a timely manner. Instead of just one user decrypting the ciphertext, multiple alternate users are assigned to work together to be safe. In this paper, we present a shared decryption ciphertext-policy ABE scheme. The messages can be recovered independently by an authorized user. Simultaneously, these other clients (semi-approved clients) can cooperate to receive the messages. We likewise work on the fundamental plan to guarantee that the semi-approved clients play out the unscrambling errands genuinely. Our strategy's efficiency is enhanced by employing an integrated access tree. The standard model demonstrates that the new scheme is CPA-secure. The trial result shows that our plan is exceptionally productive on both computational above and capacity cost.

## 1.INTRODUCTION

Distributed storage [1,2] is another capacity innovation in light of organization and distributed computing, which gives "limitless" capacity assets for information clients. The cloud-based data can be easily accessed by users from any location. Cloud storage servers are storing more personal and business data. By storing their data on the remote cloud storage servers, these businesses and individuals can significantly reduce the cost of data storage and management. In any case, the cloud specialist co-op, for example, Google Cloud, IBM Cloud, and Microsoft Cloud, might be interested or benefit headed to release clients' delicate information. Furthermore, these information put away on remote distributed storage servers might be gone after, altered, and unveiled by programmers. As a result, before storing

their files on an unreliable cloud storage server, users typically encrypt them. To guarantee the accuracy of the documents, a few far off information trustworthiness checking plans [3-7] were proposed. However, there are still issues with the data for cloud storage [8].

In recent years, attribute-based encryption (ABE), which has the potential to guarantee data stored on cloud servers' privacy, has become a hot cryptography research topic. Sahai and co. 9] proposed the idea of ABE as an extension of the previous identity-based encryption. An attribute set replaces a user's identity in the presented ABE. There are two types of current ABE schemes: ciphertext-policy ABE (CP-ABE) and key-policy ABE (KP-ABE) schemes. Goyal et al. [ 10] implemented a KP-ABE plan in 2006. In this plan, an entrance structure is connected with the confidential key of a client. A ciphertext-related attribute set exists simultaneously. In 2007, Bethencourt et al. [ 11] offered a CP-ABE plan. His plan is more reasonable and more adaptable than KP-ABE conspire. In a CP-ABE conspire, a quality set is connected with the confidential key of the client, while an entrance structure is connected with the code text. The cipher text can only be decrypted by a user whose attribute set meets the access policy.

Later, a number of ABE plans [12-26] were suggested. ABE schemes with a hidden access structure have been proposed [12, 15] to safeguard user privacy. Multi-authority ABE [16-21] schemes are presented because user attributes typically are managed by multiple authorities. To make decryption more user-friendly, ABE schemes with outsourced decryption (ABE-OD) [22, 25] have been proposed. To make ABE-encrypted data more searchable, searchable ABE schemes have been proposed [25,26]. Data access control systems are increasingly incorporating ABE [27-32].

From the perspective of the users, the two primary requirements for any ABE scheme are efficiency and security. Enhancing the effectiveness of these existing secure ABE schemes is crucial. Wang et al. in 2016 33] offered a file hierarchical cipher text-policy attribute based encryption (FH-CP-ABE) method

that significantly enhanced scheme [11]'s efficiency without compromising security. These public cloud-stored data files frequently exhibit a multi-level hierarchy. Conspire [33] joins various different progressive access strategy trees into a solitary one. As depicted in Fig. On access, file 1 m and file 2 m are linked in a hierarchy. Access tree 1 can be coordinated with access tree 2 into another entrance tree . Finally, rather than encrypting file 1 m twice with two distinct access trees, file 2 m and file 1 m can be encrypted simultaneously using the access tree. Scheme [33] is effective for both encryption and decryption, and it also greatly reduces the cipher text's storage overhead. However, scheme [33] is not appropriate for a multi-authority system in which a user's attributes are managed by multiple authorities. To address the issue, Zhang et al. [ 34] better above FH-CP-ABE conspire and gave a multi-authority various leveled ABE plot. There are different experts in plot [34] and a coordinated admittance tree is utilized to scramble these progressive records. However, scheme [34] includes a centralized authority, which is insufficient for distributed systems. Guo et al. based their solution to this problem on the hierarchical structure of personal health record (PHR) files [ 35] furnished a special ABE plot with various specialists. What's more, Li et al. [ 36] gave a more down to earth document progressive CP-ABE plan to defeat the impediment that FH-CP-ABE conspire [33] can't scramble more than one record in a similar level. Scheme [36] can securely and effectively store data in the cloud for large institutions or businesses, making it more adaptable and practical than scheme [33]. However, the above schemes [33-36] will fail due to the absence of integrated access trees if the stored files do not exhibit the characteristics of multiple hierarchical structures. Fu et al. [] propose a solution to this problem: To encrypt a collection of documents, 37] proposed an attribute-based hierarchy encryption scheme (ABHE). In view of the entrance credits of these records in the report assortment, a coordinated admittance tree is built with a covetous calculation in conspire [37]. Finally, the integrated access tree is used to encrypt the document collection, just like the previous scheme [33-36]..

## 2.LITERATURE SURVEY

**2.1) S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya, “Cloud-based**

**augmentation for mobile devices: motivation, taxonomies, and open challenges," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 337–368, 2014.**

Recently, Cloud-based Mobile Augmentation (CMA) approaches have gained remarkable ground from academia and industry. CMA is the state-of-the-art mobile augmentation model that employs resource-rich clouds to increase, enhance, and optimize computing capabilities of mobile devices aiming at execution of resource-intensive mobile applications. Augmented mobile devices envision to perform extensive computations and to store big data beyond their intrinsic capabilities with least footprint and vulnerability. Researchers utilize varied cloud-based computing resources (e.g., distant clouds and nearby mobile nodes) to meet various computing requirements of mobile users. However, employing cloud-based computing resources is not a straightforward panacea. Comprehending critical factors (e.g., current state of mobile client and remote resources) that impact on augmentation process and optimum selection of cloud-based resource types are some challenges that hinder CMA adaptability. This paper comprehensively surveys the mobile augmentation domain and presents taxonomy of CMA approaches. The objectives of this study is to highlight the effects of remote resources on the quality and reliability of augmentation processes and discuss the challenges and opportunities of employing varied cloud-based resources in augmenting mobile devices. We present augmentation definition, motivation, and taxonomy of augmentation types, including traditional and cloud-based. We critically analyze the state-of-the-art CMA approaches and classify them into four groups of distant fixed, proximate fixed, proximate mobile, and hybrid to present a taxonomy. Vital decision making and performance limitation factors that influence on the adoption of CMA approaches are introduced and an exemplary decision making flowchart for future CMA approaches are presented. Impacts of CMA approaches on mobile computing is discussed and open challenges are presented as the future research directions

**2. 2) Control Cloud Data Access Privilege and Anonymity With Fully**

Industrial Engineering Journal
ISSN: 0970-2555

Volume : 52, Issue 7, July : 2023

**Anonymous Attribute-Based Encryption**

**AUTHORS:** Jung, T., Li, X. Y., Wan, Z. and Wan, M

Although some cloud servers store data, which raises a number of privacy concerns, cloud computing is a revolutionary computing paradigm that enables flexible, on-demand, and low-cost resource utilization. To protect cloud storage, a number of approaches based on attribute-based encryption have been proposed. However, identity privacy and privilege control receive less attention than data content privacy and access control in most projects. AnonyControl, a semi-anonymous privilege control method, is presented in this paper to address the data privacy and user identity privacy concerns of existing access control methods. To prevent identity leaks, AnonyControl decentralizes 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. Then, we present the AnonyControlF, which achieves complete anonymity and completely prevents identity leakage. Our performance evaluation demonstrates the viability of our schemes, and our security analysis demonstrates that, under the DBDH assumption, both AnonyControl and AnonyControl-F are secure.

**3.PROPOSED SYSTEM**

To solve the aforementioned issue, the proposed system proposed the CP-ABE with shared decryption (CP-ABE-SD) scheme. In our solution, in addition to the authorised user, multiple delegated users may also work together to recover the message. We can simultaneously confirm the accuracy of the results of the decryption. An integrated access tree is used in our scheme as that in the scheme to reduce the computation cost for encryption and decryption and save storage costs. Finally, the integrated access tree encrypts the plaintext. Cloud storage is very inefficient because it requires frequent data encryption and decryption operations. Our system only encrypts the shared message once, and the ciphertext is compact. Our approach boosts the effectiveness of cloud storage.

**3.1 IMPLEMENTATION**

- **Data Owner**

In this module, the data provider uploads their encrypted data in the Cloud server. For the security purpose the data owner

encrypts the data file and then store in the server. The Data owner can have capable of manipulating the encrypted data file and performs the following operations Register and Login, Add Document, View Uploaded and Verify Details.

- **Cloud Server**

The **Cloud** server manages which is to provide data storage service for the Data Owners. Data owners encrypt their data files and store them in the Server for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the Server and then Server will decrypt them. The server will generate the aggregate key if the end user requests for file authorization to access and performs the following operations such as Login, Attackers, Authorize User, Authorize Owner, View Documents, Top Searched Keywords, Search Keyword Chart,

View File Rank Chart .

**User**

In this module, the user can only access the data file with the secret key. The user can search the file for a specified keyword. The data which matches for a particular keyword will be indexed in the cloud server and then response to the end user and user will do the following operations Register and Login, Search, My Profile, View Files, Request Secret Key and Public Key Permission, Request Hash Key Permission.

- **Trusted Authority –**is responsible for Login, View Files, View Transactions, Generate Hash Code, View Keys Requests and Permit**.**

.

Industrial Engineering Journal
ISSN: 0970-2555

Volume : 52, Issue 7, July : 2023

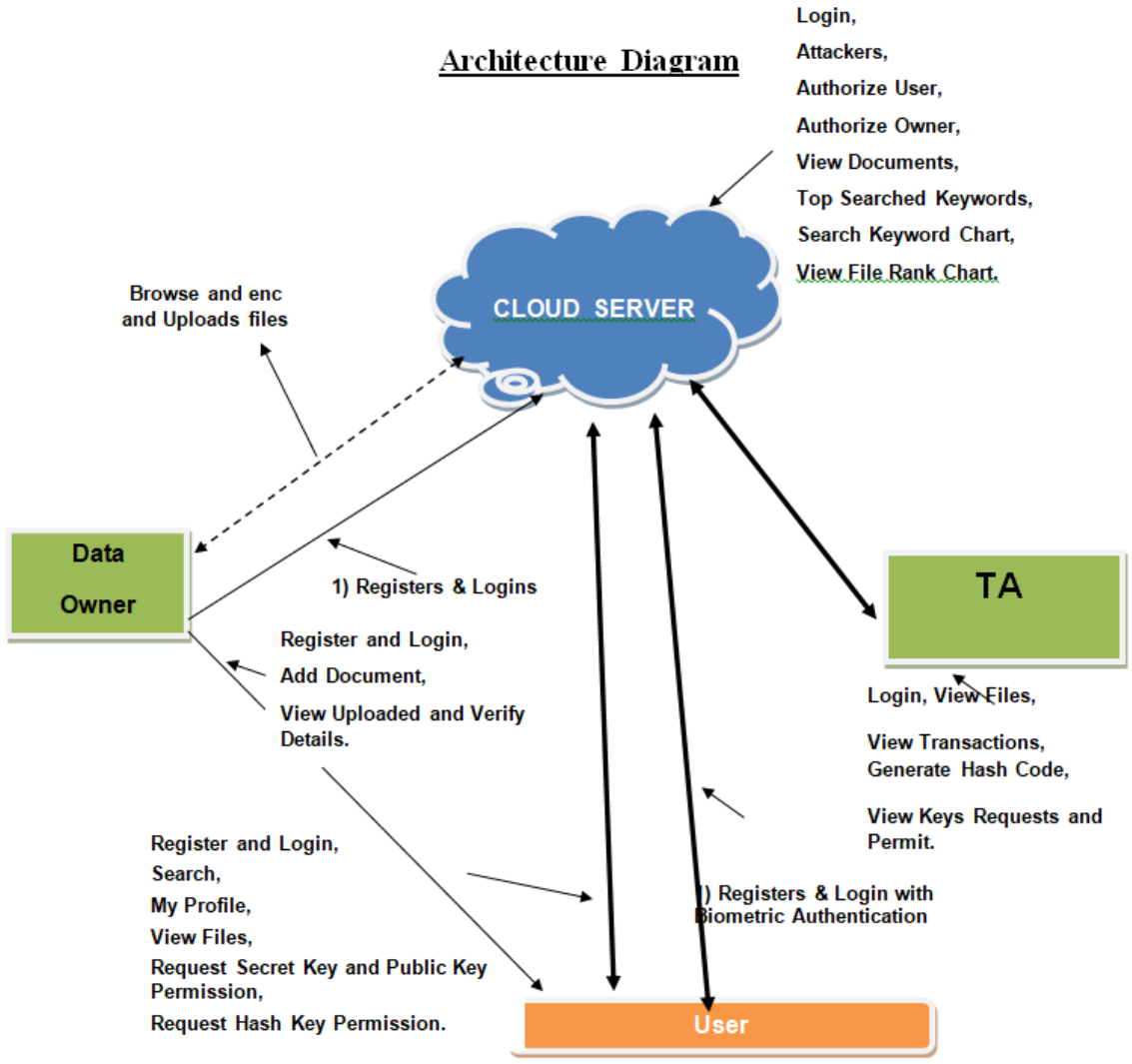


**Fig 1: Architecture**

## 4.RESULTS AND DISCUSSION

Industrial Engineering Journal
ISSN: 0970-2555

Volume : 52, Issue 7, July : 2023

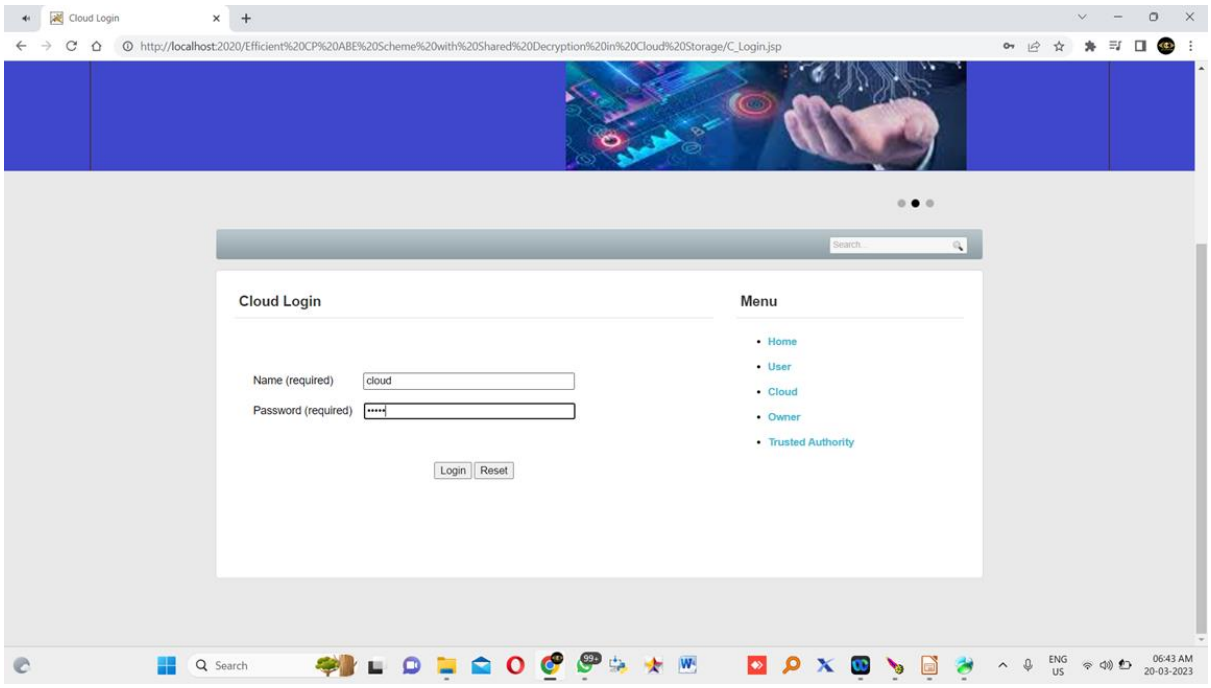


**Fig 2:in this screen cloud can login by using name and password**

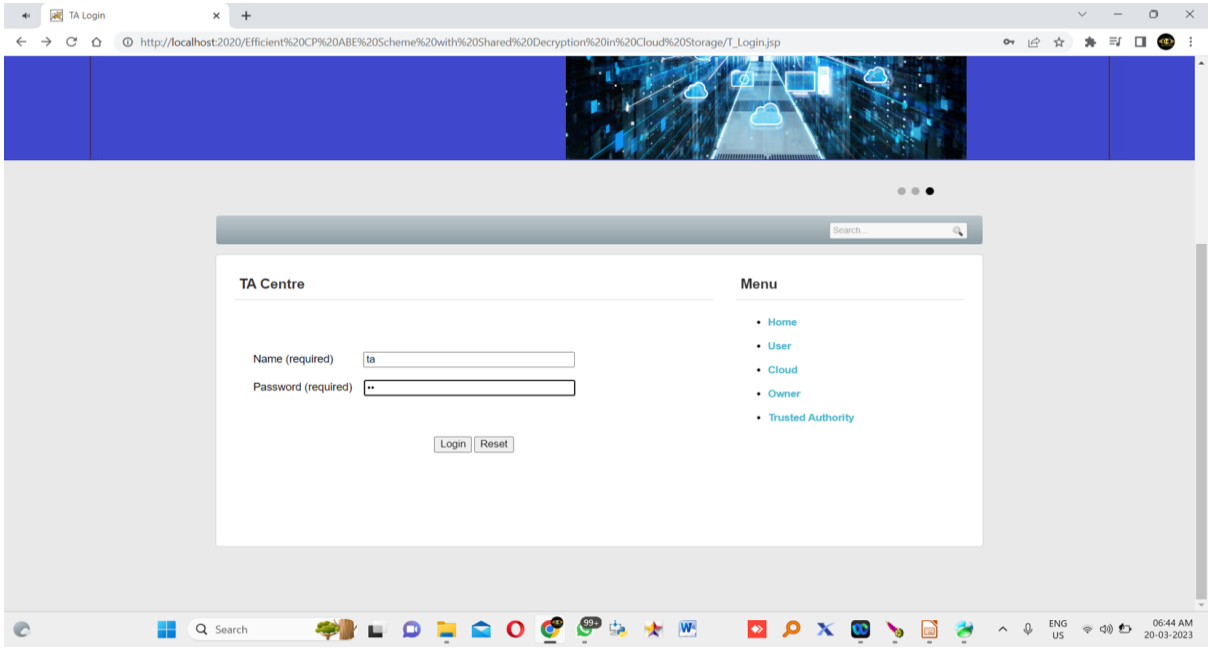


**Fig 3:in this screen TA can login by using name and password after login they can perform future actions**

Industrial Engineering Journal
ISSN: 0970-2555

Volume : 52, Issue 7, July : 2023

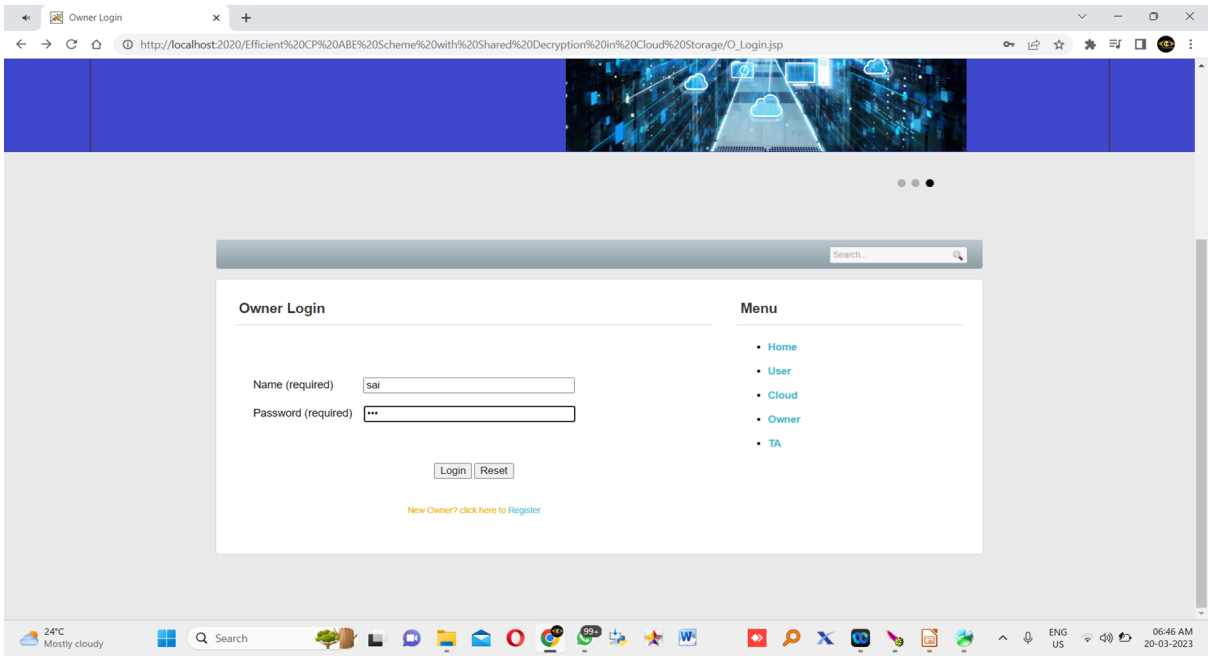


**Fig 4:in this screen data owner can login by using name and password before that they has register after registration only they can login**

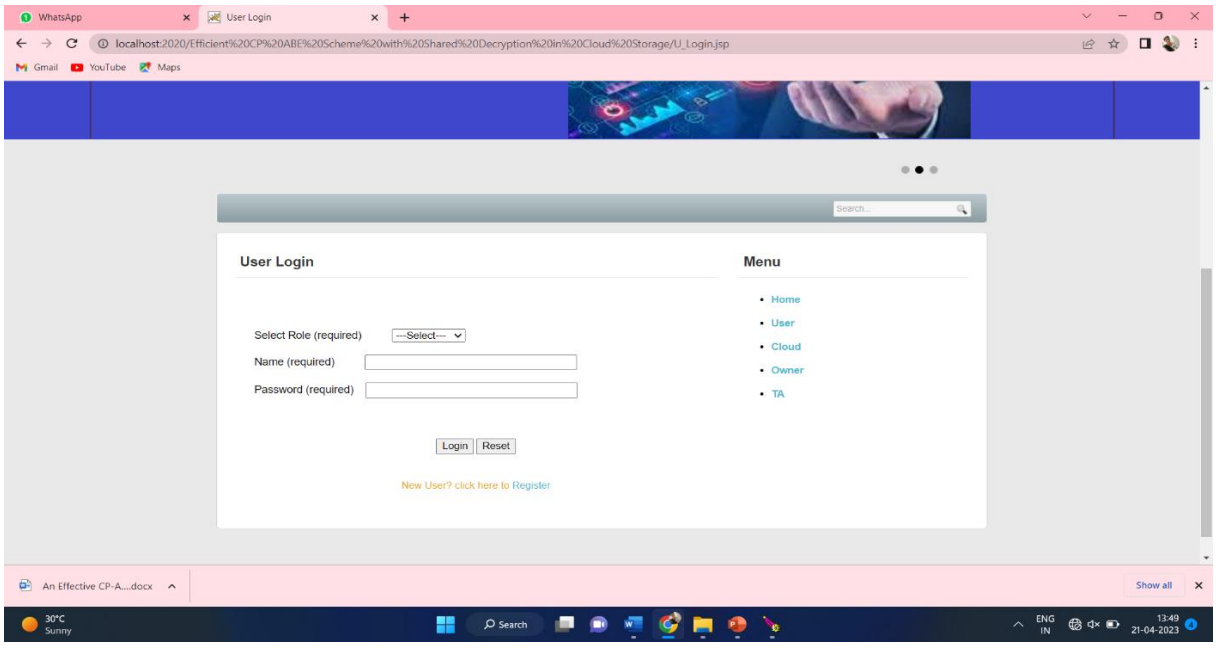


**Fig 4:in this screen data user can login by using name and password then user can access data from cloud but they need authentication then they can download information from cloud**

## 5.CONCLUSION

We offer two encryption schemes that use cypher text-policy attributes and share decryption. In our schemes, there are two different types of data users. An authorised user has the ability to recover the message on their own. These semi-authorized users can work together to decrypt the cypher text to take the place of the authorised user if for some reason the authorised user is unable to do so in time. In order to increase the efficiency of the proposed schemes, an integrated access tree is used. Under the DBDH assumption, the security of our schemes has been demonstrated. The experimental finding demonstrates that, in terms of storage cost and computational overhead, the CP-ABE-SD scheme outperforms the schemes [11,33,36].

## REFERENCES

[1] S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya, "Cloud-based augmentation for mobile devices: motivation, taxonomies, and open challenges," IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 337–368, 2014.

[2] J. Aikat et al., "Rethinking security in the era of cloud computing," IEEE Security Privacy, vol. 15, no. 3, pp. 60-69, Jun. 2017.

[3] J. Li, H. Yan, and Y. Zhang, "Efficient identity-based provable multi-copy data possession in multi-cloud storage," IEEE Transactions on Cloud Computing, DOI: 10.1109/TCC.2019.2929045.

[4] J. Li, H. Yan, and Y. Zhang, "Certificateless public integrity checking of group shared data on cloud storage," IEEE Transactions on Services Computing, to be published. DOI 10.1109/TSC.2018.2789893.

[5] H. Yan, J. Li, and J. Han, "A novel efficient remote data possession checking protocol in cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, no. 1, pp. 78-88, Jan. 2017.

[6] H. Yan, J. Li, and Y Zhang, "Remote data checking with designated verifier in cloud storage," IEEE Systems Journal, vol. 14, no. 2, pp. 1788-1797, 2020.

[7] J. Li, H. Yan, and Y. Zhang, "Identity-based privacy preserving remote data integrity checking for cloud storage," IEEE Systems Journal. DOI:10.1109/JSYST.2020.2978146

Industrial Engineering Journal
ISSN: 0970-2555

Volume : 52, Issue 7, July : 2023

## AUTHOR PROFILES

Mr. K.Ravichand working as Associate Professor in Department of CSE, Visvodaya Engineering College, Kavali. He completed his MCA in Computer Science from T.J.P.S. College, Guntur and completed his M.Tech in Computer Science from Acharya Nagarjuna University. He had 20 years of Teaching experience in various engineering colleges. Published 5 national and 5 international publications in various journals.

Miss. Momidi Suvarna M.Tech student in the department of CSE at Visvodaya Engineering College, Kavali, SPSR Nellore (DT). She has completed B.Tech in CSE from Visvodaya Engineering College, Kavali.