IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, May 2026
Impact Factor: 8.2

Data Privacy in Cloud Computing Secure Data Storage and Computation

Kiran Khandu Hipparkar[1] and Sushant Arun Hipparkar[2]
Department of Computer Science[1-2]
A.M College, Hadapsar, Pune, Maharashtra, India

Abstract: *The world has seen a quick transition from hard devices to local storage to massive virtual data centers, all because of cloud storage technology. Cloud computing has transforming the way we do business making it more efficient that leads to new types of cyber crime. Securing the data in cloud is a challenging task. While cloud platforms offer scalability, flexibility, and cost efficiency, they also introduce significance concerns in cloud security and data storage. This research project focuses on addressing the challenges of ensuring secure data storage and computation in cloud environments. The propose of this abstract is to offer a through of issues, solutions and future development related to data privacy and security in cloud computing. Keeping data private and secure while being and stored in outside data centers is the main difficulty in cloud computing systems. The abstract describes the dangers of insider threats, data breaches, and illegal access to sensitive information. Today a lot of companies sensitive data are stored in a cloud computing so securing those data is the main goal of cloud computing providers. This research propose five optimized frameworks to address these challenges.*
In addition, these research highlights the importance of secure communication between cloud entities and the role of intelligent security mechanism in preventing data breaches. Techniques such as duplicate file detection, user-generated encryption keys, and optimized node selection for distributed cloud storage are evaluated to improve performance, reduce storage overhead, and increase system reliability. The project ultimately contributes toward building a more secure, efficient, and trustworthy cloud computing environment for future applications and digital services.

Keywords: Cloud Data Security, Duplicate File Detector, FADE, Partial Description, Optimized Algorithm, Shared Secret Session (3S) Key

I. INTRODUCTION

Cloud computing works by connecting many computers and storage systems together to create large data centers that provides storage and computing power over the internet. These data center consists of multiple servers and storage devices placed in dedicated locations to manage and process huge amount of data efficiently. Users can store, access, and share their data online without depending completely on their personal devices. Devices such as desktops, smartphones, and tablets can all be used to access cloud services. Cloud storage allows users to access their data anytime and from anywhere through an internet connection.

Cloud Computing

The term "cloud" originates from the telecommunication world of the 1990s, when providers began using virtual private network (VPN) services for data communication. VPNs maintained the same bandwidth as fixed networks with considerably less cost these networks supported dynamic routing, which allowed for a balanced utilization across the network and an increase in bandwidth efficiency, and led to the coining of the tem "Telecom Cloud". Cloud Computing (CC) is a technology that provides services like storage, servers, and software through the internet instead of local storage. It helps organization reduce the cost of managing hardware and software while offering flexibility and scalable resources. The right to access the computing resources based on on-demand that relives the customer in task like

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, May 2026
Impact Factor: 8.2

storing, security, resource allocation, and infrastructure. Due to this demand, by analyzing the capabilities of the cloud, the providers needs to concentrate much on the parameters like security, performance, and quality. Cloud computing uses technologies like virtualization and Service-Oriented Architecture (SOA) to provide services such as storage, software, and computing power over the internet. CC architecture is compromised of two parts: Front end and Back end which are connected through Internet as shown in figure 1.1

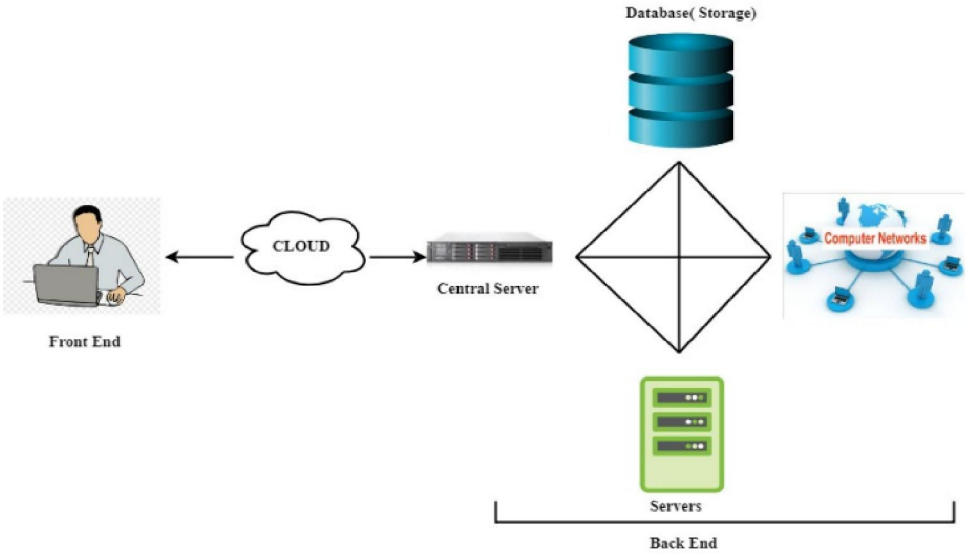


Figure 1.1: Cloud Architecture

Front end represents the computer that client sees. This acquires the access to the computer system. Gaining access can be simple as using the Internet browser or more complex by using Internet software which provides the access to the cloud. Back end compromises of computer networks, servers, database which stores all the data and information. Central servers that manages the system, monitors the traffic that ensures everything runs smoothly. Naturally cloud computing companies built in with donjon that they save multiple copies of your data/work in case of any problems.

Cloud Data Storage Security

Cloud storage services allow users to store and access data through the internet. These services are managed by Storage Service Providers (SSPs), which use large storage systems and servers to store user data securely. Cloud storage provides flexible storage capacity that cab be increased or decreased based on user needs. It is commonly used for data backup, recovery, file sharing, and collaboration among individuals and organizations. Data encryption and tokenization are important technique used to improve data security in cloud computing. Encryption converts readable data into an unreadable format called cipher text, which can only be accessed using correct encryption key. Tokenization replaces sensitive data with randomly generate tokens, while the original data is stored securely in a separate database. These methods help protect sensitive information from unauthorized access and improve privacy and security in cloud environments.

Cloud Data Privacy

In cloud computing, users store their important data on servers managed by third-party companies. Although cloud services allow users to access files and applications from anywhere, there is always a concern about privacy once the

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, May 2026 Impact Factor: 8.2

data is stored outside personal devices. Protecting personal information is a major issue in cloud computing because sensitive data, also known as Personally Identifiable Information (PII), must be securely collected, stored, and managed to prevent unauthorized access and misuse.

II. LITERATURE REVIEW

Cloud computing provides a modern and cost-effective way for organizations to use IT services without investing heavily in hardware and software infrastructure. It offers features such as on-demand resources, flexible storage, and pay-as-you-use services, which help reduce maintenance costs and improve accessibility. However, despite these advantages, security and privacy remain major concerns in cloud computing. Since sensitive information such as financial records, employee details, medical data, and business information is stored on remote cloud servers, there is always a risk of unauthorized access, data breaches, and privacy loss. Therefore, strong encryption and security mechanisms are necessary to protect data stored in the cloud.

Cloud Storage Providers (CSPs) offer storage services to users and organizations through the internet under specific service agreements. Cloud storage works on the concept of Storage-as-a-Service, where users can store and access data without managing physical storage systems. Cloud computing also includes different service models such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). Although these models provide flexibility and cost benefits, they also introduce security challenges related to data protection, privacy, and system vulnerabilities.

Certificateless Compressed Data sharing

Predicate Encryption (PE) is an advanced form of Identity-Based Encryption (IBE) where secret keys are associated with specific conditions or predicates, and ciphertexts are linked with attributes. It helps provide fine-grained access control to encrypted data. Fine-Grained Access Control (FGAC) is used to create secure encryption policies and manage access permissions. Researchers have also proposed certificateless public key cryptography techniques to simplify key management and improve security. In addition, Revocable Storage Identity-Based Encryption (RS-IBE) supports user revocation and ciphertext updates, helping maintain forward and backward security in cloud environments.

The FADE model was introduced using a semi-trusted third party for key generation, which icreased system complexity and made it more appropriate for corporate environments. To overcome these limitations, SFADE was developed as a simpler and more user-friendly alternative. This approach removes the need for a key manager while still providing assured data deletion, helping cloud storage users preserve data confidentiality. However, both FADE and SFADE do not support file-sharing functionality.

To address this drawback, SFADE+ was proposed, allowing files to be shared among multiple users . The enhanced model introduces several additional features, including:

A version control mechanism.

File-sharing support for multiple users.

A mobile-compatible version of the system.

SFADE+ is a system that retain data integrity and access. It maintains data security through encryption techniques and helps to access these encrypted data in a secure way. SFADE+ provides data sharing as well as accessibility and deletion of data. However, SFADE+ leads to revocation problem and the algorithm used for key generation is not much secure and key length is also very large.

III. METHODOLOGY

Cloud Data Security with Scheduled Key Management:

Introduction*:*

Encryption is then main approach to protect the privacy and confidentiality of the data stored. The main concern of the encryption is the key management. The keys that are used must also be stored securely. The entity that is responsible

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, May 2026
Impact Factor: 8.2

for generating the key may have the chances of compromising with the intruders that leads to the data leakage. The policy file controls access to encryption keys and defines the permissions associated with the stored data. During the encryption process, a random symmetric key is generated at the client side and secured using the public keys of the key managers. No local copy of the key is maintained at the client side, which improves security. The encrypted data along with the encrypted keys are then uploaded to the cloud. When the user wants to retrieve the file, the policy file must be presented to the cloud within the permitted time limit. The encrypted keys are then decrypted using the private keys of the key managers, allowing the client to recover the symmetric key and finally decrypt the data to obtain the original file.

Motivation

When the key managers get the request for the keys, they may be busy in accomplishing other tasks. This makes the users wait for the key managers to complete its previous work and take up the users work. While uploading the file, there is valid verifier for the duplicate file. This motivated to introduce scheduler that schedules the tasks based on the workload of the key managers.

Problem statement

Given the data storage model that consist of client and the cloud, where the client has to wait for all the key managers to send the keys upon request by completing the tasks previously allotted.

Contributions

The proposed system improves cloud security using symmetric and asymmetric encryption to protect user data. Access policies control permissions based on time and read/write access. A scheduler reduces key waiting time by managing key managers efficiently, while duplicate file detection prevents repeated uploads and saves cloud storage space.

Proposed System

The proposed system provides secure cloud storage for organizations that move their data from on-premises systems to the cloud for cost efficiency. Since cloud data may face risks such as attacks or data leakage, the system is designed to improve the security and protection of records stored in third-party cloud environments

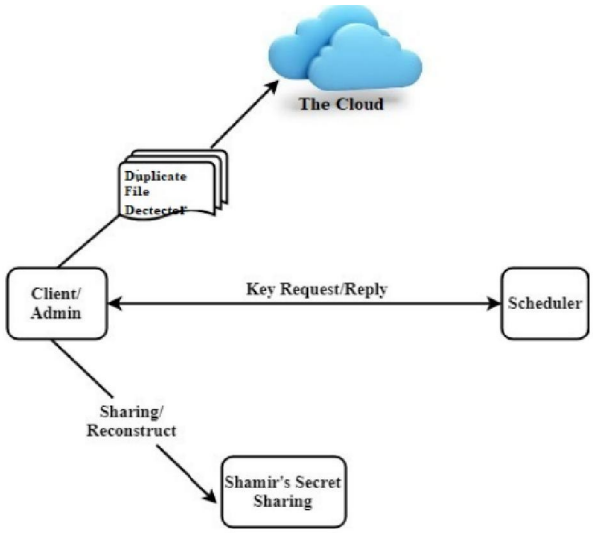


Figure 1.5 DSCESM Architecture

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, May 2026
Impact Factor: 8.2

The proposed system consists of four main modules: the client, cloud, scheduler, and duplicate finder. The client encrypts the file using a secret random key before uploading it to the cloud. The scheduler communicates with key managers to provide public keys, which are used along with Shamir's Secret Sharing to divide and secure the secret key into multiple shares. These encrypted shares are stored with the encrypted file in the cloud. Before uploading, the duplicate finder checks whether the file already exists by comparing hash values, preventing duplicate storage. During file retrieval, the client obtains the encrypted file and keys from the cloud, receives private keys from the scheduler, reconstructs the secret key using Shamir's Secret Sharing scheme, and finally decrypts the file to recover the original data.

Implementation

Before communication begins between the user, cloud, and key managers, a secure channel is established using the Station-to-Station Protocol to protect the exchange of keys from intruders. The system also uses access policies to control user permissions, while Shamir's Secret Sharing ensures key secrecy by requiring only a minimum number of shares to reconstruct the key. In addition, a scheduler manages key manager tasks efficiently, and a duplicate file detector prevents repeated file uploads to the cloud.

Policy

Policies define the access permissions for keys and files based on factors such as time limits and read/write access. The policy file contains file permissions and file path details instead of the original file, which helps maintain confidentiality. During file access, the client submits the policy file to the cloud and key manager to retrieve encrypted data and keys according to the allowed permissions. The key manager validates the policy based on its expiry time and can renew it only when requested by the client. If the encrypted policy is sent for deletion, the key manager removes the related keys and authentication data, thereby ending further communication and file access securely.

Scheduler

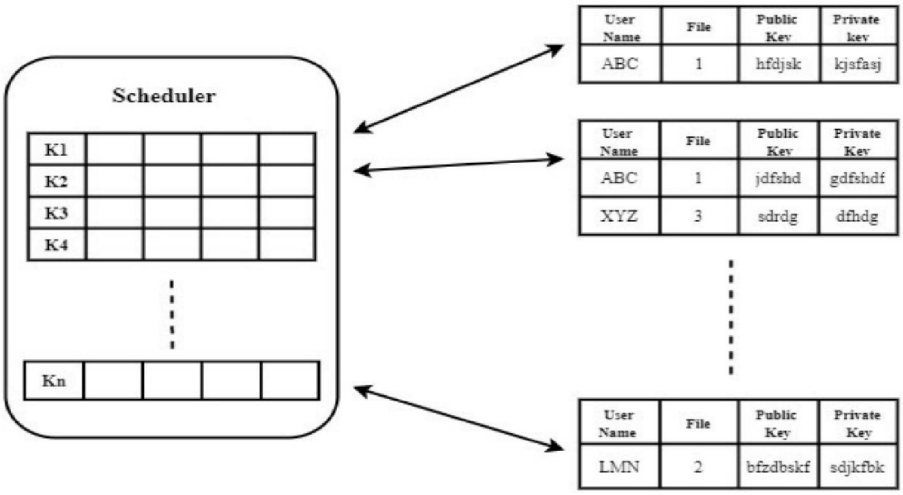


Figure 3.2 Interaction between Scheduler and the key managers

Scheduler allots the job to the key manager who has less task to complete. The scheduler must keep track the status of the key managers and update the database. The relationship between the scheduler and key managers is shown in Figure 3.2 and takes the following steps:

1. The client contacts the scheduler for the keys.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, May 2026
Impact Factor: 8.2

2. After getting the request, the scheduler checks with the key managers (K1, K2,... ,Kn) table to verify with which key manager is free or has less task to complete.
3. Later, the key manager generates the private key and public key using a random key generator.
4. In order to upload the file, public keys are sent to the client.
5. In order to download the file, private key are sent to the client on request.

For each of these steps, the scheduler maintains the database that keeps track of these transactions of the keys between the key managers and the client.

Shamir's Secret Sharing Scheme

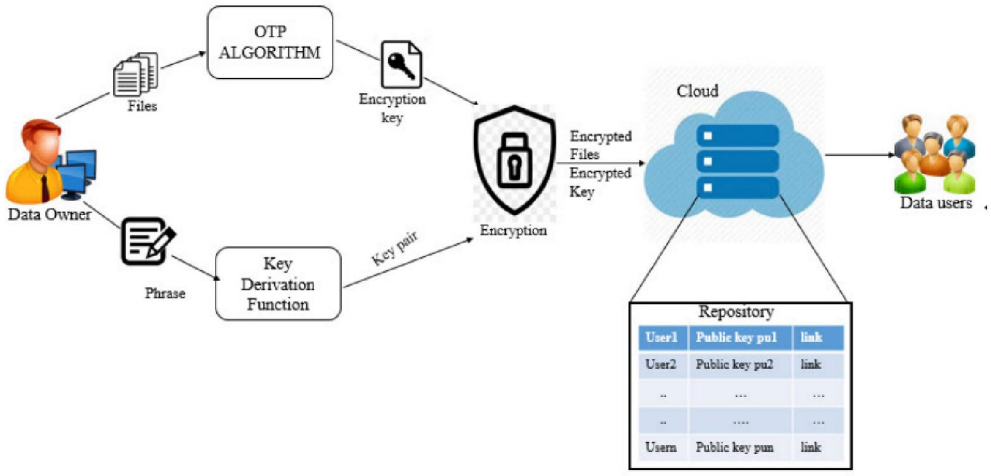
The proposed system uses Shamir's Secret Sharing to protect encryption keys, where only a minimum number of shares are needed to reconstruct the original key. This approach improves the security of data stored with third-party cloud providers by supporting secure key management, access control, and assured file deletion

Summary

In this work, a Scheduler is introduced to manage the tasks of key managers and assigns the tasks based on workload that reduces the waiting time of the client. Deletion of files are assured based on the policy of the client related to the file. The space is also saved by not uploading the repeated file to the cloud with the help of Duplicate File Detector.

S³DCE: Secure Storing and Sharing of Data in Cloud Using User Phrase

Cloud storage has made data access convenient, but since the data sits on servers owned by third parties, security remains a genuine concern. Earlier approaches like DaSCE and DSCESM relied on external key managers to generate and handle encryption keys — a setup that introduced waiting time and a single point of failure through the scheduler. S³DCE was built to fix exactly that.



2.1: S3DCE Architecture

The Core Ideas

Instead of depending on any external key manager, the data owner generates keys independently using two custom algorithms. A secret symmetric key is created via the OTK (One-Time Key) algorithm, which randomly selects and shuffles characters from a pool of letters, digits, and special characters. To protect this secret key, the owner's personally chosen phrase is passed through a Key Derivation Function (KDF), which converts it into a consistent encoded string and then generates a public-private key pair using ECC. This means keys are never stored anywhere — they're recreated on demand from the phrase every time.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, May 2026
Impact Factor: 8.2

Three Ways to Use It

The system handles three interaction types. In single interaction, the owner uploads and accesses their own files encrypting with their phrase-derived keys and decrypting the same way later. In one-to-one sharing, the owner fetches the intended recipient's public key from a cloud repository and encrypts the secret key with it, so only that user can decrypt. In one-to-many sharing, a group admin creates a shared phrase, and the resulting group key is used to encrypt files shared across the entire group.

Removing the scheduler and key managers had a dramatic effect on performance. Key generation in DaSCE and DSCESM took between 27 to 83 milliseconds depending on how many key managers were involved. S³DCE brings that down to just 9–11 milliseconds. Upload time improved by 88% over DaSCE and 61% over DSCESM, with similar gains on the download side.

Performance Analysis:

The evaluation focuses on the one-to-one interaction scenario, where a single owner shares data with a single user. All three entities owner, user, and cloud are assumed to have already authenticated securely before any file transfer begins.

2.3.1 Key Generation

The biggest bottleneck in older systems was waiting on external key managers. DaSCE required responses from all key managers, while DSCESM improved this using a scheduler to pick the least busy one. Even so, both systems averaged between 27 and 83 milliseconds just for key generation. S³DCE eliminates this dependency entirely the owner generates keys locally using their phrase bringing that figure down to just 9–11 milliseconds.

2.3.2 Upload Performance

Across all tested file sizes (10KB to 1MB), S³DCE consistently outperformed both predecessors. For a 1MB file, DaSCE took 498ms and DSCESM took 155ms, while S³DCE completed the same upload in just 89ms. Overall, S³DCE is 88% faster than DaSCE and 61% faster than DSCESM on uploads.

2.3.3 Download Performance

The download process involves fetching the encrypted file and key, regenerating the private key from the phrase, and decrypting both layers. Again, S³DCE led by a wide margin — finishing a 1MB download in 75ms compared to 439ms for DaSCE and 118ms for DSCESM. That translates to an 89% improvement over DaSCE and 61% over DSCESM.

The key generation time in the existing system considers either all the key manager or any number of key managers. The existing system DaSCE [134] uses all the key mangers and DSCESM [136] uses only those key managers who have less workload with the help of scheduler. Irrespective of file size, the time taken to generate keys is on an average between 27 to 83 msec. But the proposed system S3DCE doesnot depend on any key manager to generate key. Table 5.1 shows the time taken generate key with and without key managers by the three methods i.e., DaSCE, DACESM and S3DCE.

The performance is analysed in terms of time required to generate keys, total time to upload and download the encrypted file and encrypted secret key. The file size varies from 10kb to 1000kb that is used to analyse the performance

Figure 2.1 shows the time taken to upload the file. The graph is plotted by considering the values given in the Table 2.1 with the file size. As the file size increases, the time taken to upload the file also increases. By eliminating the key manager and shamir's concept, the proposed method S3DCE takes much less time compared to the existing system DaSCE and DSCESM. Thus the cost incurred in storing is reduced. The uploading time reduces by 88% in S3DCE compared to DaSCE and 61% in S3DCE compared to DSCESM. The total time taken to download the file from the cloud includes retrieving both encrypted file and the encrypted key from the link, generating the private key, decrypting the encrypted secret key, decrypting the file using the secret key.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, May 2026
Impact Factor: 8.2

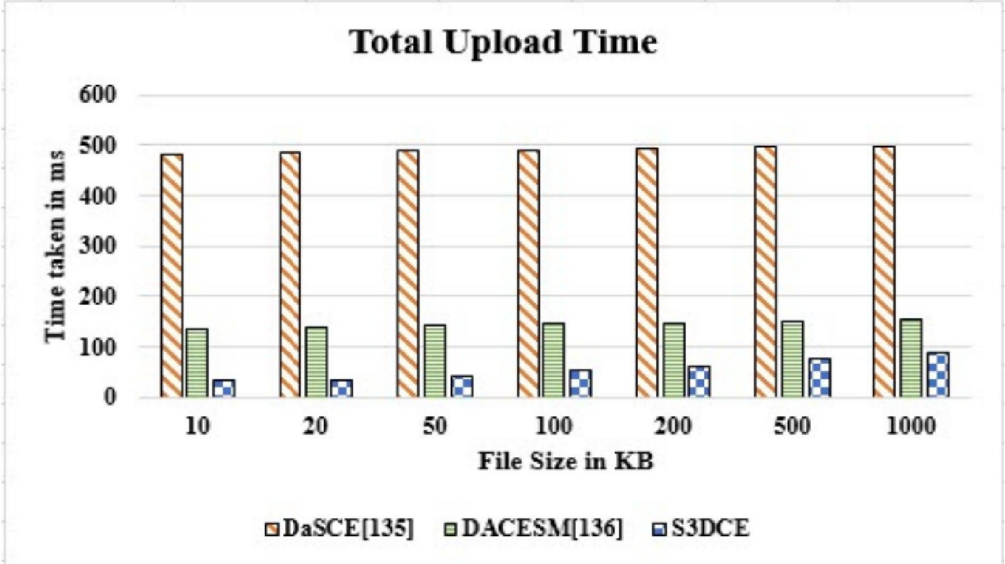


Figure 2.1: Comparison of Total Upload Time of DACSE, DACESM and S3DCE

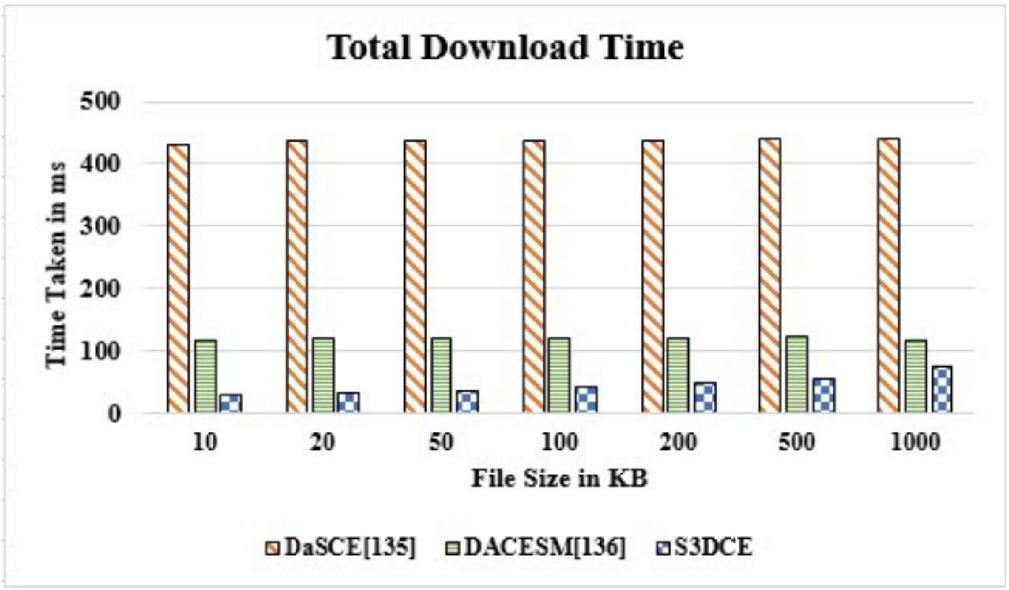


Figure 2.2: Comparison of Total Download Time of DACSE, DACESM and S3DCE

Summary

S3DCE is a cloud security model that reduces waiting time by removing key managers and using user phrases for dynamic key generation. The system uses an OTK algorithm and key derivation function for efficient and consistent key creation, while Elliptic Curve Cryptography provides stronger security than RSA.

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, May 2026
Impact Factor: 8.2

IV. FUTURE SCOPE

AI-Based Threat Detection

Artificial Intelligence and Machine Learning can be used to identify cyberattacks, abnormal activities, and security threats in real time with higher accuracy.

Blockchain for Secure Data Management

Blockchain can improve data integrity, transparency, and secure access control in cloud environments.

Quantum-Resistant Encryption

Future cloud systems may adopt advanced encryption techniques that can resist attacks from quantum computers and provide stronger data protection.

Zero Trust Security Models

Zero Trust Architecture will become more important, where every user and device must be continuously verified before accessing cloud resources.

Enhanced User Authentication

Biometric authentication, behavioral analysis, and multi-factor authentication will provide stronger protection against unauthorized access.

LIMITATIONS

Data Breaches and Cyberattacks

Cloud systems are vulnerable to hacking, malware, and unauthorized access, which may lead to data leakage.

Dependence on Third-Party Providers

Users must trust cloud service providers for storing and managing sensitive data, reducing direct control over security.

Complex Key Management

Managing encryption keys securely is difficult, especially in large-scale cloud environments.

Privacy Concerns

Sensitive information stored in the cloud may be exposed if proper encryption and access controls are not implemented.

Limited Control Over Data Location

Users may not know the exact physical location of their stored data, creating legal and compliance challenges.

V. CONCLUSION

Data privacy and security are major concerns in cloud computing due to the increasing use of cloud services for storing and sharing sensitive information. Various security models and encryption techniques have been developed to protect cloud data from unauthorized access, data leakage, and cyberattacks. Techniques such as Shamir's Secret Sharing, policy-based access control, duplicate file detection, and advanced encryption algorithms improve confidentiality, integrity, and secure data sharing in cloud environments. Models like CCDSPD, DSCESM, and S3DCE help reduce storage overhead, improve key management, and enhance overall cloud security. Although challenges such as cyber threats, privacy issues, and complex key management still exist, continuous advancements in security technologies can make cloud computing more reliable and secure for future applications.

REFERENCES

[1]. Loki M. Kaufman, "Data Security in the World of Cloud Computing", IEEE Security and Privacy Magazine, vol. 7, no. 4, pp. 61-64, 2009.

[2]. Luis M. Vaquero, Luis Rodero-Merino, Juan Caceres, and Maik Lindner, "A Break in the Clouds: Towards a Cloud Definition", ACM SIGCOMM on Computer Communication Review, vol. 39, no. 1, pp. 50-55, January 2009.

[3]. Jeevitha B K, Thriveni J, and Venugopal K R, "Data Storage Security and Privacy in Cloud Computing: A Comprehensive Survey", International Journal on Computer Applications, vol. 156, no. 12, pp. 16-27, December 2016.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, May 2026
Impact Factor: 8.2

[4]. Hassan Takabi, James B.D. Joshi, and GailJoon Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE transaction on Security and Privacy, vol. 8, issue. 6, November-December 2010.

[5]. Kolluru Venkata Nagendra and N. Haritha, "To Improve Data Storage Security Levels in the Cloud", International Journal on Recent and Innovation Trends in Computing and Communication, vol. 5, issue. 10, pp. 59-63, 2015

[6]. Sajjad Hashemi, "Data Storage Security Challenges in Cloud Computing" International Journal of Security, Privacy and Trust Management (IJSPTM), vol. 2, no. 4, pp. 1-10, August 2013.

[7]. Bob Duncan and Mark Whittington, "Enhancing Cloud Security and Privacy: The Cloud Audit Problem", Seventh International Conference on Cloud Computing, Grid and Virtualization, pp. 119-124, 2016.

[8]. Wayne A Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing", 44th Hawaii International Conference on System Sciences, pp. 1-10, Jan 2011

[9]. Mamta Sharma and Prachi Bhopi, "Study on Mobile Cloud Computing, its Architecture, Challenges and Various Trends", International Research Journal of Engineering, vol. 4, issue. 6, pp. 1168-1177, June 2017.

[10]. Rajkumar Buyya, Chee Shin Yeo, Srikumar Venuhopal, James Broberg, and Ivona Brandic, "Cloud Computing and Energing IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility", Future Generation Computer Systems, vol. 25, no.6, pp. 599-616, 2009.

[11]. P. Mell and T. Grance, "The NIST Definition of Cloud Computing", National Institute of Standards and Technology, vol. 53, no. 6, pp. 1-3, 2009.