Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 6 (2023)

A Multi-Cloud Approach for Secure Data Storage Using Double Signature Based Cryptocraphy Ds-Sha256 Methodology in Cloud Cimputing

K. Prathapkumar
Research Scholar,
Department of Computer Science, School of Computing Sciences, Vels Institute of Science Technology and Advanced Studies (VISTAS),
Chennai, India
prathapmcadept@gmail.com

Dr. A. Thirumurthi Raja
Research Supervisor & Assistant Professor,
Department of Computer Science, School of Computing Sciences, Vels Institute of Science Technology and Advanced Studies (VISTAS),
Chennai, India
dr.a.thirumurthiraja@gmail.com

Abstract

Mobile devices are vulnerable to storing sensitive data because those stored data can be easily attacked or lost. Cloud storage is also not advisable because while uploading the data in the cloud, it can be captured easily; hacking the ID cloud data can be easily stolen, etc. We proposed an enhanced data storage secure mechanism for mobile cloud computing using a multi-cloud approach to overcome these issues. The proposed system inherits the various benefits of multi-clouds like data security using data cryptography, secure distribution using data compression, data splitting into segments, segment compression, segment distribution, and segment encryptions as single segments in the mobile memory. A double encryption algorithm with the combination of SHA256 with RSA, known as DS-SHA256, is implemented to secure those stored data. It secures the data extraction in the distributed segments with minimum energy consumption. The proposed multicloud DS-SHA256 performance is evaluated with existing fuzzy formal concept analyses (fuzzy FCA) and CSBAuditor on the aspect of security, time taken for uploading the file, downloading the file, encrypting the file and decrypting the file. The proposed DS-SHA256 overall performance and security are far better than the existing systems.

Keywords: Mobile devices, Cloud computing, encryption, decryption, multi-cloud systems.

1. Introduction

The evolution of cloud computing has been remarkable, and its footprint spread globally in all fields. It seems to be a boon for the technology era and various salient features. However, its features are popular; it is subject to various risks and challenges. National Institute of Standard and Technology (NIST) defines cloud computing as a universal model for sharing pool of resources like applications, networks, services, and storage. These cloud resources or services can be avail to the user in an on-demand and convenient manner. The user can use the cloud services remotely with minimum effort under the management of service provider interaction". The growth of availing cloud services using smart devices has a rapid growth recently. It is estimated that by 2019, the consumer and enterprise market using cloud services via mobile applications has increased to $46.90 billion . In cloud computing, the day-by-day need for cloud services and demands are continuously improving. The primary reasons for this growth are pay-per-use, elasticity, ubiquitous access, elasticity, and pooling resources. The cloud services are deployed under various methods, including private cloud, community cloud, public cloud and hybrid cloud. These cloud services are delivered under multiple delivery methods such as Infrastructure as a Service (PaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [1- 4].

Cloud storage is popular for its advanced efficiency and low cost compared to other technologies. Cloud storage consists of many pools that increase computing services such as"software as a service ."The data center can access the data remotely through a high-quality network connection [1]. Jaidi et al. [2] discussed the access control rules on higher-level integrity. Traditional storage systems, such as cloud storage, fail to provide large storage space accessed from any geographical location. Cloud storage enables cloud customers to access any network with any device, with the essential requirement as a reliable internet connection. Although cloud storage has several advantages, data security remains a difficult issue. Data security has become complex and challenging in handling the number of cloud users, and businesses have grown intensely. As a result, addressing and overcoming data security breaches is critical. Cloud customers can use Cloud Service Provider to get cloud services (CSP). The CSP is a third-party cloud service provider that will deliver services based on the users' needs [1-2].

The CSP contains its security regulations for delivering a service to an approved cloud user. Sometimes the security aspects in cloud storage are questionable, and the reason is users' sensitive data is securely stored, but a third-party vendor provides CSP's storage space. It allows for various attacks, such as virtual machine side-channel attacks . Although the cloud architecture is built with high-security measures, data loss is common. The CSP may occasionally delete data that the user does not frequently use. Even if the user's data is erased, it is still accessible [. These are the most typical problems that cloud users have encountered. These limitations made it difficult for individual cloud users to access cloud services and diminished their popularity.

Verification is complex and essential in the cloud service; it provides data integrity and authenticity in the cloud environment. The verification method had a strong influence on reducing the risk of data theft. The conventional public verification approach for authenticating saved data in cloud storage is the third-party auditing process [6]. Several security models employ the classic public verification approach [7]. The third-party auditing procedure requires verifying and exchanging the acquired data to ensure data integrity. The cloud user does not need to know about the Third-Party Auditor (TPA) process. The TPA will provide the cloud user with a complete auditing report, and the user's stored data integrity verification history. Cloud users do not need to exert any additional effort to use and obtain validated data. A competent TPA policy ensures an error-free working mechanism and guarantees that no copies of user data are obtained [3-7].

The increasing use of mobile devices (mobile computing) also inerts cloud computing's benefits [8]. The latest cloud computing model which gains a lot of attention is Mobile Cloud Computing (MCC). The MCC combines the benefits of cloud computing technology with mobile computing and overcomes mobile computing restrictions. Those are maximization of battery life by outsourcing cloud activities, expanding capabilities and storage, improving dependability by including scalability and dynamic provisioning, etc. The MCC could be characterized as "the availability of cloud computing services in a mobile ecosystem," Cox [9]. Song and Su [10] describe the MCC as a cloud computing application embedded on mobile devices. Technically, the diversity in MCC architectures creates the differentiation in defining the MCC.
This work is organized as follows; in section 1 introduction is discussed, section 2 contains the related work, section 3 contains proposed system and workflow, section 4 contains experimental work and discussion. Finally, section 5 contains the conclusion.

2. Related work

This section discusses various security-based solutions for multi-cloud data storage and retrieval in detail. Lahmar and Mezni [10] established a security-aware multi-cloud service composition approach. It combines RS and fuzzy formal concept analyses (fuzzy FCA) with a solid mathematical foundation. They use FCA and RS calculations to ensure a higher level of security for the hosting cloud and the chosen service. With the elimination of unsecured services and ineligible clouds, this strategy would help to reduce the search space. The experimental results demonstrated the method's overall efficiency and performance.
Patiala et al. [11] designed a hybrid method with a multi-cloud hosting platform to enhance cloud security and privacy. It contains Byzantine protocol for autonomously tolerating security breaches during a cloud server failure. Next, for maximizing the data reliability and security DepSky framework is used in the cloud with encoding and decoding methods. Shamir secret sharing process for improving the trust and privacy of the data storage. In hybrid methods, privacy and security are handled using SAML with Kerberos and proxy re-encryption protocols based on the client requirements.
Tortura et al. [12] developed an advanced cloud security scheme known as CSBAuditor for monitoring the cloud framework. It effectively detects unauthorized modifications and malicious activities in the cloud. The CSB Auditor employs two concepts to overcome the above security issues: state transition analysis and the reconciler pattern. Additionally, a new scoring scheme called Cloud Security Scoring Scheme uses security metrics to compute severity scores to detect vulnerabilities.

Zhu et al. [13] developed MMA, a new scheduling technique for cost optimizing and makespan on maintaining security and dependability. For task scheduling, this technique is divided into two steps. In a multi-cloud platform, the first stage is to find an optimal matching candidate resource for the task to meet their superior requirements such as reliability, security, and performance. The second stage is to iteratively execute many reallocating rounds to achieve optimization on time and cost by reducing the difference between the estimated and actual finishing times. Hybrid chaotic particle search (HCPS), Modified artificial bee colony (MABC), max-min and min-min, modified cuckoo search (MCS), and other algorithms are used to create simulations in CloudSim.
Megouache et al. [14] proposed an advanced system for addressing the security issues in cloud platforms. It contains three stages; in the first stage, a private virtual network is enabled to establish secure data transmission. Secondly, implementing authentication techniques with data encryption to preserve user information and identity. Thirdly, understanding the data reliability of cloud systems is stored. The module achieves identity verification and the ability to communicate with processes running on different cloud providers. As a result, a data integrity technique is established.
Viswanath and Krishna [15] are focused on enhancing the safe architecture that prevents internal attacks. The proposed architecture includes encryption, decryption, data uploading, distribution, indexing, merging, slicing, and retrieval. The hybrid encryption method was created to provide privacy to huge data that had been previously stored in several clouds. The investigation is carried out using a real-world cloud storage platform. For encryption processing, the time taken is approximate 2630 KB/S.
In [16] proposed an advanced framework for achieving cloud security and integrity. It composes the encryption and decryption mechanism, which results in a higher level of data security. The proposed mechanism performances prove its excellence not only in security but also in overall performances. It is suitable for various processes, including malware detection, forensic virtual machine, and real-time monitoring.

In [17] analyzed the various framework and their goal of storing data in the cloud. The proposed framework is a combined approach of 3DES and RSA encryption. However, it has drawbacks inefficiency, privacy, and overload issues while executing multiple functions.
In [18] analyzed the multilevel licensing framework for cloud data penetration. The three-cover framework is used for protecting sensitive cloud data. The security framework for the three films includes overload controls, safety and approval regulations, and security and privacy approaches.
In [19-20] developed a quality-based cloud service broker framework (QCSB). By enforcing metric standards on cloud service providers, the author developed QCSB. However, implementing QCSB takes more time and work. Finally, the author stated that the proposed QCSB material does not help CSPs with cloud computing.

Research motivation

The research work focuses on securing data in multi-clouds. Consider a user who works in the Oil platform and deals with highly sensitive data via smart devices. For the reasons described in the 'Related Work' section, preserving this sensitive information on-site (on a smart device) poses a major concern. But on the other side, the cloud cannot be trusted for storing data in its original format. Even if it has been encrypted for transit, it is not secure. As a result, we offer a new way for safeguarding user data in an untrusted mobile cloud environment by utilizing multi-clouds. The proposed method will secure the privacy and integrity of the user's data, which can be accomplished by splitting, distributing, and protecting the files over many storage clouds. The file's parts will be encrypted before being distributed, increasing security. One file fragment will be retained on the mobile device; it allows future data recovery and reconstruction, ensuring the privacy and secrecy of the targeted file. In the actual world, keeping data in multiple locations increases the possibility of being attacked. Still, this problem can be handled by using data partitioning and encryption on the stored data.

3. Proposed methodology

This section describes the proposed models' architecture and workflow in detail. Initially begins with an explanation about the architecture of the proposed framework. Next, the multi-cloud scheme implementation is described with several comparisons among the used free storage among the CSP’s. Finally, with a discussion about the operational aspects, including data splitting, data compression, API, and Data Encryption.

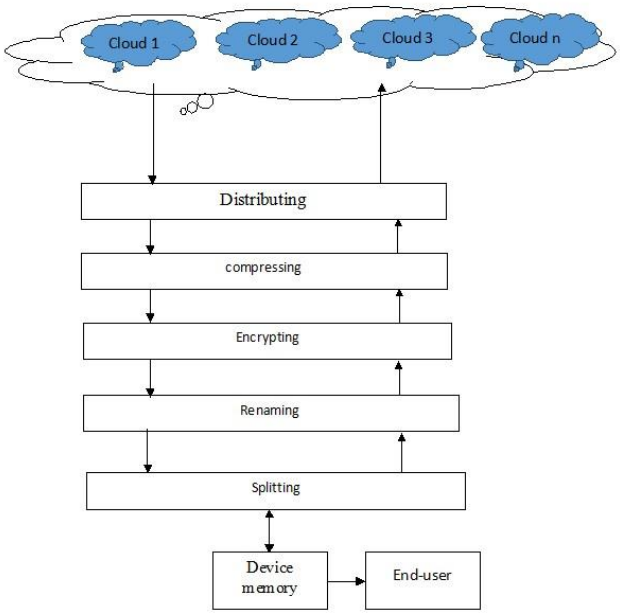

Fig-1 proposed architecture

Frame modules

In the delivered system, on higher layer it is impossible to construct a cloud system with the capability of offering maximum security, availability and reliability. But instead of that lowest layer should be involved. We believe that instead of relying on the service provider, the end-user should specify the necessary security and privacy settings. Furthermore, rather than on the cloud platform, data encryption must be handled on the end user's machine. This will ensure that the information remains private. The end-user assures that the CSP's will be unable to read or alter the data if they do not have the appropriate key, therefore data transmission after encryption is considerably secure.

In the end user's system, keeping of one segment will block any effort to retrieve the distributed data. The reason is that the attacker will need all of the segments and the key to doing so. Furthermore, by preserving the last segment on the end user's workstation, the attacker will be unable to distinguish between the first and last segments of the targeted data, as all exchange segments have the same size.

This process includes partitioning, encrypting, and data distribution over numerous secure multi-cloud storage services and storing only one segment on the smart device. This proposed system fulfills the below-mentioned objectives;

✓ A novel and strong mathematical algorithm, known as the chaotic map encryption technique, is implemented to encrypt the targeted data.
✓ In mobile devices, storing one segment locally prevents the reconstruction of chunk data.
✓ Restricting unauthenticated access during data distribution in a multi-cloud environment and requesting two levels of authentications.

The proposed technique aims to provide a broad range of encryption methods that should be used according to the user's requirements. The user can store one of the segments on the device itself to improve the security level, ensuring that data is not modified or read or decrypted outside of the device. The final method is used to analyze and confirm that claim will be part of future work.

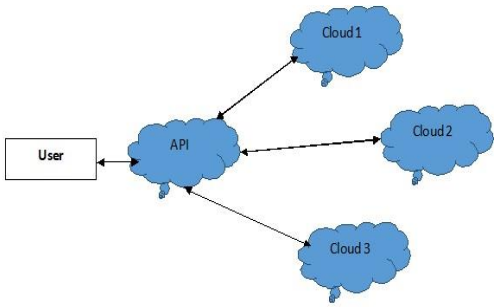

Fig-2 Architecture for multi-cloud

As discussed earlier, the multi-clouds approaches include different free clouds for constructing the multi-clouds model. There are two types of multi-cloud computing schemas as Service-based and Library based. Developers are responsible for creating services that operate as a mediator between users and clouds in a service-based model. The main disadvantage of the service-based model is that if the designed service (mediator) is unavailable then no services are delivered [27]. The developed service allocates between the cloud and the user is illustrated in Fig 2. The library-based architecture allows users to communicate with clouds through a broker, which will be in the form of a library. The developed broker (library) is incorporated with the users' machine (mobile device), offering a higher level of availability than the service-based architecture .

Cloud service providers

In this section, the proposed approach is used to build the cloud and enables multi-clouds library-based architecture with the features as mentioned below;

1) Free capacity
2) Maximum uploaded file size
3) API availability
4) Each GB cost is per month for paid subscription.

Based on the above features, distributed data will be stored, and the distribution process involves two important factors such as

1) User security requirements
2) Involved cloud status

The involved cloud status contains various parameters like access with correct user name and password and service status such as offline or online—the available storage and storage size where the segments are sent.

API

The library-based method will address many of the security and availability problems. From a safety aspect, the library-based method is dependent on a developed library (broker) through cloud APIs. The library is developed by minimizing the exchange of authentication messages among the mobile devices and clouds. As a result, it reduces the opportunity of phishing accessing the information. The unified API connects physical (mobile customer device) and virtual (clouds) resources to compute, monitor, manage and control the usage of multi-cloud resources, as well as accomplish customer privileges. The API also allows customers to select certain cloud service providers, compression, segment sizes, and encryption algorithms. On a technical aspect, the established API is combined with appropriate cryptography and authentication approaches will improve the integrity of the transferred data .

Data Splitting

The targeted file is undergoing data splitting for various reasons such as multi-cloud distribution, restricting cloud maximum-size file problems, etc. Additionally, file partitioning will improve the available bandwidth consumption and load balancing. It will also make the encryption and decryption operations easier by lowering

the size of processed files. Generally, data splitting enhances processing across the board by permitting parallel and pipeline processes, minimizing operational time and costs .

Data compression

In the cloud, data compression on distributed data minimizes the size of the segment's before uploading. It results in the minimization of time consumption, bandwidth, and storages spaces in the cloud. The compression efficiency is determined by the compressed data type, which includes text, image, and videos. For example, the text file is compressed; however, compressing pdf files will not significantly minimize the file size as it is compressed already. All the compressed file sizes are not reduced or save time or money; instead, it will waste system resources with little benefit. In the mobile devices, the compression problem is addressed by utilizing the selected optimum algorithm that provides the best compression while ignoring incompressible data.

4. Cryptography modules (Encryption and decryption process)

Data Authority: Data authority collects or formulates the text, image, audio, and video data. In the cloud platform, the data authority owns the acquired data. which can be shared with other cloud users based on the requirements. Information gathered by the data authority must be protected from unauthorized cloud users. The certificate validates each user requesting the data. The user's credentials are validated, and authorized users can access the cloud data.

Cloud Storage: The CSP provides cloud storage as a cloud service. Through the internet, an authorized user can save and access data remotely. Cloud-based data may be maintained, managed, and backed up. Amazon Elastic Compute Cloud (EC2), Windows Azure, Sun Cloud and Amazon's S3 are the industry's known cloud service providers. It enables the user for data storing and data transferring without incurring any charges. The CSP enables additional capabilities on the private cloud at a cost based on the user's needs. It has various benefits, including confidentiality, dependability, and low cost.

Cloud Service Provider (CSP): CSP manages the necessary data storage service and provides a storage location with some computing resources. The user can access/retrieve the related data from the storage service provided by the CSP. The cloud data storage and servers were handled by the CSP. The host application process is managed by the virtual infrastructure.

End Users: End-user is the most important aspect of cloud computing. The cloud service provider (CSP) must meet end-users' needs, which are conveniently accessible and extremely reliable. The data authorities grant end-users some permissions to process the stored data based on their ability. Reading/writing on the e-stored updated data is included in the consent.

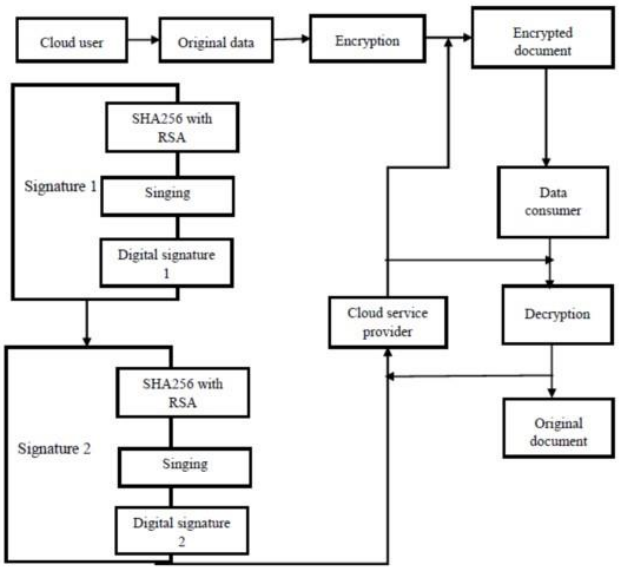

Figure 3 encryption and decryption architecture

Working principle:

Figure 3 describes the proposed architecture, and the process begins with the user registration to the CSP for offering the services. After successful registration, the cloud user can perform operations in the cloud environment. In this paper, the implementation of the proposed system for achieving data storage security is

described. Text, photos, music, and video are the initial data types saved in the cloud. These data types are considered the original data, and it is encrypted before being stored in the cloud. The process of transforming plain text into ciphertext is known as encryption. The proposed system applies a double signature mechanism for protecting data privacy. According to the proposed system, data is first encrypted and sent to the data consumer. Before accessing the storage service, the cloud user encrypts the data using SHA256 with RSA. It's a two-part symmetric algorithm with public and private keys. Initially, the data is encrypted and sent to the CSP with a digital signature 1. Next, the CSP encrypted the data with digital signature 2 and saved it in the cloud. The user will have issued a request to the data consumer for retrieving the original data. The data consumer verifies the request's digital signature and, if it's valid, the user is allowed to access the data stored in CSP. The user must submit the private key during encryption, and the decryption is performed using that key for obtaining the original data. Transforming ciphertext into plain or original text is known as decryption. The implementation of the proposed algorithm involves a step-by-step process as described below;

DSSHA256 with RSA

Step 1: Read the original document, which is to be stored in the cloud database.
Step 2: The sender uses a signing algorithm to sign the message. The message and the signature are sent to the Cloud Server.
Step 3: Key Generation
a) A prime p between 512 and 1024 bits in length is chosen. The number of bits in p must be a multiple of 64.
b) A prime q of 160 bit is chosen to divide (p-1).
c) A primitive element in Zp is chosen and e1 = e0(p-1)/q mod p is calculated.
d) d is chosen as the private key, and e2 = e1d is calculated.
Public key – (e1, e2, p, q)
Private key – d
Step 4: Double Signature
1. A random number r is chosen (1 <= r <=q). New r needs to be chosen each time to sign a new message.
2. The first signature S1 = (e1r mod p) mod q. The value of the first signature does not depend on M.
3. The second signature S2 = (M +dS1) r-1 mod q.
Step 5: Encrypted Document will be sent to cloud Server.
Step 6: Data Consumer initialize the document request
Step 7: Signature Verification
1. 0 < S1 < q is checked.
2. 0 < S2 < q is checked.
3. V = [(e1h(M)S2-1 e2S1S2-1) mod p]mod q
4. If S1 is congruent to V, message is accepted otherwise rejected.

5. Experimental results

Experimental work is conducted to evaluate the proposed multicloud double encryption algorithm with SHA256 with RSA (MC-DS-SHA256) performances. The performance of the proposed MC-DS-SHA256 is compared with fuzzy formal concept analyses (fuzzy FCA) and CSBAuditor. The same dataset with different data types like text, image, audio, and video is taken for executing all three algorithms. The evaluation parameters taken for comparison are file uploading time, file downloading time, encryption, and decryption time concerning file size. Observation of all three algorithms is graphically represented for discussion. The below figures illustrate the observation from the comparison works.

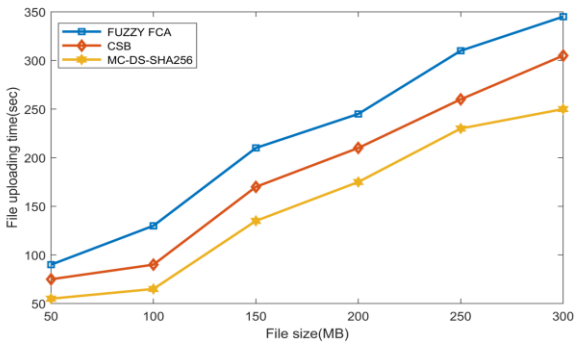

Figure 4: File uploading time VS File Size

Figure 4 shows the comparison work on file uploading time between the proposed MC-DS-SHA256 with CSB and FUZZY FCA. The X-axis defines the file size, and Y-axis defines the time taken for uploading. The file size given as input is measured in terms of MegaBytes (MB), and the time taken is measured in terms of sec. At regular intervals, the given input increases in terms of 50 MB. The observation is plotted in the graph, and each algorithm is represented in a unique color.

File size	FUZZY FCA	CSB	MC-DS-SHA256
50	90	75	55
100	130	90	65
150	210	170	135
200	245	210	175
250	310	260	230
300	345	305	250

Table 1: File size and uploading time taken respective algorithms

Above table 1 shows the obtained result concerning the given load. The file uploading time of proposed MC-DS-SHA256 with 50 MB is 55 sec, 100 MB is 65 sec, 150 MB is 135 sec, 200 MB is 175 sec, 250 MB is 230 sec, and 300 MB is 250 sec. Whereas CSB takes uploading time of 50 MB in 75 sec, 100 MB in 90 sec, 150 MB in 170 sec, 200 MB in 210 sec, 250 MB in 260 sec, and 300 MB in 305 sec. FUZZY FCA took uploading time of 50 MB in 90 sec, 100 MB in 130 sec, 150 MB in 210 sec, 200 MB in 245 sec, 250 MB in 310 sec, and 300 MB in 345 sec. It clearly shows that the uploading time taken by the proposed algorithm is minimal compared to the existing systems.

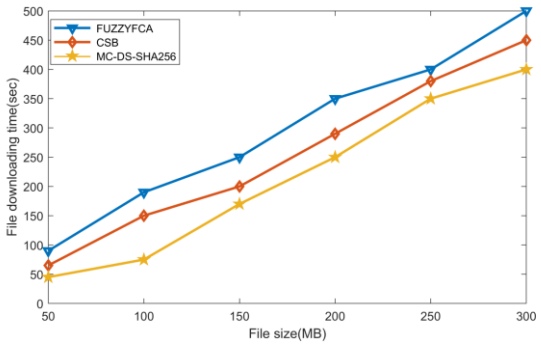

Figure 5: File downloading time VS File Size

Figure 5 shows the comparison work on file downloading time between the proposed MC-DS-SHA256 with CSB and FUZZY FCA. The X-axis defines the file size, and the Y-axis defines the time taken to download the file. The file size given as input is measured in terms of MegaBytes (MB), and the time taken is measured in terms of sec. At regular intervals, the given input increases in terms of 50 MB. The observation is plotted in the graph, and each algorithm is represented in a unique color.

Table 2: File size and downloading time is taken by the respective algorithms

File size	FUZZY FCA	CSB	MC-DS-SHA256
50	90	65	45
100	190	150	75
150	250	200	170
200	350	290	250
250	400	380	350
300	500	450	400

Above table 2 shows the obtained result concerning the given load. The file downloading time of the proposed MC-DS-SHA256 with 50 MB is 45 sec, 100 MB is 75 sec, 150 MB is 170 sec, 200 MB is 250 sec, 250 MB is 350 sec, and 300 MB is 400 sec. Whereas CSB takes downloading time of 50 MB in 65 sec, 100 MB in 150 sec, 150 MB in 200 sec, 200 MB in 290 sec, 250 MB in 380 sec, and 300 MB in 450 sec. FUZZY FCA took uploading time of 50 MB in 90 sec, 100 MB in 190 sec, 150 MB in 250 sec, 200 MB in 350 sec, 250 MB in 400 sec, and 300 MB in 500 sec. It clearly shows that the downloading time taken by the proposed algorithm is minimal compared to the existing systems.

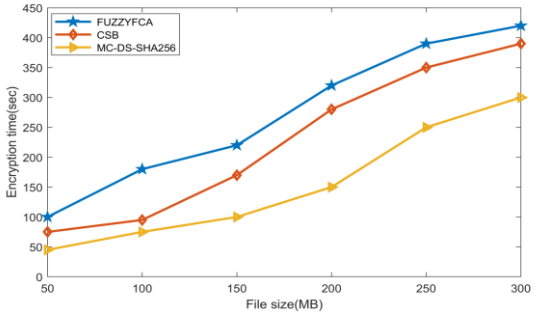

Figure 6: Encryption time VS File Size

Figure 6 shows the comparison work on file encryption time between the proposed MC-DS-SHA256 with CSB and FUZZY FCA. The X-axis defines the file size, and the Y-axis defines the time to encrypt the file. The file size given as input is measured in terms of MegaBytes (MB), and the time taken is measured in terms of sec. At regular intervals, the given input increases in terms of 50 MB. The observation is plotted in the graph, and each algorithm is represented in a unique color.

File size	FUZZY FCA	CSB	MC-DS-SHA256
50	100	75	45
100	180	95	75
150	220	170	100
200	320	280	150
250	390	350	250
300	420	390	300

Table 3: File size and encryption time taken by the respective algorithms

Above table 3 shows the obtained result concerning the given load. According to which the file encryption time of proposed MC-DS-SHA256 with 50 MB is 45 sec, 100 MB is 75 sec, 100 MB is 170 sec, 200 MB is 150 sec, 250 MB is 250 sec, and 300 MB is 300 sec. whereas CSB takes encryption time for 50 MB in 75 sec, 100 MB in 95 sec, 150 MB in 170 sec, 200 MB in 280 sec, 250 MB in 350 sec and 300 MB in 390 sec. FUZZY FCA took encryption time for 50 MB in 100 sec, 100 MB in 180 sec, 150 MB in 220 sec, 200 MB in 320 sec, 250 MB in 390 sec, and 300 MB in 420 sec. The encryption time taken by the proposed system is minimum in comparison to the existing systems.

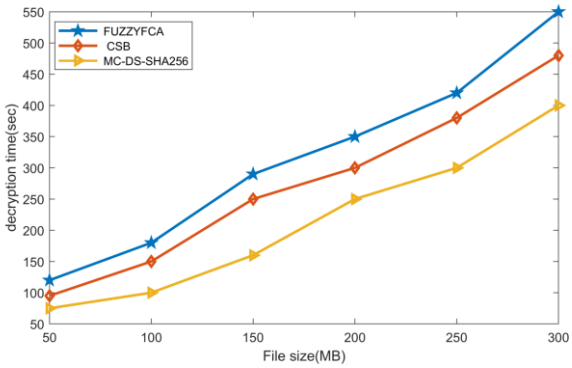

Figure 7: Decryption time VS File Size

Figure 7 shows the comparison work on file decryption time between the proposed MC-DS-SHA256 with CSB and FUZZY FCA. The X-axis defines the file size, and Y-axis defines the time taken for decryption of the file. The file size given as input is measured in terms of MegaBytes (MB), and the time taken is measured in terms of sec. At regular intervals, the given input increases in terms of 50 MB. The observation is plotted in the graph, and each algorithm is represented in a unique color.

Table 4: File size and decryption time taken by the respective algorithms

File size	FUZZY FCA	CSB	MC-DS-SHA256
50	120	95	75
100	180	150	100
150	290	250	160
200	350	300	250
250	420	380	300
300	550	480	400

Above table 3 shows the obtained result concerning the given load. The file decryption time of proposed MC-DS-SHA256 with 50 MB is 75 sec, 100 MB is 100 sec, 100 MB is 160 sec, 200 MB is 250 sec, 250 MB is 300 sec, and 300 MB is 400 sec. Whereas CSB takes decryption time for 50 MB in 95 sec, 100 MB in 150 sec, 150 MB in 250 sec, 200 MB in 300 sec, 250 MB in 380 sec, and 300 MB in 480 sec. FUZZY FCA took decryption time for 50 MB in 120 sec, 100 MB in 180 sec, 150 MB in 290 sec, 200 MB in 350 sec, 250 MB in 420 sec, and 300 MB in 550 sec. The encryption time taken by the proposed system is minimum in comparison to the existing systems.

6. Conclusion and Future Work

In this paper, we proposed a multicloud double encryption algorithm combining SHA256 with RSA (MC-DS-SHA256). The primary goal of this work is to ensure security for mobile computing users at minimum costs. In this work, the significance of cloud computing services and the need for enhancement in security is demonstrated intensely. The concept of transforming cloud services rather than traditional IT solutions increases widely. As a result, there is a massive demand for mobile computing services. Most of the existing systems limit cloud computing services and mobile cloud computing because of the various security threats related to MCC. Hence in this work, using the proposed MC-DS-SHA256, we address the drawbacks of single cloud storage and efficiently avoid phishing attacks by storing one segment of the distributed data on the mobile device. To prove the proposed performance, a comparison work is carried out with fuzzy formal concept analyses (fuzzy FCA) and CSBAuditor. The evaluation metrics for comparison are file uploading time, file downloading time, encryption, and decryption time concerning file size. The observations are plotted graphically, and results are discussed with different workloads. The experimental work shows that the proposed MC-DS-SHA256 performance is far better than the FUZZY FCA and CSB systems.

The future scope can be considered by including additional features and techniques in detecting anonymous attacks and enhancing the security level for cloud users. Implementing own cloud storage (private) in mobile applications and developing a unique security mechanism will be required and appreciable.

Reference

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," 2011.
[2] MarketsandMarkets, "Mobile Cloud Market by Application (Gaming, Entertainment, Utilities, Education, Productivity, Business & Finance, Social Networking, Healthcare, Travel & Navigation), & By User (Enterprise User, Consumer) - Worldwide Market Forecast and Analysis (2014 - 2019) ", 2014. Available at: http://goo.gl/ZF3aVE [Last Access: March 2016]
[3] Josyula, M. Orr and G. Page, Cloud computing: Automating the virtualized data center, Cisco Press, 2011.
[4] B. Furht, "Cloud computing fundamentals," in Handbook of cloud computing, Springer, 2010, pp. 3-19.
[5] Stallings W., Cryptography and Network Security: Principles and Practice, Prentice Hall, 2011
[6] Li T., Liu Z., Li J., Jia C., and Li K., “CDPS: A Cryptographic Data Publishing System,” Journal of Computer and System Sciences, vol. 89, pp 80-91, 2017.

[7] Perbawa M., Afryansyah D., and Sari R., “Comparison of ECDSA and RSA Signature Scheme on NLSR Performance,” in Proceedings of IEEE Asia Pacific Conference on Wireless and Mobile, Bandung, pp. 7-11, 2017
[8] Kaaniche N. and Laurent M., “Data Security and Privacy Preservation in Cloud Storage Environments Based on Cryptographic Mechanisms,” Computer Communications, vol. 111, pp 120-141, 2017
[9] Kumar S., Kumar M., Budhiraja R., Das M., and Singh S., “A Cryptographic Model for Better Information Security,” Journal of Information Security and Applications, vol. 43, pp. 123-138, 2018.
[10] M. Alizadeh and W.H. Hassan, "Challenges and opportunities of mobile cloud computing," in Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International, pp. 660-666,2013.
[11] P.A. Cox, "Mobile cloud computing," Ibm Developerworks, pp. 1-10, 2011.
[12] W. Song and X. Su, "Review of mobile cloud computing," in 2011 IEEE 3rd International Conference on Communication Software and Networks, 2011.
[13] Pachala, S., Rupa, C. and Sumalatha, L., 2021. An improved security and privacy management system for data in multi-cloud environments using a hybrid approach. Evolutionary Intelligence, pp.1-17.
[14] Torkura, K.A., Sukmana, M.I., Cheng, F. and Meinel, C., 2021. Continuous auditing and threat detection in multi-cloud infrastructure. Computers & Security, 102, p.102124.
[15] Zhu, Q.H., Tang, H., Huang, J.J. and Hou, Y., 2021. Task Scheduling for Multi-Cloud Computing Subject to Security and Reliability Constraints. IEEE/CAA Journal of AutomaticaSinica, 8(4), pp.848-865.
[16] Megouache, L., Zitouni, A. and Djoudi, M., 2020. Ensuring user authentication and data integrity in multi-cloud environment. Humancentric Computing and Information Sciences, 10, pp.1-20.
[17] Viswanath, G. and Krishna, P.V., 2020. Hybrid encryption framework for securing big data storage in multi-cloud environment. Evolutionary Intelligence, pp.1-8.
[18] P. Sirohi and A. Agarwal, “Cloud computing data storage security framework relating to data integrity, privacy and trust,” in Proceedings of the 2015 1st International Conference on Next Generation Computing Technologies (NGCT), pp. 4-5, Dehradun, India, September 2015.
[19] K. Subramanian, F. L. John, and F. L. John, “Dynamic and secure unstructured data sharing in multi-cloud storage using the hybrid crypto-system,” International Journal of Advanced and Applied Sciences, vol. 5, no. 1, pp. 15–23, 2018.
[20] H. J. Muhasin, R. Atan, M.A. Jabar, and S. Abdullah, “Cloud computing sensitive data protection using multi layered approach,” in Proceedings of the 2016 2nd International Conference on Science in Information Technology (ICSITech), pp. 69–73, Balikpapan, Indonesia, October 2016.
[21] K. Ravi and K. B. Rajesh, “Quality based cloud service broker for optimal cloud service provider selection,” International Journal of Applied Engineering Research, vol. 12, no. 18, pp. 7962–7975, 2017
[22] H. S. Alqahtani and P. Sant, "A multi-cloud approach for secure data storage on smart device," 2016 Sixth International Conference on Digital Information and Communication Technology and its Applications (DICTAP), 2016, pp. 63-69, doi: 10.1109/DICTAP.2016.7544002.