IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710


# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 7, July 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307131 |

# Secure Video File Sharing in Attribute-Hiding Fuzzy Encryption based Cloud Computing

**Dr .R .Uma, M.E., Ph.D[1],R.Asha[2]**

Assistant Professor, Department of CSE, Jayamatha Engineering College, Muppanthal, Kanyakumari, India [1]

PG Student, Department of CSE, Jayamatha Engineering College, Muppanthal, Kanyakumari, India[2]

**ABSTRACT:** Clients can store and share data on the cloud. It is essential to create an efficient access control strategy to assure that only authorized users have access to the information, based on the needs of the user. In this manuscript, Secure Video File Sharing in Attribute-Hiding Fuzzy Encryption based Cloud Computing (SVFS-AHFE-CC) is proposed. Initially, the input video file is gathered from YouTube-8M Segments dataset. A user accesses the system's user interface in order to share a video file. The user chooses the video file to distribute. After then, Attribute-Hiding Fuzzy Encryption (AHFE) is used to encrypt the chosen video file. Only users who possess the necessary qualities can decrypt and see the video. The encrypted video file is then safely saved in the cloud after encryption. Decryption requests are accepted from users who meet the requirements to see the video. Users get an email with a secret key after their authentication and attribute verification are successful. Through the system, users authenticate themselves, demonstrating their identity and confirming their access credentials. Encryption keys are only distributed to authorized users using secret key management. The user can safely download the video content by decrypting it using the secret key that they got through email. The proposed SVFS-AHFE-CC approach is implemented in python platform. The performance of the proposed SVFS-AHFE-CC approach attains higher encryption time, and lower download time analysed with existing techniques likes MKSABE-VAAR, SMCCCP-ABE and MQKDCP-ABE-CSC methods respectively.

**KEYWORDS:** Attribute-Hiding Fuzzy Encryption, liveness Detection Dataset, Cloud Computing, email, Decryption.

## I. INTRODUCTION

Cloud computing has been one of the most important information technology techniques. The government and industry have given significant attention to this technology. To improve cloud performance, four primary components are used: Service-Oriented Architecture (SOA), virtualization, a diversity of services, and deployment architecture [1]. When utilize it, pay for the services it delivers. Various features are offered, such as pricing, measurement, and on-demand access to optimize resource utilization. Although the cloud provides numerous benefits, it also poses security and data storage issues. Cloud storage is typically used for sensitive and secret data, including medical and military information. Encrypting user data before outsourcing to the cloud ensures superior data protection [2]. These motivated to do this work.

In this work, the SVFS-AHFE-CC approach lies in its use of Attribute-Hiding Fuzzy Encryption (AHFE) for secure video file sharing, combining user-friendly interface, robust authentication, and efficient secret key management to ensure only authorized users can access encrypted content, outperforming existing methods in encryption and download times.

Major contribution of this research work summarized below,

- The proposed SVFS-AHFE-CC system contributes to the field based Secure Video File Sharing in Attribute-Hiding Fuzzy Encryption based Cloud Computing,
- The YouTube-8M Segments dataset is utilized as the source for the input video files by the system. Users may choose and share video files with ease to the user-friendly interface of the suggested system.
- By using Attribute-Hiding Fuzzy Encryption (AHFE) technique makes sure that the video files can only be decrypted and viewed by those who have the required characteristics.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307131 |

- The video data are safely kept on the cloud after encryption. Users get an email with a secret key in it when their authentication and attribute verification are successful. A robust authentication system guarantees the ability to request decryption keys only to authorized users.

The remainder of paper is arranged in given below. Literature review presented in part 2, materials and procedures are employed article discussed in part 3, outcome and discussion designated in part 4, conclusion is provided in part 5.

## II. LITERATURE SURVEY

Numerous research works suggested in literature depending upon Encryption based cloud computing, few current works were reviewed here, In 2023, Shen, H, et.al [3] have presented the Multi-Keywords Searchable Attribute-Based Encryption with Verification and Attribute Revocation over Cloud Data. Here, the suggested paper presents a new system called MKSABE-VaAR. To achieve multi-keyword search, the presented study first bundle several keywords into a polynomial, addressing the issues of slowness, extreme computation during the search procedure, and only providing singlekeyword search in the majority of attribute-based searchable encryption techniques. It provides high encryption time and low download time.

In 2023, Swetha, M, et.al [4] have presented the security on mobile cloud computing with cipher text policy and attribute based encryption system. The suggested paper showcases several studies that use CP-ABE techniques to securely save, read, and share data via untrusted cloud settings. Every studied work was scrutinized, assessed, and compared with each other to ascertain the best. It provides high download time and low encryption time.

In 2023, Singamaneni, K.K, et.al, [5] have sugggested text-Policy Attribute-Based Encryption Model to Enhance Cloud Security for Users of the Multi-Qubit Quantum Key Distribution Cipher. The presented study suggests a multi-qubit Quantum Key Distribution (QKD) cipher text-policy attribute-based encryption (CP-ABE) to enhance cloud security. The suggested multi-qubit QKD paradigm for cloud data security uses a quantum key distribution protocol to create a secure key for encryption and decryption. It provides high encryption time and low download time.

In 2023, Yan, L, et.al, [6] have suggested an attribute-based searchable encryption system and blockchain-based access control system for cloud environments. The suggested paper supports policy concealment and attributes revocation and implements proxy encryption and decryption to provide fine-grained access control with minimal computing overhead. Data integrity and confidentiality are guaranteed by storing the encrypted file in IPFS and metadata cipher text on the blockchain. It provides high download time and low encryption time.

## III. PROPOSED METHODOLOGY

In this section SVFS-AHFE-CC is covered. This unit offers an in-depth explanation of the research approach that was employed in Attribute-Hiding Fuzzy Encryption based Cloud Computing from YouTube-8M Segments dataset. The Proposed diagram of SVFS-AHFE-CC is shown in Figure 1. Therefore, the comprehensive description about SVFS-AHFE-CC is given below,

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307131 |

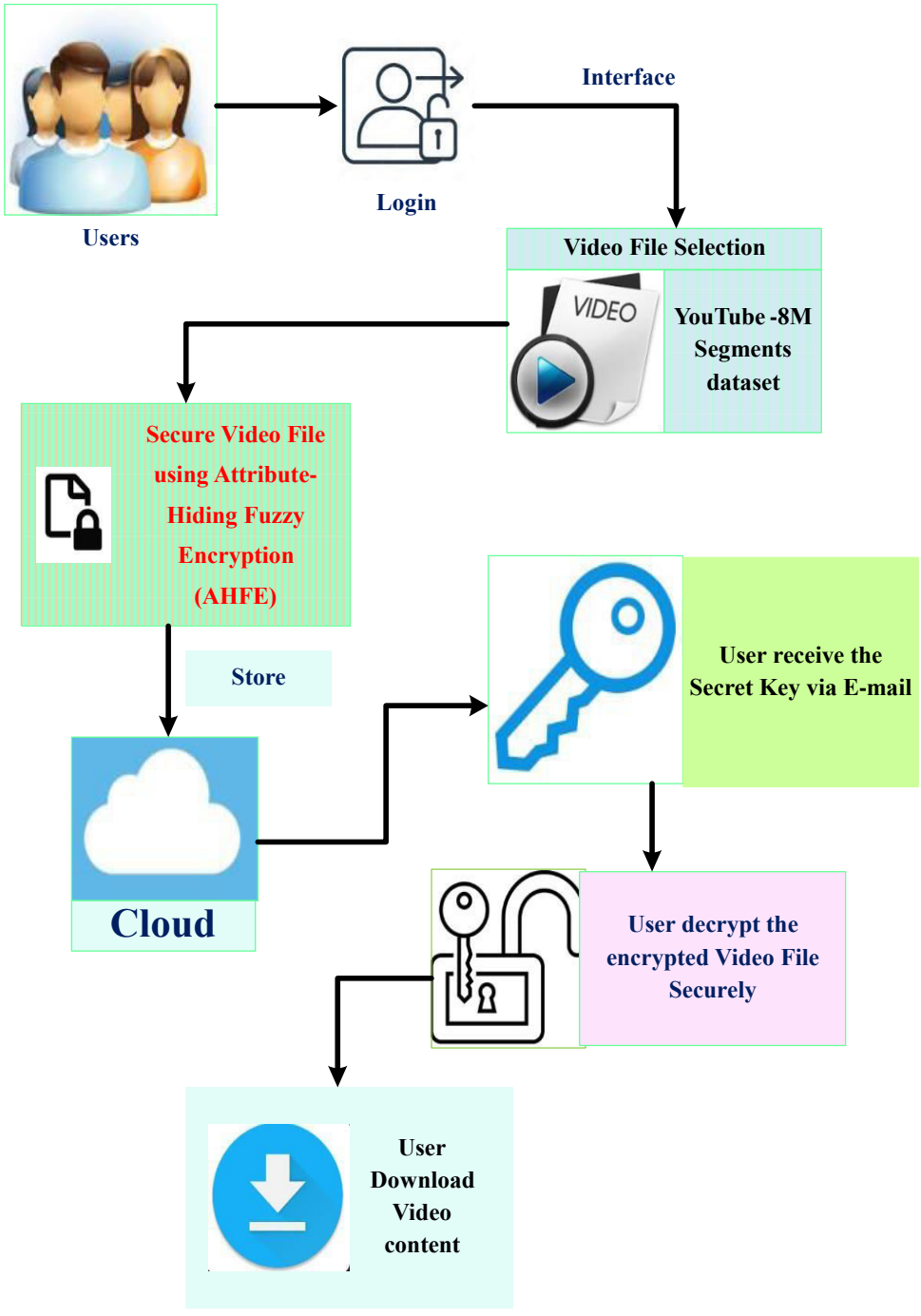


**Figure 1: Block diagram of the proposed SVFS-AHFE-CC system for Attribute-Hiding Fuzzy Encryption based Cloud Computing**

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307131 |

### 3.1 Data Acquisition

Initially, the input video is collected from the YouTube-8M Segments dataset [7].This dataset is an expansion of YouTube-8M dataset that includes human-verified segment annotations. In addition to annotating films, it likes to temporally localize the entities in them, i.e. determine when they appear.

### 3.2 Login Phase

Usually, users will be prompted to register their username or username, password, age, and gender before they can use the system. This will frequently have a username and password. To gain access to and control over any PCs or administrations, one needs a login. To access information, the customer enters his client ID and secret key. In the verification stage, the user's login credentials are checked. The user is authorized to view the stored video file because their information has been accurately confirmed. If not, the user's request is turned down. Then the user selects the video file from the system. After it encrypt the video file.

### 3.3 Secure Video File using Attribute-Hiding Fuzzy Encryption (AHFE)

The four operations of the proposed Attribute-Hiding Fuzzy Encryption (AHFE) [8] are delegation, encryption, decryption, and key generation. Below is a description of these operations' foundation.

- **Setup**($1^{\sqcup}$,r,u): A master key pair (tby,tcy)is produced using key generation center's setup algorithm that receives as inputs a safety parameter ($\llcorner$ ),length of strings (r ), and size of universe (u ).
- **Key Generation**(tby,tcy,T$\llcorner$,h): The master public key tby , the master secret key tcy , string T$\llcorner$, and threshold h represents inputs used by the key generation center. The keygen algorithm outputs the private key $cy_{T\sqcup}$ .
- **Encryption**(tby,v,T): After a user enters a dataset, a stringT , and the master public keytby , the encryption method outputs a encrypted video file, $vi_f$. Here, it encrypt the selected video.
- **Decryption**(tby,$cy_{T\sqcup}$,$vi_f$r,h): The decryption algorithm outputs the video v if the overlap distance among T , T$\llcorner$ is greater than threshold h . The evaluator takes the master public key tby , video vi , private key $cy_{T\sqcup}$ , length of strings r , and threshold h as input. Here, user decrypts the encrypted video file securely.

### 3.4 Secure Video playback

Upon receiving a secret key via email and successful authentication, users can securely preview or download decrypted video content.

## IV. RESULT WITH DISCUSSION

In this part, the experimental outcomes of the indicated procedures are discussed. The proposed SVFS-AHFE-CC method is applied by using python. The obtained outcome of the proposed SVFS-AHFE-CC approach is analysed with existing methods such as MKSABEVAAR [3], SMCC-CP-ABE [4] and MQKDCP-ABE-CSC [5] respectively.

### 4.1 Performance measures

Performance metric like Encryption time and Decryption time are examined for performance measures. To scale the performance measures, in performance matrix is deemed. The following matrixes are required to scale the performance measures.

#### 4.1.1. Encryption Time

The disparity between the beginning and ending times of the encryption process is known as the encryption time. It is measured through in equation (20),

$$\text{Encryptiontime} = E_{end} - E_{start} \quad (20)$$

#### 4.1.2 Decryption Time

The amount of time needed to decode encrypted data back into its original format is referred to as the decryption time. It is scaled by the equation (21),

$$\text{Decryptiontime} = \text{Data size}\llcorner \text{ Decryption Speed} \quad (21)$$

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307131 |

**4.2. Performance Analysis**

Figure 2-3 determines the simulation result of SVFS-AHFE-CC method. Then, the proposed SVFS-AHFE-CC technique is compared with existing as MKSABE-VAAR, SMCC-CP-ABE and MQKDCP-ABE-CSC methods respectively.

Figure 2 shows Encryption time analysis. The size of the encrypted video file is shown on the graph's X-axis. The encryption time needed to encrypt a video file of a given size is displayed on the Y-axis. Here, proposed SVFS-AHFE-CC method attains 21.51%, 12.38%, and 21.51% lower Encryption time at node 100; 11.11%, 16.18%, and 20.21% lower Encryption time at node 300; 23.07%, 26.56% and 29.05% lower Encryption time at node 500 evaluated with existing MKSABE-VAAR, SMCC-CP-ABE and MQKDCP-ABE-CSC methods.

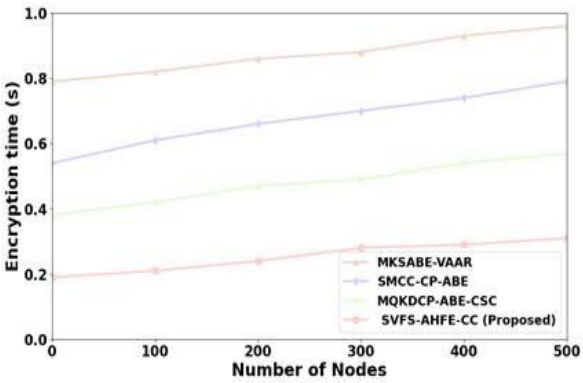


Figure 2

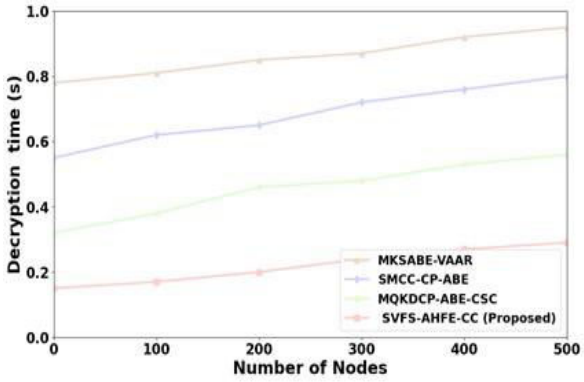


Figure 3

**Figure 2, 3: Performance analysis of Encryption and Decryption Time**

Figure 3 shows Decryption time analysis. The size of the video file that is being decrypted is shown on the graph's X-axis. The time it takes to decode a video file of a specific size is displayed on this Y-axis. Here, proposed SVFS-AHFE-CC method attains 28%, 22.50%, and 21.51% lower Decryption time at node 100; 13.09%, 17.09 %, and 25.31% lower decryption time at node 300; 26.88%, 27.04% and 28.05% lower decryption time at node 500 compared with existing MKSABE-VAAR, SMCC-CP-ABE and MQKDCP-ABE-CSC approaches.

Figure 4(a) shows the login page framework, it prioritizes security and user-friendliness for management access and new user registration. Figure 4(b) shows the Registration process, with a registration-based access control system for file sharing; improved security and expedited access are ensured by requiring new managers and users to fill out a registration form before accessing shared files.

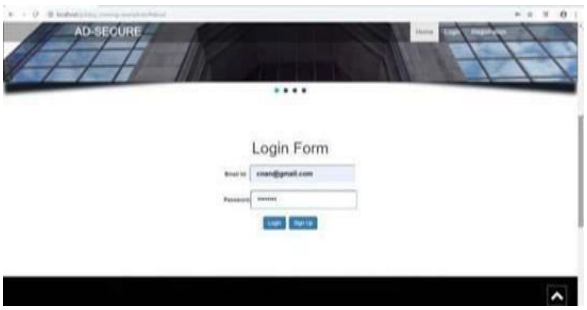


Figure: 4(a)


Figure: 4(b)

Figure 4(a), 4(b): Login Page Framework and Registration Process

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307131 |

Figure 4(c) shows the view file page. The depthfirst search technique allows users to look for a certain number of files inside the files they have been sent. Figure 4(d) shows the secure file transmission. When providing files to staff, managers use encryption technologies to ensure secure file transmission.

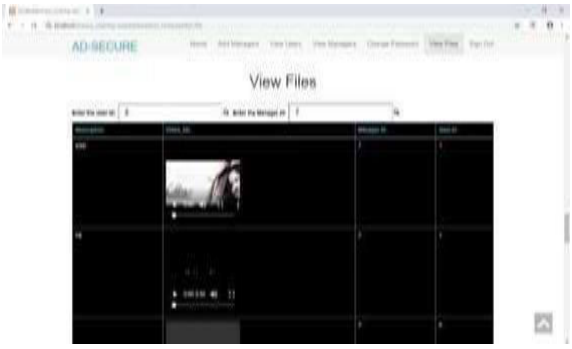


Figure: 4(c)

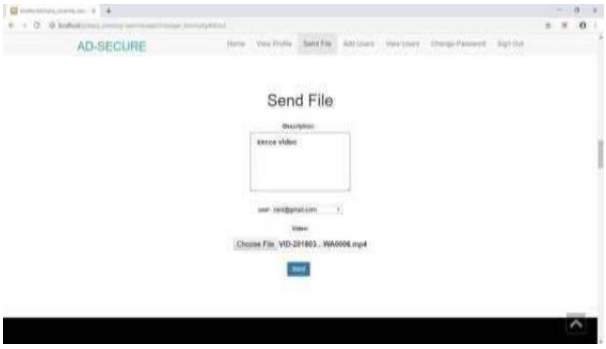


Figure: 4(d)

**Figure 4(c), 4(d): the view file page and Secure File Transmission**

Figure 4(e) shows the file access process. Here, users are emailed a secret key as part of the file access procedure; this is a requirement in order to view encrypted video files. Figure 4(f) shows the file download process. Users must enter the secret key supplied to their email address during the file download procedure in order to decrypt the file. Users can safely access the video file after the encrypted file smoothly converts to a decrypted format upon successful key entry.


Figure: 4(e)

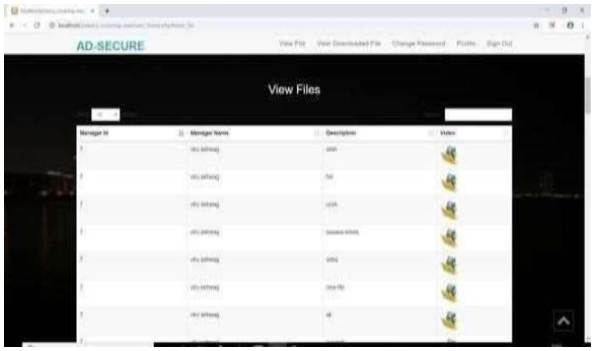


Figure: 4(f)

**Figure 4(e): File access process, Figure 4(f): File download process.**

### 4.3 Discussion

In this section, SVFS-AHFE-CC method is developed in this paper. It considerably minimize the decryption and encryption time in the attribute process by re-formulating the access policy, computing a portion of the index, and uploading it using the linear reconstruction function of video file sharing system. Additionally, depending on computational and storage overhead, techniques that already exist are compared. Experimental findings and theoretical research show that the method provides security, effectiveness, and adaptability.

## V. CONCLUSION

In this manuscript, Secure Video File Sharing in Attribute-Hiding Fuzzy Encryption based Cloud Computing (SVFS-AHFE-CC) is successfully executed. The proposed method is executed on python. The execution of the suggested SVFS-AHFE-CC method approach contains 21.51%, 12.38%, and 21.51% lower encryption time, 28%, 22.50%, and 21.51% lower decryption time, when analysed to the existing MKSABE-VAAR, SMCC-CP-ABE and MQKDCP-ABE-

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307131 |

CSC methods. Future study concentrates on strengthening the system's security safeguards, expanding administrator-user interaction for a more efficient communication and collaboration experience, enhancing backup capability, and allowing users to handle deleted data.

## REFERENCES

1. Gharib, M. and Fazli, M., 2023. Secure cloud storage with anonymous deduplication using ID-based key management. The Journal of Supercomputing, 79(2), pp.2356-2382.
2. Paulraj, D., Neelakandan, S., Prakash, M. and Baburaj, E., 2023. Admission control policy and key agreement based on anonymous identity in cloud computing. Journal of Cloud Computing, 12(1), p.71.
3. Shen, H., Zhou, J., Wu, G. and Zhang, M., 2023. Multi-Keywords Searchable AttributeBased Encryption With Verification and Attribute Revocation Over Cloud Data. IEEE Access.
4. Swetha, M. and Latha, M., 2023. Security on mobile cloud computing using cipher text policy and attribute based encryption scheme. Materials Today: Proceedings, 80, pp.30593063.
5. Singamaneni, K.K., Muhammad, G. and Ali, Z., 2023. A Novel Multi-Qubit Quantum Key Distribution Ciphertext-Policy Attribute-Based Encryption Model to Improve Cloud Security for Consumers. IEEE Transactions on Consumer Electronics.
6. [6]Yan, L., Ge, L., Wang, Z., Zhang, G., Xu, J. and Hu, Z., 2023. Access control scheme based on blockchain and attribute-based searchable encryption in cloud environment. Journal of Cloud Computing, 12(1), p.61.
7. https://research.google.com/youtube8m/
8. Chen, Z., Huang, L., Yang, G., Susilo, W., Fu, X. and Jia, X., 2024. Attribute-hiding fuzzy encryption for privacy-preserving data evaluation. IEEE Transactions on Services Computing.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details