International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V70I11P228

Volume 70 Issue 11, 258-267, November 2022
© 2022 Seventh Sense Research Group®

Original Article

A Hybrid Cryptography Technique for Cloud Data Security

Swetha Gadde[1] , J. Amutharaj[2] , S. Usha[3]

[1,3]Department of Computer Science and Engineering, Rajarajeswari College of Engineering, Affiliated to VTU, Bengaluru, Karnataka, India
[2]Department of Information Science and Engineering, Rajarajeswari College of Engineering, Affiliated to VTU, Bengaluru, Karnataka, India

[1]Corresponding Author : ursgadde@gmail.com

Received: 12 August 2022 Revised: 07 November 2022 Accepted: 17 November 2022 Published: 26 November 2022

Abstract - *Nowadays, data sharing and storage is one of the most frequent activities associated with cloud computing. Since cloud computing handles large-scale user data at a time, sometimes it contains confidential information or data of the user that needs additional security so that the user can store the information in the cloud storage over the un-trusted computing network. In this regard, cloud data security becomes the primary need for storing confidential information or data over the cloud. The symmetric encryption approach is considered one of the best cryptography techniques to secure cloud data. It provides more security to the cloud information or data than other techniques. This research paper proposes a hybrid symmetric encryption technique to offer additional security to the user's data stored in the cloud compared to the single symmetric encryption approach. The investigated techniques show high processing speed and secure data sharing over the cloud with others. In addition, the computation time associated with the encryption and decryption is also minimized even when multiple users access the same file over the cloud. The proposed method aims to improve the privacy policy by investigating new algorithms for extra cloud data security. There is a broad scope of cryptography techniques in cloud computing, not only for securing the cloud data but also for solving various security and privacy issues while dealing with confidential data.*

Keywords - *Cryptography, Cloud Data, Decryption, Data Security, Encryption.*

1. Introduction

Cloud computing presents a holistic approach to offering services by reorganizing diverse content developed for consumers based on individual needs. It is also crucial for next-generation cellular telecommunications, hacking, and social computation. Cloud storage substantially decreases customers' storage load and provides them access flexibility, making it one of the essential cloud computing[1]. However, cloud data protection, transparency, and trust have emerged as critical issues affecting the viability of cloud services and perhaps impeding the advancement of 5G (Fifth Generation) and cyber systems. To begin with, putting data in the cloud raises the danger of data leakage and fraudulent activity. Second, cloud computing services are increasingly emerging targets of assaults and breaches, posing a threat to cloud data security[2]. Database management activities in the cloud, such as information storage, restoration, migration, erasure, update, searching, querying, and accessibility, may not be fully trusted by their owners. Cloud providers should preferentially audit the dependability of data management. Any source of incursions and assaults should be detectable and trackable. The above criteria provide a significant security issue, particularly for ample data storage and processing. Data processing and computing on the cloud may expose data owners' or associated entities' privacy to unauthorized parties. Another intriguing and essential research issue is approving cloud data processes and safeguarding data processing results. Cloud data security, transparency, and trust are indeed becoming critical factors affecting cloud technology success[3].

Cryptography is frequently used in cloud technology to protect data, confidentiality, and integrity. Cloud cryptographic algorithms data encryption to safeguard data will be used or kept private[4]. It enables customers to quickly and safely use shared cloud storage since any data held by cloud service providers is encrypted[5]. Cloud cryptography secures sensitive information without slowing the flow of information. Cloud cryptography is centered on encryption, which involves machines and methods to jumble text into ciphertext. This ciphertext can then be turned into plaintext by deciphering it using a sequence of bits using an encryption key[29]. The encryption of data can take place in one of the following ways, listed in Table 1.

Table 1. List of the Different Ways for the Encryption of the Data in Order to Hidden or Inaccessible to Unauthorized Users

S. No.	Cryptography algorithms	Description
1	Cryptographic Algorithm Based on Symmetric Key	Because data encrypted with a single secret identifier cannot be decoded with any other key, this technique provides authentication and authorization to the data. The most common Symmetric-key Algorithms used in cloud computing for cryptography are Data Encryption Standard (DES) and Advanced Encryption Standard (AES).
2	Cryptographic Algorithm Based on Asymmetric Key	In order to safeguard the data on the cloud, this method employs two distinct keys for encryption and decryption. RSA (Rivest-Shamir-Adleman) and Diffie-Helman Algorithm are the algorithms utilized in cloud technology.
3	Hashing	It is mostly used to index and retrieve entries from a database. It also employs two distinct keys for encryption and decryption messages.

Table 2. List of the Cryptography Algorithms Utilized for Cloud Data Security to Prevent from Any Unauthorized Access of Data.

S. No	Data encryption ways	Description
1	Synchronization of the pre-encrypted data with cloud storage	There is a technology system to pre-encrypt data before it is sent to the cloud, making it difficult to read for anybody attempting to hack it.
2	End-to-end Data encryption	Communications are sent by senders and received by receivers, who are the only people who really can receive them.
3	Encryption of File	When information is at rest, it is encrypted, so if an intruder tries to intercept the file, it will not be able to read the data it contains.
4	Encryption of Full disk	When saving files to an external disc, they are immediately encrypted. This is the most critical method for securing computer hard drives.

Cloud cryptography provides the same degree of security to cloud computing by encrypting stored data. It can secure critical cloud data without causing data transfer to be delayed. To incursion stability among security as well as efficiency, several companies design multiple cryptographic protocols for cloud computing[7]. The cryptography algorithms used for Cloud Security are discussed in Table 2.

Among all three cryptography algorithms, the symmetric key cryptography algorithm is considered one of the most promising techniques for cloud data security. It provides better security features as compared to the other techniques. In recent years, it gained significant attention from many researchers for improving the security features of cloud computing. Previously, various techniques have been investigated based on the single key symmetric encryption algorithms, but the most common challenges these techniques face are high computation time for encryption and description while multi-users are accessing or sharing the files over the cloud. In order to overcome such challenges, this research paper investigates a novel method for enhancing the security associated with cloud data. The investigated approach is established on the hybrid symmetric key cryptography, which provides additional security features and high processing speed compared to the single key symmetric encryption algorithms. The Research gap identified that there is no security to storing data in the cloud and accessing data from the cloud using normal encryption and decryption techniques. Providing privacy and security of data to store in the cloud is a major issue for users. So, here, using a Hybrid cryptographic technique provides security to the data.

2. Literature Review

For increasing information security over the internet, many researchers have investigated various methods for offering security to data stored in the cloud to maintain data integrity and confidentiality. Sudha et al. investigated a security architecture based on the cryptography technique for increasing the certainty of information by incorporating private and public key-based cryptosystems. The proposed method was explored for different cloud-based applications. The method's performance was evaluated and verified by utilizing the test cases. The proposed method was based on the AES, Secure hash algorithm (SHA) and RSA algorithms, which provided additional security to the cloud data at a low cost. The reported method had a scalability feature with the lost cost for accessing and sharing the data over the cloud more efficiently [8].

Arockiam et al. investigated an approach for ensuring the confidentiality of the data over the cloud. This study presented a novel cryptographic approach for dealing with this challenge. Encrypted data is kept on a cloud server while the data owner retains the secret key(s); consumer accessibility is provided by distributing the relevant information encrypted messages. Obfuscation, in addition to encryption, is used to improve data secrecy. The data before transfer to cloud storage, the user information is encrypted or obfuscated. The proposed approach is secure for storing cloud users' data in the cloud services. Only encryption or concealment is insufficient for cloud storage. The combination of these approaches should give the highest level of security for user information in the cloud[9].

Sandeep K. Sood proposed a technique for improving cloud data security in cloud computing. The suggested approach protects information, confirms its reliability, and validates it by retaining the finest manufacturing procedures. It includes data dissection, a directory producer, 128-bit secure sockets layer (SSL) cryptography, communication authentication cypher, as well as a dual verification of the user, firstly done by the owner and the secondary done by the cloud service provider, as well as certification of the digital signature of the owner. It ensures data obtainability by overcoming numerous difficulties, such as data leaks, manipulation, and illegal contact from service providers. The investigated technique ensures information's obtainability, dependability, and authenticity as it travels from the proprietor to the cloud and from cloud storage to the user. Furthermore, it gives greater tractability and competence to encounter the changing demands of an increasingly challenging and diversified network and the capacity to recover files from the cloud by scanning through encrypted data[10].

Swetha et al. investigated a symmetric key-based technique for protected data access in the cloud through the internet. Only authorized users have access to the key used in the decryption procedure. By utilizing the hybrid symmetrical encryption method, the data owner assures that it offers additional protection for information, and the user is certain that the data obtained by the user is unbroken and free of intruder access. Because the cloud service provider is an untrustworthy third party, the system administrator cannot keep their private data in its raw form.[11]. Hosam et al. developed a hybrid framework for cloud data security. To provide safe data storage and exchange, the symmetrical algorithm AES [28] and the asymmetric cryptography technique of Elliptic curve cryptography (ECC) are utilized. To safeguard encryption keys from unauthorized attackers, Least significant bit (LSB) image steganography was employed[12].

Cloud computing is prevalent in businesses and organizations because it offers low-cost storage and computing services. However, it poses additional problems in maintaining data confidentiality, integrity, and access control. Various techniques are provided to satisfy these security criteria; however, they fall short in some respects, such as data confidentiality violations owing to collusion attacks and expensive processing (due to the large no. of keys). As previously stated, considerable research in the literature has been conducted to address these concerns. The reported algorithms for providing security over the cloud are facing challenges while a number of users access the file over the cloud. It significantly increases the computation time for encryption and decryption[13]. The proposed hybrid algorithm helps to overcome such challenges while dealing with multi-users over the cloud, minimizes processing time for encryption and decryption, and provides additional security to could data.

Subramanian, E.K. and Tamilselvan, L. [31] has been proposed an Elliptic curve with Diffie-Hellman (ECDH) algorithm for data security in the cloud storage system. This approach enhanced data security by encrypting the data before being preserved in the cloud. It maximized the encryption effectively and minimized the computational complexity. ECDH was compared with the RSA, MRSA and MRSAC.

3. Methodology

3.1. Design

The proposed methodology utilizes the hybrid symmetric key encryption algorithm, which consists of mainly four components, as illustrated in Figure 1. Each component plays an essential role in the whole process while dealing with the information or data.

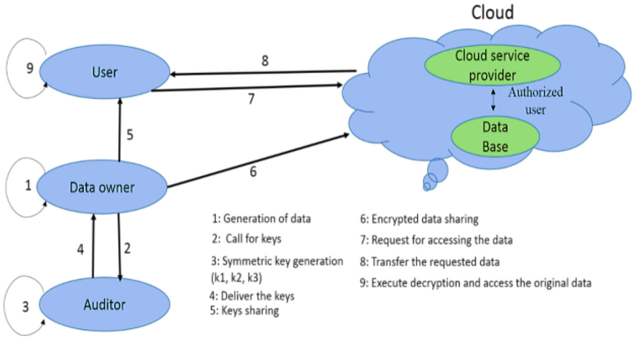
Cloud
User
Data owner
Auditor
Cloud service provider
Authorized user
Data Base
1
2
3
4
5
6
7
8
9
1: Generation of data
2: Call for keys
3: Symmetric key generation (k1, k2, k3)
4: Deliver the keys
5: Keys sharing
6: Encrypted data sharing
7: Request for accessing the data
8: Transfer the requested data
9: Execute decryption and access the original data

Fig. 1 Schematic Illustration of the Proposed Methodology Based on Hybrid Symmetric Key Algorithm for Cloud Data Security

3.1.1. Data Owner

The data owner [14]is responsible for managing all user activity, which implies that various users are accessing their files and have network privilege access. The administrator has the authority to approve or reject recently registered user requests. If the owner grants permission to a new user, the user may log in to their panel and access their privileges, such as uploading, downloading, and sharing files. The owner may also examine all files saved by all users as well as the activity of the sharing mechanism[15]—multiple users listed on the user portal whom the owner may also view. The owner's data requires protection against harmful behavior by intruders and the release of sensitive information. As a result, the owner must encrypt the information before transferring as well as maintaining it on a server of the cloud

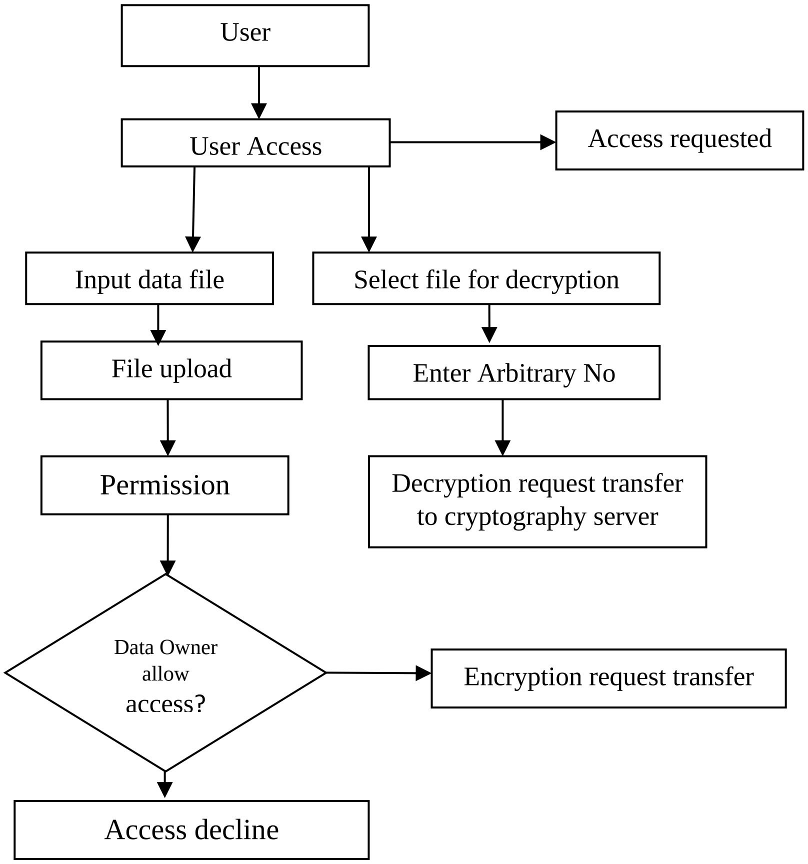

Fig. 2 Schematic Illustration of Flow Diagram of the Various Activities Performed by User Side for Accessing the Data

3.1.2. Cloud Service Provider

Cloud services[16] provide cloud computing-based infrastructure and platform services for customers using their own data centers and computational resources. It serves as the owner's data storage and infrastructure and a service provider[30] for end customers. In this case, the service supplier is an exterior third firm in which the data owner does not have total trust.

3.1.3. User

It is an individual that uses data created and shared by the system administrator via an untrusted network. Only the authorized user for a particular data set can access the decryption key. After the cloud service provider authenticates the user, the user will receive the needed service. Different actions are being performed concurrently in the user area, such as file syncing. The overall process of the user portal is demonstrated using Figure 2.

3.1.4. Key Producer

It is a vital object that is in charge of creating the keys that will be utilized for the encryption and decryption of private information and the session key that will be pooled amongst various users during the syncing or transferring of information over an unprotected system[17]. The utilization of a term key aids in the establishment of safety concerns such as truthfulness as well as non-repudiation.

The Cryptography servers[26] are a responsible third party in charge of key management, encryption, decryption, and user access permissions. The cryptography servers (CS) produce the symmetric key and use it to secure sensitive information. The cryptography server keeps track of all possible user requests and sharing kinds. In our proposed approach, the CS is considered a secure object. The CS might be held by a corporation or third-party supplier[18]. However, an organization's CS will establish greater faith in the system for end-user applications. The suggested method keeps a single secret key for each user's data file. Figure3 illustrates the whole encryption, decryption, and management of keys procedure. The user entities and the CS interface are both required for the entire data protection and sharing procedure to be completed.

In the preceding instance, we saw how access requests are sent to the CS portal[19] for encryption and decryption. Once a file has been uploaded by the user and comparable access and sharing permissions have been executed by CS, the primary responsibility for guaranteeing user data security is the encryption and decryption of the file.

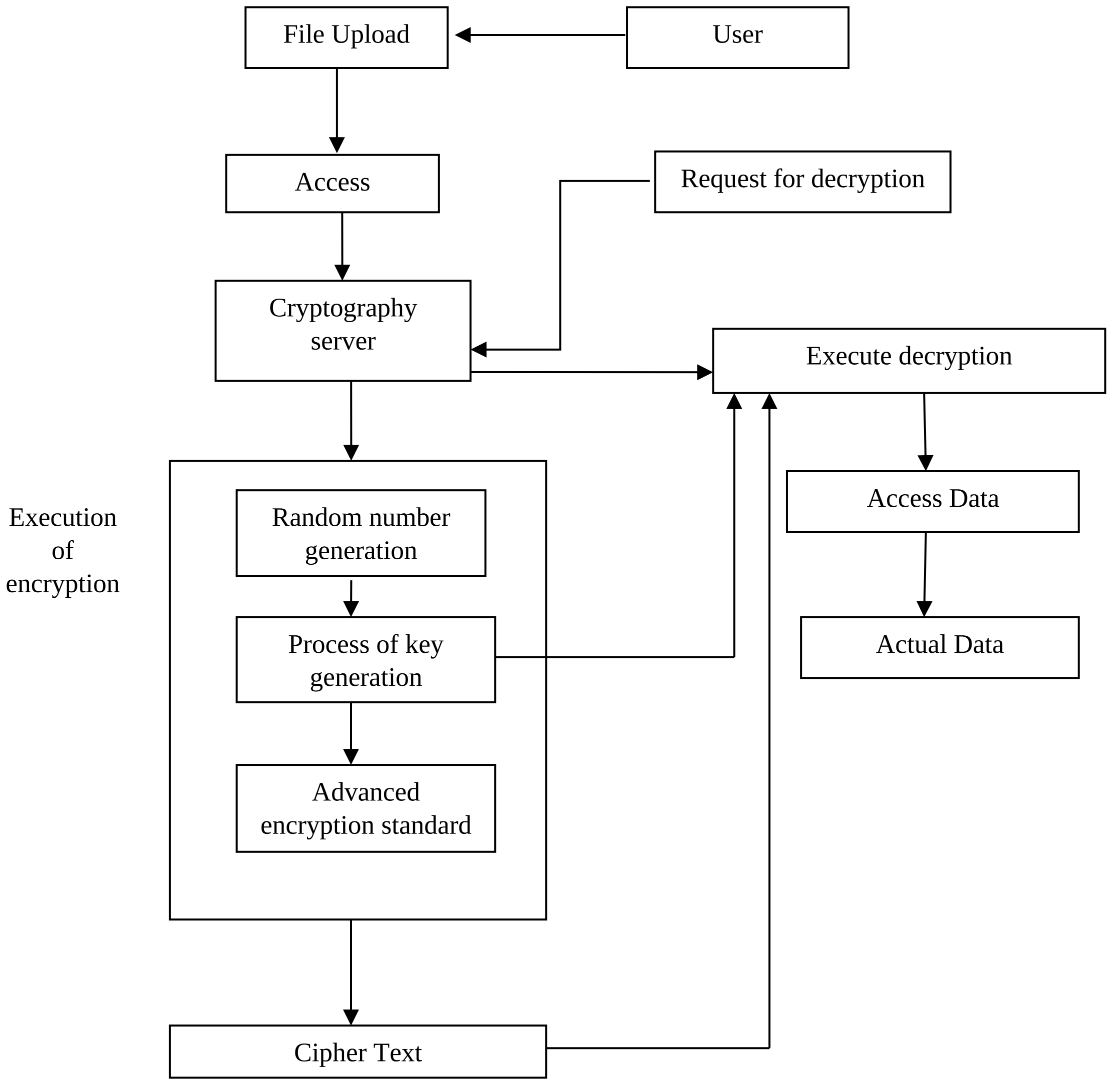

Fig. 3 Schematic Illustration of the Flow Diagram of the Overall Process Performed by the Cryptographic Server

In the first instance, the CS initiates the encryption process and is only utilized when the user needs to decrypt a file at the end of decryption. This random number will be emailed to the group user's email address. Following that, an encryption key is created for use by the cryptography. The overall process of key generation is shown using Figure 4.

It is necessary to emphasize the process of key encryption at the key generation level. In order to keep our security commitments, encrypt the key that is also used for file encryption. First, produced the components and bytes from the input file data. The SHA-1 [20]hash method and particular flag value are then applied to this data. Depending on the Key, the flag should be 0 or 1. This procedure will produce a hash key and apply a cryptosystem to this hash value. This method encrypts the key positively. For the aim of key variation[25], feed the components and byte information of the file name into the protected key again, and it will receive the full primary key of data that is required for data encryption using the AES algorithm[21]. As a result, it encrypts the input data file with this total key data value. As a result, it will create the ciphertext (encrypted text). The whole procedure combines essential creation and file encryption.

Similarly, the user sends a decryption request to the CS to decrypt a data file, and the CS processes the request. The CS will decode the data by obtaining the ciphertext and total key data value, which will then be sent via the AES algorithm. Following this procedure, encrypted data, i.e. original text, is generated. This information is obtained from the user portal. The whole operation of the CS that is fully maintained systematically involves encryption, decryption, and key management[23][24]. It ensures safe data file exchange among users and complete security against harmful outside activities.

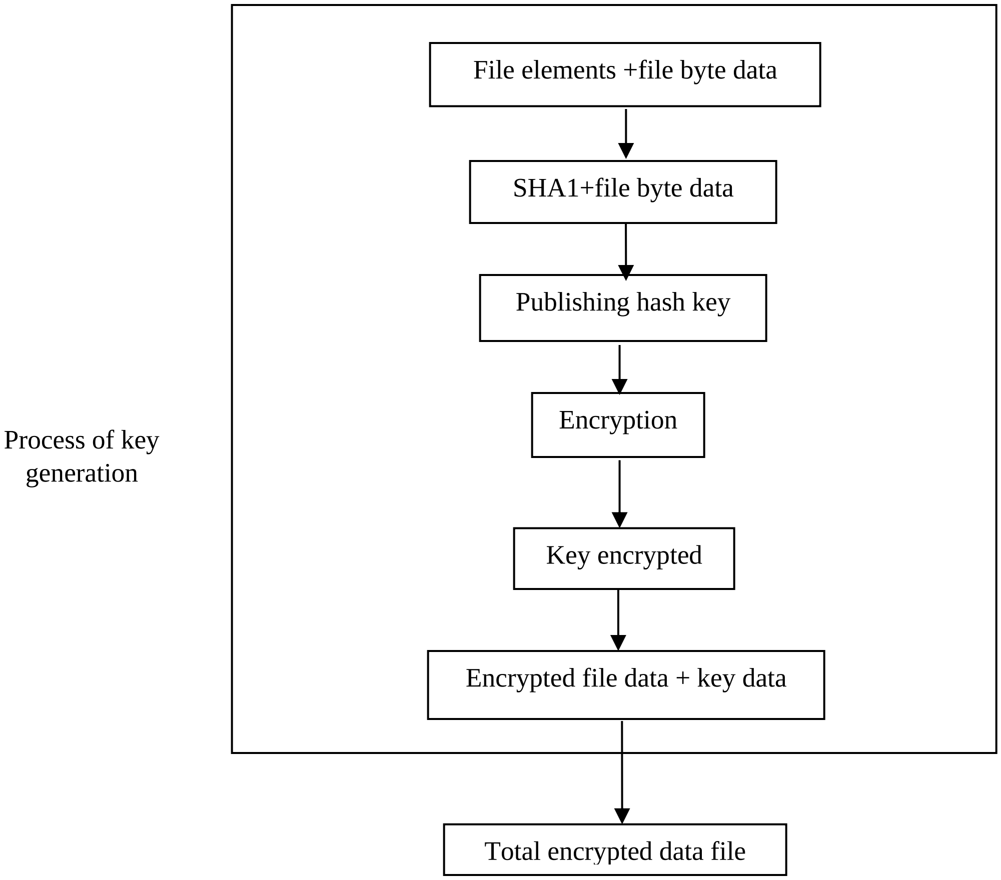
File elements +file byte data
SHA1+file byte data
Publishing hash key
Encryption
Key encrypted
Encrypted file data + key data
Process of key generation
Total encrypted data file

Fig. 4 Schematic Illustration of the Process of Key Generation Based on Secure Hash Algorithm-1 (SHA-1)

3.2. Instrument

A functional prototype of the proposed methodology is developed using python language comprising features of NetBeans IDE 8.1 as well as database support of MySQL 5.6. This framework's scheme is powered by an Intel Quad-Core CPU, 4 GB RAM, a 1 TB storage disc, and the Windows 10 operating system. To name a few, a square matrix is constructed, filled from left side and bottom to top, a key is generated, the plaintext is encrypted and decoded and so on. The data owner's exclusive responsibility is to secure sensitive information and transmit it to the provider. Keys are only distributed to authorized users via a secure network. Data owners do not truly save any content, instead sending everything to the provider, who then stores it on its servers[31]. Data storage of owner and transmission expenses are identical to those of the key generators. The user also gets data from the provider and keeps it for future analysis, while the provider is responsible for storing and sending the owner's data to authorized users, thereby saving on both transmission and storage costs.

3.3. Data Collection

Cloud computing is now utilized to provide various on-demand services, including servers, databases, software, and storage. Among all cloud computing services, cloud storage is considered a promising service is offering cloud computing. Cloud storage provides the facility to store large-scale data on the internet by the cloud computing provider which handles cloud computing. Despite having various benefits of cloud storage, one of the most common issues associated with cloud storage is security. Due to the lack of visibility and inability to control the data, there is a chance of leaking confidential data. Data security is one of the most significant challenges associated with cloud storage. To tackle this issue, cryptography is considered one of the most promising techniques for offering the security data of the cloud. Cryptography provides encryption algorithms in order to secure cloud data. By giving importance to cloud data security, this paper investigated a hybrid cryptography technique for cloud data security. The hybrid symmetric key algorithm has been developed by utilizing the python language features with NetBeans IDE 8.1 as well as database support of MySQL 5.6. In order to collect the data for the computation time for the encryption and decryption, many experiments have been performed, as illustrated in Table 3.

3.4. Data Analysis

To understand the proposed technique's working, the collected data has been analyzed by comparing various parameters. Some of the most common analysis parameters are bits changed and sensitivity. These security parameters are used to evaluate the parameters through data analysis. Figure

5&6 illustrates the data associated with the bits changed and the sensitivity High-speed processing ability, the computation time for the encryption and decryption of the data over the cloud and multiple users accessing files from the cloud at a time, respectively.

Table 3. Number of Experiments Performed for Encryption and Decryption of Cloud for the Measurement of Data Computation Time

Number of Experiments	Encryption Time (ms)				Decryption Time (ms)			
	10 kB	20 kB	30 kB	40 kB	10 kB	20 kB	30 kB	40 kB
1	2.4	3.2	4.3	5.5	2.3	3.3	4.2	5.4
2	2.3	3.2	4.1	5.5	2.4	3.3	4.3	5.5
3	2.4	3.3	4.3	5.4	2.4	3.2	4.3	5.5
4	2.4	3.2	4.3	5.5	2.4	3.2	4.2	5.3
5	2.3	3.2	4.3	5.5	2.4	3.2	4.2	5.5

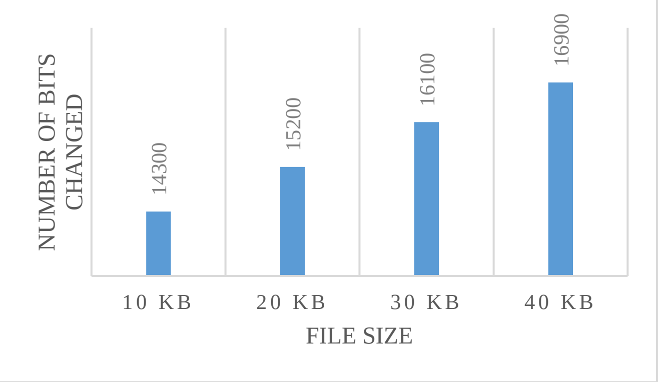

Fig. 5 Bar Diagram of the Number of Bits Changed for Different File Sizes of Data Which Stored in the Cloud through the Internet

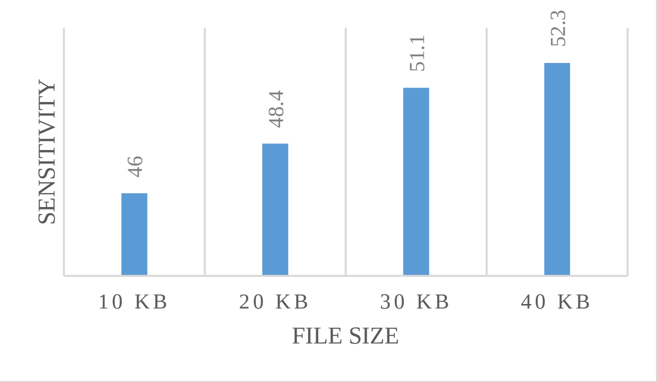

Fig. 6 Bar Diagram of the Sensitivity for Different File Sizes of Data Which Stored in the Cloud through the Internet

4. Results and Discussion

The investigated algorithm for cloud data security over the cloud is responsible for the key generation used for encrypting the data. In order to generate the primary key (k_1), the key generator initializes and creates a keyword with the length of 5 elements, followed by filling in the 4×4 table. In order to prevent the repetition of the character, the character fills from the bottom to the top and right to left. Select a variable length keyword for generating the secondary keys (i.e., k2 and k3).

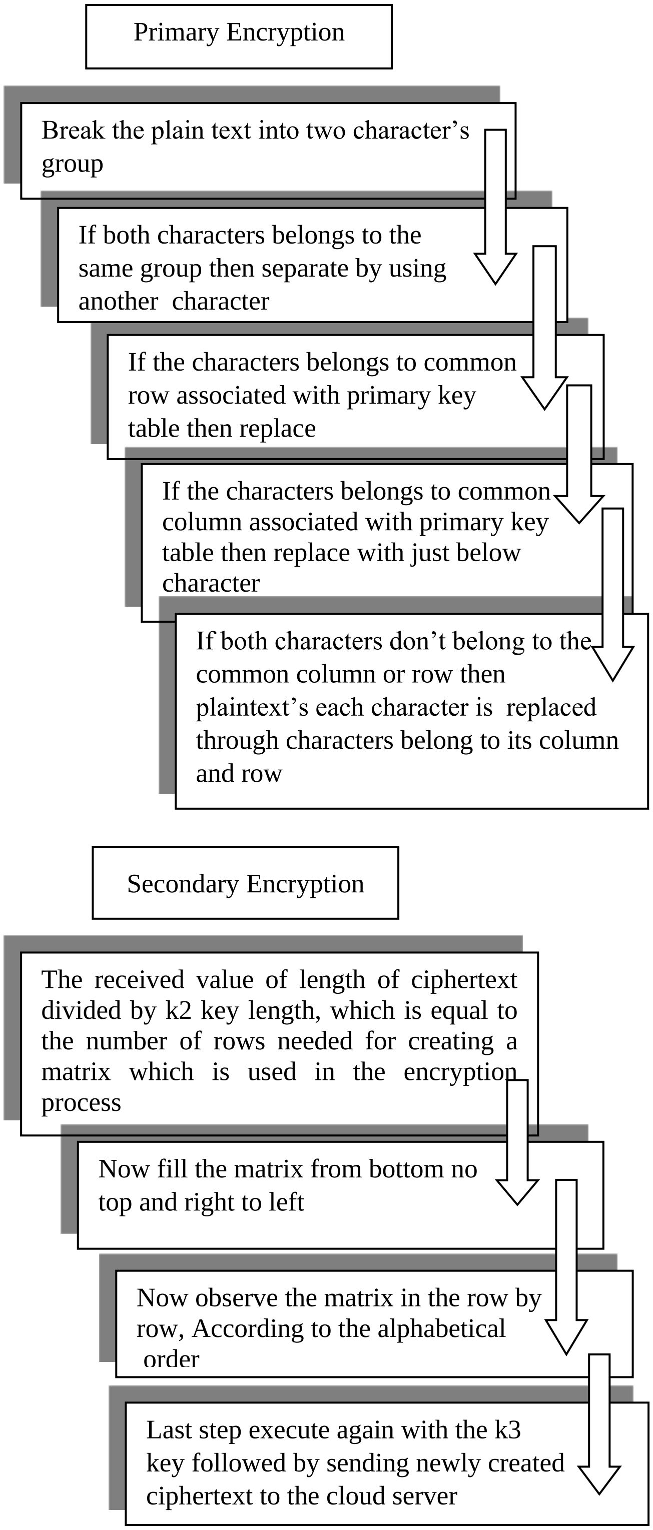
Primary Encryption
Break the plain text into two character's group
If both characters belongs to the same group then separate by using another character
If the characters belongs to common row associated with primary key table then replace
If the characters belongs to common column associated with primary key table then replace with just below character
If both characters don't belong to the common column or row then plaintext's each character is replaced through characters belong to its column and row
Secondary Encryption
The received value of length of ciphertext divided by k2 key length, which is equal to the number of rows needed for creating a matrix which is used in the encryption process
Now fill the matrix from bottom no top and right to left
Now observe the matrix in the row by row, According to the alphabetical order
Last step execute again with the k3 key followed by sending newly created ciphertext to the cloud server

Fig. 7 Schematic Illustration of the Process Flow of the Primary and Secondary Encryption Algorithm of the Cloud Data

In order to identify the row number for re-encryption, the keyword length, as well as the message, is used. The encryption has been done in two parts, i.e., primary and secondary. The encryption algorithm is described in Figure 7. In order to effectively

In the process of encryption and decryption over the cloud, the results produced from the suggested approach are examined for different text file sizes. The encryption time of the system is the amount of time necessary to execute the encryption process using the chosen algorithm. The algorithm's decryption time is the length of time it takes to retrieve the original data from encrypted text. The computation time for the encryption and decryption of the data is illustrated in Figure 8. The figure clearly shows that the reported model performance is excellent in terms of processing speed. The computation time for encryption and decryption is significantly minimized compared to the existing methodologies for cloud storage security.

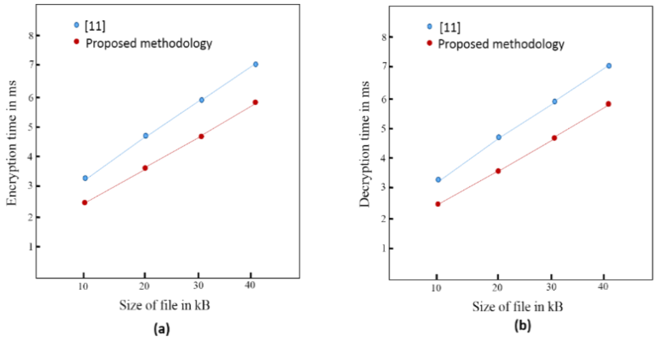

Fig. 8 Graphical Representation of the Computation Time of the Proposed Methodology for: (a) Encryption and (b) Decryption[11]

The computation time for the encryption and decryption of the proposed methodology has been obtained for the different sizes of the file. In this study, 10 kB, 20 kB, 30 kB and 40 kB sizes of the file data were utilized to order to evaluate the computation time. It has been observed that when the file size of the data increases, the computation time for encryption and decryption increases significantly. For the encryption of the data, 2.4 ms, 3.2 ms, 4.3 ms and 5.5 ms computation time has been recorded for the 10 kB, 20 kB, 30 kB and 40 kB file size data, respectively. For the decryption of the same data, almost the same computation time is required. The result of the computation time data shows the potential of the proposed methodology in terms of the high processing speed while accessing the data over the cloud. A comparative study has been done (as shown in Table 4) to evaluate the working of the proposed method. In Table 3, it is clear that the working of the investigated method is excellent in terms of the various parameters compared to the proposed methodologies in the literature.

Table 4. Functionality Comparison amongst the Various Proposed Methodologies in the Literature

Functionality	[13]	[14]	[15]	[16]	**Proposed technique**
Authorization	Yes	Yes	No	Yes	Yes
Integrity	Yes	Yes	No	No	Yes
Authentication	No	Yes	Yes	Yes	Yes
Encryption	Yes	No	No	Yes	Yes
Identification	Yes	Yes	Yes	Yes	Yes

5. Conclusion and Implication

Before sending and storing any private data over the cloud, data security becomes a fundamental need. Cloud computing allows storing data over the cloud more flexibly, which raises the risk of an intruder assault. To address this issue, cryptography is the only method that allows sensitive data to be encrypted before being transferred to the cloud, with only authorized users having access to the decryption key. This paper investigates a novel method based on the hybrid encryption approach for providing security to the data over the cloud. Hybrid cryptography techniques provide various advantages over the single cryptography technique, including high-speed processing ability and minimized computation time for the encryption and decryption of the data over the cloud. Another significant advantage is that it can handle the number of users at a particular time while accessing the file over the cloud. Due to the high complexity of the framework, the proposed method provides additional security to the cloud storage data that will prevent any cyber-attack. Although extensive research has been done in the field of cryptography techniques for data protection, there is a broad scope to explore the frameworks based on advanced encryption algorithms for cloud data security. The Hybrid Cryptography techniques prove the novelty of work compared to existing methods in terms of performance metrics like computation time, accessing files and providing high security to the data that will store in the cloud to prevent cyber attacks.

References

[1] Lizhe Wang, Gregor von Laszewski, Andrew Younge, Xi He, Marcel Kunze, Jie Tao and Cheng Fu "Cloud Computing: A Perspective Study," *New Generation Computing*, vol. 28, no. 2, pp. 137–146, 2010. Crossref, https://doi.org/10.1007/s00354-008-0081-5

[2] L. M. Kaufman, "Data Security in the World of Cloud Computing," *IEEE Security & Privacy*, vol. 7, no. 4, pp. 61–64, 2009. Crossref, https://doi.org/10.1109/MSP.2009.87

[3] R. V. Rao and K. Selvamani, "Data Security Challenges and its Solutions in Cloud Computing," *Procedia Computer Science*, vol. 48, pp. 204–209, 2015 Crossref, https://doi.org/10.1016/j.procs.2015.04.171

[4] N. Jirwan, A. Singh, and S. Vijay, "Review and Analysis of Cryptography Techniques," *International Journal of Scientific and Engineering Research*, vol. 4, no. 3, pp. 1–6, 2013.

[5] A. J. Amalraj and J. R. Jose, "A Survey Paper on Cryptography Techniques," *International Journal of Computer Science and Mobile Computing*, vol. 5, no. 8, pp. 55–59, 2016.

[6] Olu Olu Osaronwolu, Matthias Daniel and V. I. E Anireh, "A Secured Deduplication of Encrypted Data Over an Attribute-Based Cloud Storage," *SSRG International Journal of Computer Science and Engineering,* vol. 7, no. 7, pp. 77-83, 2020. Crossref, https://doi.org/10.14445/23488387/IJCSE-V7I7P113

[7] V. K. Mitali and A. Sharma, "A Survey on Various Cryptography Techniques," *International Journal on Emerging Trends in Technology*, vol. 3, no. 4, pp. 307–312, 2014.

[8] M. Sudha and M. Monica, "Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography," *Advances in Computer Science and its Applications*, vol. 1, no. 1, pp. 32–37, 2012.

[9] L. Arockiam and S. Monikandan, "Efficient Cloud Storage Confidentiality to Ensure Data Security," in *2014 International Conference on Computer Communication and Informatics,* pp. 1-5, 2014. Crossref, https://doi.org/10.1109/ICCCI.2014.6921762

[10] S. K. Sood, "A Combined Approach to Ensure Data Security in Cloud Computing," *Journal of Network and Computer Applications*, vol. 35, no. 6, pp. 1831–1838, 2012. Crossref, https://doi.org/10.1016/j.jnca.2012.07.007

[11] S. Kaushik and C. Gandhi, "Cloud Data Security with Hybrid Symmetric Encryption," in *2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT),* pp. 636-640, 2016. Crossref, https://doi.org/10.1109/ICCTICT.2016.7514656

[12] O. Hosam and M. H. Ahmad, "Hybrid Design for Cloud Data Security using Combination of AES, ECC and LSB Steganography," *International Journal of Computational Science and Engineering,* vol. 19, no. 2, pp. 153–161, 2019. Crossref, https://doi.org/10.1504/IJCSE.2019.100236

[13] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure Ranked Keyword Search Over Encrypted Cloud Data," in *2010 IEEE 30th International Conference on Distributed Computing Systems*, pp. 253–262, 2010. Crossref, https://doi.org/10.1109/ICDCS.2010.34

[14] B. Chor, N. Gilboa, and M. Naor, “Private Information Retrieval by Keywords,” *Citeseer*, 1997.

[15] P. Prasad, B. Ojha, R. R. Shahi, R. Lal, A. Vaish, and U. Goel, "3-Dimensional Security in Cloud Computing," in *2011 3rd International Conference on Computer Research and Development*, vol. 3, pp. 198–201, 2011. Crossref, https://doi.org/10.1109/ICCRD.2011.5764279

[16] S. K. Sood, A. K. Sarje and K. Singh, "A Secure Dynamic Identity-Based Authentication Protocol for Multi-Server Architecture," *Journal of Network and Computer Applications*, vol. 34, no. 2, pp. 609–618, 2011. Crossref, https://doi.org/10.1016/j.jnca.2010.11.011

[17] Atiewi S, Al-Rahayfeh A, Almiani M, Yussof S, Alfandi O, Abugabah A and Jararweh Y, “Scalable and Secure Big Data Iot System Based on Multifactor Authentication and Lightweight Cryptography,” *IEEE Access*, vol. 8, pp. 113498–113511, 2020. Crossref, https://doi.org/10.1109/ACCESS.2020.3002815

[18] Barrett P, “Implementing the Rivest Shamir and Adleman Public Key Encryption Algorithm on a Standard Digital Signal Processor,” In *Conference on the Theory and Application of Cryptographic Techniques*, *Springer*, Berlin, Heidelberg, vol. 263, pp. 311–323, 1986. Crossref, https://doi.org/10.1007/3-540-47721-7_24

[19] Chidambaram N, Raj P, Thenmozhi K and Amirtharajan R, “Advanced Framework for Highly Secure and Cloud-Based Storage of Colour Images,” *IET Image Process*, vol. 14, no. 13, pp. 3143–3153, 2020. Crossref, https://doi.org/10.1049/iet-ipr.2018.5654

[20] Fu X, Nie X, Wu T and Li F, “Large Universe Attribute based Access Control with Efficient Decryption in Cloud Storage System,” *Journal of Systems and Software*, vol. 135, no.c, pp. 157–164, 2018 Crossref, https://doi.org/10.1016/j.jss.2017.10.020

[21] BalasubramanianPrabhu kavin and Ganapathy S, “A Secured Storage and Privacy-Preserving Model Using CRT for Providing Security on Cloud and Iot-Based Applications,” *Comput Networks*, vol. 151, pp. 181–190, 2019. Crossref, https://doi.org/10.1016/j.comnet.2019.01.032

[22] Arun Pratap Singh and Himanshu Pundir, "Secure File Storage On Cloud Using Cryptography," *SSRG International Journal of Computer Science and Engineering*, vol. 7, no. 5, pp. 12-15, 2020. Crossref, https://doi.org/10.14445/23488387/IJCSE-V7I5P104

[23] Guan Y, Shao J, Wei G and Xie M, “Data Security and Privacy in Fog Computing,” *IEEE Networks*, vol. 32, no. 5, pp. 106– 111, 2018. Crossref, https://doi.org/10.1109/MNET.2018.1700250

[24] Gudeme JR, Pasupuleti SK and Kandukuri R, “Attribute-Based Public Integrity Auditing for Shared Data with Efficient User Revocation in Cloud Storage,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 1-14, 2020. Crossref, https://doi.org/10.1007/s12652-020-02302-6

[25] Guo C, Jia J, Choo K-KR and Jie Y, “Privacy-Preserving Image Search (PPIS): Secure Classification and Searching using Convolutional Neural Network Over Large-Scale Encrypted Medical Images,” *Computers & Security*, vol. 99, pp. 102021, 2020. Crossref, https://doi.org/10.1016/j.cose.2020.102021

[26] Gupta S, Deep K and Mirjalili S, “An Efficient Equilibrium Optimizer with Mutation Strategy for Numerical Optimization,” *Applied Soft Computing,* vol. 96, pp. 106542, 2020. Crossref, https://doi.org/10.1016/j.asoc.2020.106542

[27] Maryann Thomas and S. V. Athawale, "Study of Cloud Computing Security Methods: Cryptography," *SSRG International Journal of Computer Science and Engineering*, vol. 6, no. 4, pp. 1-5, 2019. Crossref, https://doi.org/10.14445/23488387/IJCSE-V6I4P101

[28] Gadde, Swetha, Amutharaj J and Usha S, “Data Security on Cloud by Cryptographic Methods Using Machine Learning Techniques," *International Journal of Computer Science and Network Security*, vol. 22, no. 5, pp. 342-347, 2022.

[29] F. Maqsood, M. Ahmed, M. M. Ali, and M. A. Shah, "Cryptography: A Comparative Analysis for Modern Techniques," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, pp. 442–448, 2017. Crossref, https://doi.org/10.14569/IJACSA.2017.080659

[30] Swetha G and Janaki K, "Cloud-Based Secure Multimedia Medical Data Using Optimized Convolutional Neural Network and Cryptography Mechanism," *Multimedia Tools and Applications*, vol. 81, no. 23, pp. 33971–34007, 2022. Crossref, https://doi.org/10.1007/s11042-022-12466-2

[31] Gomathi N and Karlekar NP, “Ontology and Hybrid Optimization Based SVNN for Privacy Preserved Medical Data Classification in the Cloud,” *International Journal on Artificial Intelligence Tools,* vol. 28, no. 3, pp. 1950009, 2019. Crossref, https://doi.org/10.1142/S021821301950009X