

Data security in cloud environment using cryptographic mechanism

Abdul Azis Fairosebanu, Antony Cruz Nisha Jebaseeli

PG and Research Department of Computer Science, Government Arts and Science College, Affiliated to Bharathidasan University, Trichy, India

Article Info

Article history:

Received Aug 20, 2022

Revised Sep 5, 2022

Accepted Oct 11, 2022

Keywords:

Block cipher

Cryptography

Data security

Encryption

Symmetric cryptosystem

ABSTRACT

Virtual computing resources are provided via a cloud system that is both clever and intelligent. Based on the user's request, computing resources are made available. A hybrid cloud is the best option for storing and accessing user data for cloud deployments. Maintaining security in a hybrid cloud environment is time-consuming. This study provides a novel strategy for securing data in the hybrid cloud by ensuring the user's data is protected. Users' data in a hybrid cloud is protected using cryptographic approaches provided in this approach. Using this strategy, users' data may be protected in public and private clouds using various encryption methods. The suggested data security paradigm offers various advantages to both consumers and providers in terms of data security. Three symmetric encryption methods are offered as a service in the cloud. The concept is implemented as a cloud-based application hosted in the cloud, and the effectiveness of three strategies is assessed. They are evaluated in terms of performance and security. Using the recommended encryption methods in a hybrid cloud environment is more efficient than using other methods. The proposed technique can be used for relational data. It can be modified and enhanced to process multimedia data.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Abdul Azis Fairosebanu

PG and Research Department of Computer Science, Government Arts and Science College

Affiliated to Bharathidasan University

Palkalaiperur, Trichy, Tamil Nadu 620024, India

Email: rschlrfairose@outlook.com

1. INTRODUCTION

Cloud computing is a new technology that makes advanced computing more accessible to both consumers and service providers. Cloud computing is a kind of computing that allows customers to access infinite processing power. The cloud data centre provides computer resources. Many computers and servers are housed in a data centre facility, which is open 24 hours a day, seven days a week, to supply the necessary resources. Most small and medium-sized businesses rely heavily on the cloud for their operations. Software, platform, and infrastructure components make up the cloud resources.

Furthermore, infrastructure as a service (IaaS) serves as the principal platform for the delivery of cloud-based services. Amazon was the first to provide IaaS, but now companies like Google, Microsoft, and others may give support for it. Using the cloud ensures that the user can access the data they've provided whenever needed. The cloud provides the greatest level of security for data against physical damage. It's worth noting, though, that the cloud is more susceptible to data breaches when it comes to cloud-based data. The cloud's ability to prevent piracy is one example of this. Abuse and tapping [1] are all examples. Public and private, as well as hybrid cloud options, are available. Using a hybrid cloud for public and private data

storage is more efficient. A high-end cloud setup, a hybrid cloud [2] is just that. The national institute of standards and technologies (NIST) defines a hybrid cloud as one that "combines two kinds of clouds such public and private cloud technology consistent or exclusive computing allowing data and application mobility. Hybrid cloud adoption may be justified for a variety of reasons.

Although they may be motivated by the goal to create elasticity, virtualized resources, metered service, or load balancing management, probably, they are not. Hybrid cloud adoption is common due to its ease of use. It excels in data recovery and cloud service availability [3]. Because of this, businesses may store sensitive data in the private cloud and non-sensitive data in the public cloud, known as the hybrid cloud model. Utilizing both public and private clouds reduce the amount of money spent on data security. It is possible to significantly reduce costs while simultaneously boosting application accessibility using a hybrid cloud disaster recovery approach. As a result, hybrid cloud solution providers would be required to use this as a major phase. The hybrid cloud also has the advantages of quick service delivery, simple transfer from capital expenditure (CAPEX) to operating expenses (OPEX), reduced administrative load, group cooperation and global scope, low cost, and ease [4]. Hybrid cloud models are used by 55% of enterprises, according to the most recent research [5]. The private cloud model is used by 45% of businesses, whereas the public cloud model is used by 32% of businesses [6].

Data security is the cloud's darkest side for users who doubt its advantages of the cloud. The largest difficulty in the cloud is data security, and that challenge is only becoming worse with time [7]. Businesses and their customers suffer greatly if their data is stolen or corrupted. The most pressing worry in the cloud is data security [8], [9], cloud computing demands stronger and better data security design [9] since it is a massive computer network. To avoid a cryptographic data leak, a hierarchical management strategy that combines user passwords with secret sharing is presented [10]. For cloud data security, [11] established and implemented symmetric key encryption, which encrypts a file locally at the client-side before to uploading to the cloud and decrypts the file after downloading on the client-side using the key obtained during encryption. Using cryptography, you may ensure the safety of your data. The cloud environment, however, does not benefit from all cryptographic methods [12]. It is proposed in this study that two separate cryptographic encryption algorithms be used to safeguard hybrid cloud data instead of one single security solution. In order to address current security and privacy problems, such as data loss, data manipulation, and data theft, this study intends to provide a data security model based on cryptography and steganography for data in cloud computing [13]. The majority of researchers focused on cloud computing's security problems. Cryptography techniques [13] may generally be used to ensure data security. Data in the cloud is protected by various cryptographic services, including authentication, confidentiality, integrity, and so on [14]. According to a majority of the writers, classical cryptography encryption approaches were used to solve cloud data security challenges [15]–[17]. A novel cryptographic method has also been suggested by various writers in [18]–[21]. The problem is that in their proposal, most of them are merged with one or more current encryption schemes.

When two encryption methods are combined, the output is not as efficient as it may be. Both internal and external assaults compromise cloud data. The authors proposed mitigation measures [22], [23]. Cloud maintenance engineers at the cloud data centre [24] carry execute this assault, making it more difficult to monitor. Because the outside cloud users attempted to access the data without authorization, the external assault can readily be traced. Security measures for data storage have previously been proposed by researchers [25]–[29]. In order to secure the data in cloud storage against unwanted exposure, this study [30] suggests a secrecy mechanism as a security service algorithm (SSA), called MONcrypt. A novel genetic algorithm-based model (GA) CryptoGA is designed to address data integrity and privacy concerns [31]. There are certain restrictions in classic symmetric and asymmetric. To address this, a novel hybrid approach [32] is presented by combining elliptical curve cryptography (ECC) and blowfish that will ensure great data security and secrecy. Joshi *et al.* [33] discusses about how security affects cloud computing and all of the difficulties that come with it. In addition to detailing the research potential for using cryptographic approaches in cloud computing, this paper offers a review of a wide range of cryptographic schemes created for protecting sensitive data in the setting of cloud computing [34]. According to the literature, a security framework is predicted to be more effective in preventing data security breaches. Cloud users are not likely to be affected by this. When it comes to cloud security, there is much-interrelated work. This section sums up the work done by each researcher thus far. In addition to this effort, cloud-based assaults on data security remain increasingly common.

Because of this, data security stored in the cloud is critical. Cloud computing provides the opportunity to outsource IT services. Outsourcing data creates a slew of new cloud security issues. Data security is the key concern when it comes to cloud security. The cloud service providers are in charge of maintaining and controlling the data that has been outsourced. Third-party cloud service providers are not known to the user. Users can't find where their data is being kept and who is responsible for maintaining it. Cloud service providers prepare user data following their standards. Providers may have more options to learn about the data uploaded to the cloud. In the cloud, data security is offered in two ways: while the data is

in transit and when the data is at rest. Internal and external users may both assault data in transit and while it is stored on the network. Data security in a hybrid cloud environment is a top priority, but it's also time-consuming. The data is encrypted by the user and saved in the cloud to prevent these issues.

2. ALGORITHM

2.1. PUCSCipher

Data stored in the public cloud is the primary target of this symmetric encryption. The public cloud service cipher (PRCSCipher)'s execution process is outlined here. The logical flow of the PUCSCipher is represented in Figure 1.

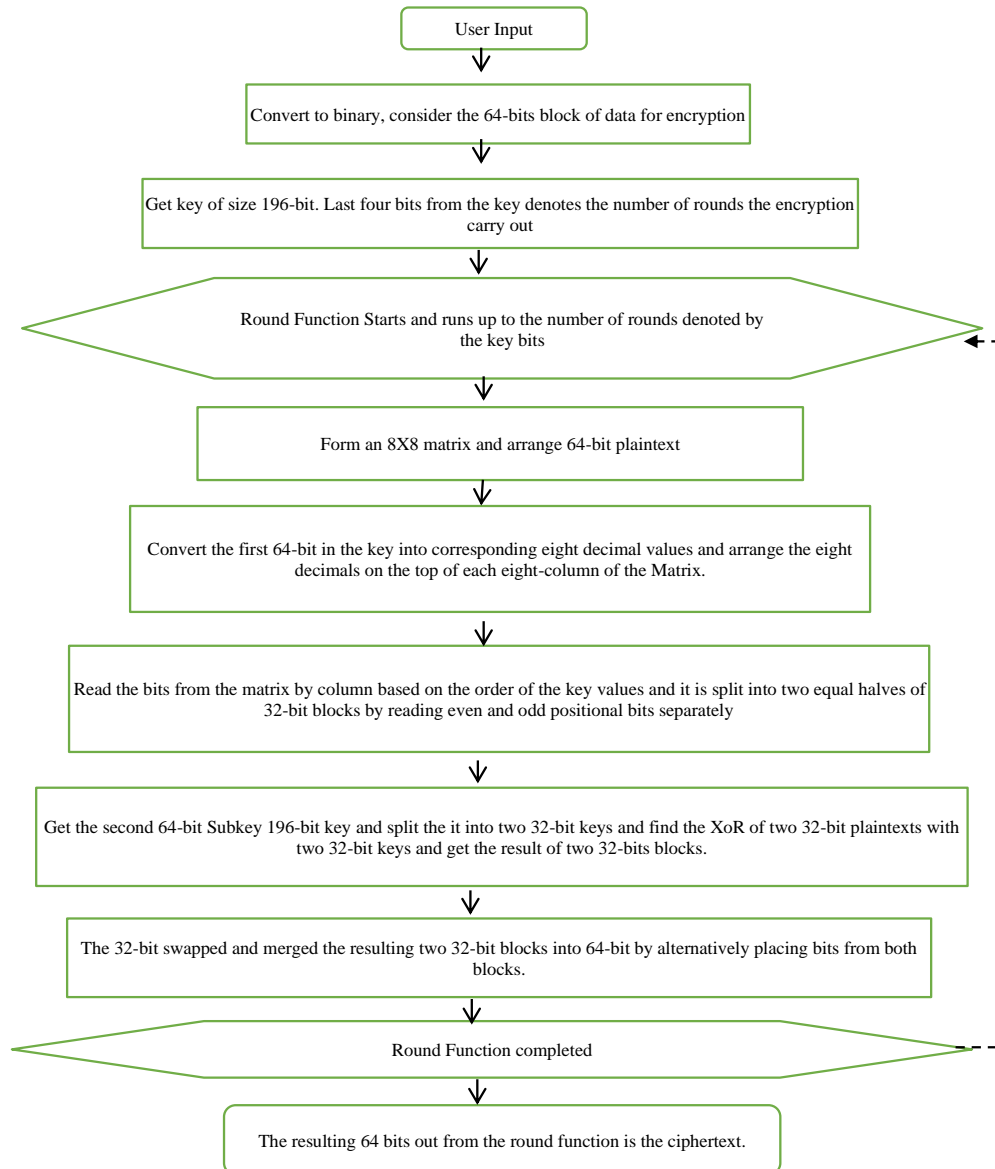


Figure 1. Logical flow of the PUCSCipher

Algorithm 1 PUCSCipher

1. Input Plain Text is used to collect data from users (PTEXT)
2. PTEXT's binary files are the next thing to look at.
3. Input PT is partitioned into 64-bit blocks in this step. 64-bit blocks are encrypted in PUCSCipher at a time.
4. The key for PUCSCipher may be obtained from KPMAaS in step 4.

5. The KEY's last four bits indicate the number of encryptions rounds to be performed.
6. This is the last step before we begin the round function. Create an 8x8 Matrix MAT using the PTEXT.
7. SKEY1 is the first 64-bit subkey of 196-bit key SKEY1 in step 7.
8. SKEY1 64-bit is converted into eight decimal values in step 8.
9. Place the eight decimal places at the top of each of the MAT's eight columns.
10. Using the ascending sequence of the eight decimal values at the top of each column, read the bits from the MAT one by one.
11. The 64-bit is divided into two equal 32-bit blocks by reading even and odd positions individually.
12. Get the second 64-bit subkey SKEY2 from the 196-bit KEY in step 12.
13. Split the SKEY2 into two 32-bit keys in step 13 of the tutorial.
14. Two 32-bit plaintexts and two 32-bit keys are used to find the XoR of each other.
15. The 32-bit swap is completed in step 15.
16. Alternately place bits from the two 32-bit blocks to merge them into a 64-bit block.
17. The round function has been performed in step 17. Depending on the number of encryption rounds, the steps from step 6 through step 15 are repeated numerous times. The first round's results are used as the starting point for the second round.
18. A 64-bit result is generated after all rounds. Subkey SKEY3 from key K is XoR with the third subkey SKEY3.
19. The ciphertext CTEXT is the 64-bit result from Step 17.

2.2. PRCS cipher

In order to protect the user's private cloud data, private cloud service cipher (PRCS cipher) uses symmetric block cypher encryption. In order to protect sensitive data, the author suggests Using PUCSCipher, the information is encrypted into a 64-bit block. Depending on the key, it will run for a certain amount of iterations. Variable pieces of input data result in a different number of rounds of encryption. The encrypting key length is 196 bits. Following is a description of the PRCS cipher's encryption process.

Algorithm 2 PRCS cipher

1. To begin, the information provided by users is entered into the system in plain text format (PTEXT)
2. The length of PTEXT binaries is determined in step two.
3. Convert PTEXT to ASCII decimal numbers and binary codes in step 3.
4. The KPMaaS generates a 128-bit Key KEY for you to enter.
5. The plain text binaries are broken down into 8-bit chunks in this step.
6. Get the first eight bits of the KEY in step 6. Each 8-bit bit is represented by one revolution in a subkey SKEY.
7. Using the key, rotate each of the 8-bits clockwise or anticlockwise. The SKEY is increased by one in each of the following eight bits.
8. In reverse order, read each of the 8-bit binaries.
9. Binaries are converted into decimal at this point.
10. The PTEXT decimal values are entered into a Matrix. Use PTEXT's length N to get the closest and largest square value.
11. Make sure that the square value you selected is a multiple of the square root.
12. In step 12, you'll create a matrix in which the rows and columns are all the same size.
13. The maximum matrix size is 25x25. If the PTEXT is longer than 625 characters, a new matrix is generated to hold the PTEXT's remaining characters.
14. Do Row Shifting following the matrix row number in Step 14. The first row, for example, moves once, the second row moves twice, and so on.
15. A total of three matrices are created: an upper matrix UMATRIX, an upper- and lower-level matrix LMATRIX, and a diagonal matrix DMATRIX
16. From the top down, invert the DMATRIX values from the left to the right, and from the bottom up.
17. Find the matrix transpose.
18. Reading from bottom to top and from left to right, begin with the even column and work your way up to the odd column, which is read from top to bottom from right to left.
19. Binaryize the matrix's decimal value.
20. To get the 128-bit KEY's XoR, go to Step 20 and use the binaries. Repeated KEYS are used throughout the binary's length.
21. The binary data is decoded into ASCII character code and numeric equivalents.
22. Cipher Text is the result of Step 21; thus, this is the next step. The logical flow of the PUCSCipher is represented in Figure 2.

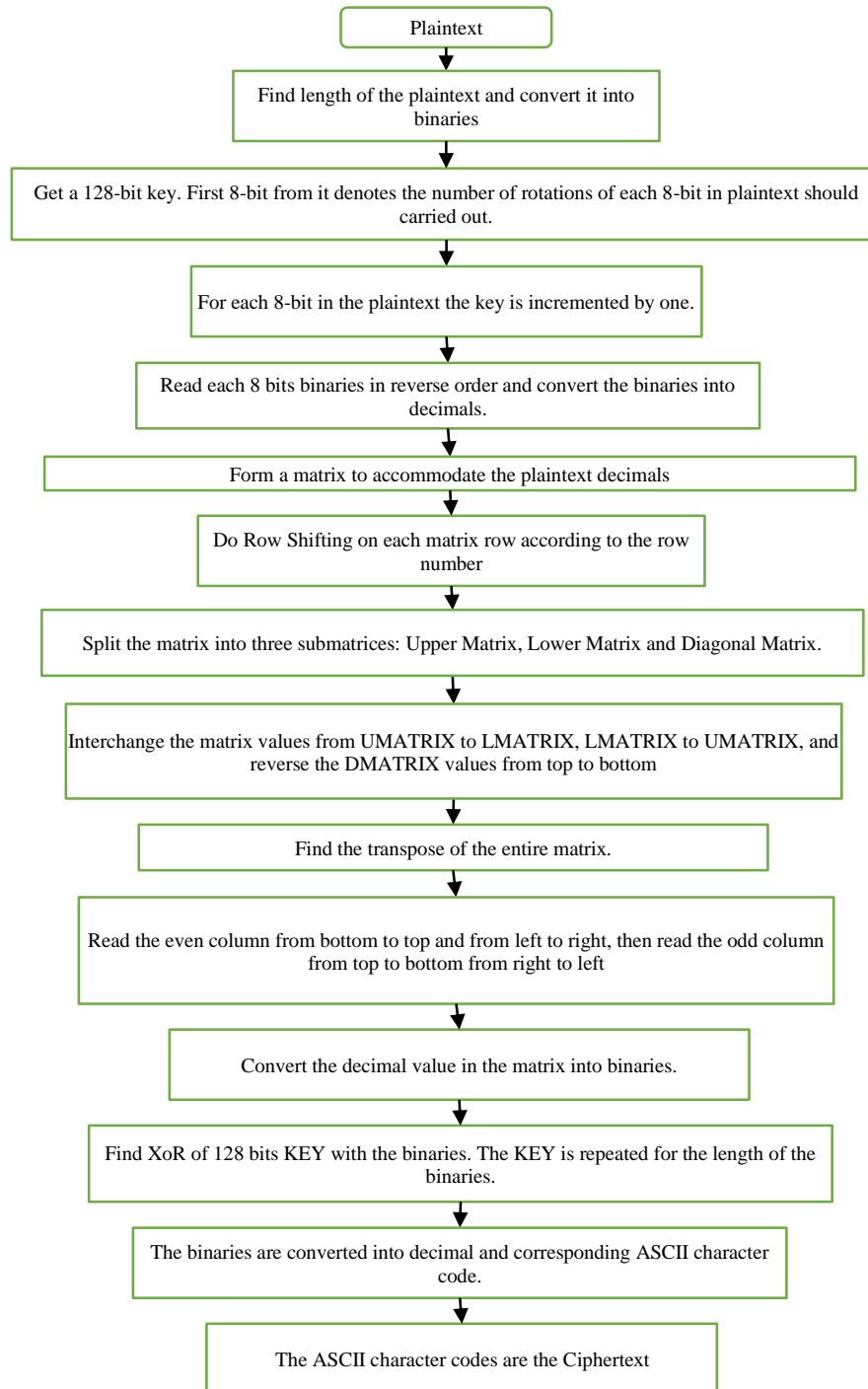


Figure 2. Logical flow of PRCS cipher

2.3. HYCSCipher

Users' data is encrypted before being sent to a public or private cloud, and the hybrid cloud service cipher (HYCSCipher) protects that data. In order to encrypt and decode data, the HYCScipher uses both of the preceding cyphers at the same time. The planned HYCSCipher's execution protocols are outlined below. The logical flow of the PUCSCipher is represented in Figure 3.

Algorithm 3 HYCSCipher

1. The public and private clouds are used to store user data.
2. Users must mention public and private cloud data.

3. Both PUCSCipher and PRCS cipher are enabled in HYCSCipher.
4. Public cloud data is encrypted using PUCSCipher, whereas private cloud data is encrypted using the PRCS cipher.
5. To produce the encrypted data, both methods are run simultaneously.
6. The user's computer transmits the encrypted data to the destination.

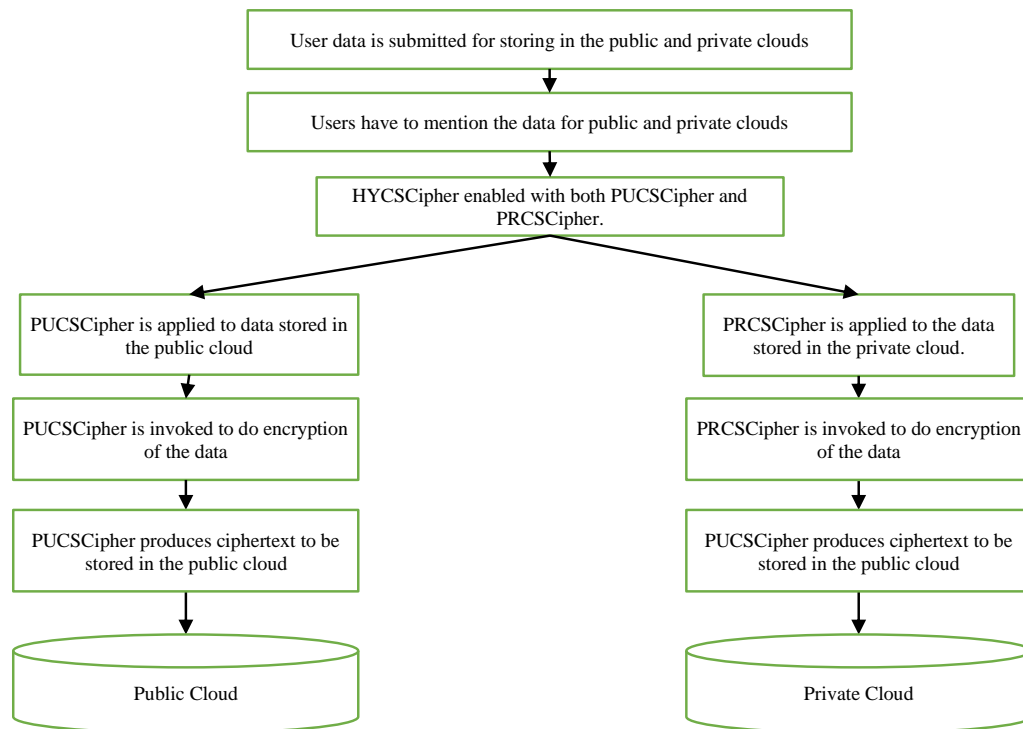


Figure 3. Logical flow of the HYCSCipher

3. METHOD

Cloud storage security is the primary focus of the suggested technique. It's possible to store the data in a hybrid cloud. The data are kept in a hybrid cloud depending on the user's preference. The data should be kept in a private or public cloud, depending on the user's preference. Users may choose the cloud type based on the sensitivity of the data. Encryption, keys, and storage would be kept in distinct parts of the cloud under the proposed system. Because the provider of all these services might know everything about the data kept in their storage if they are obtained from the same cloud provider. Using entities to protect data is seen in the suggested framework architecture in Figure 4.

The service providers don't know which encryption technique is used to encrypt the data, which key is used for encryption, and where the encrypted data is kept. 2. The data may be stored in public and private locations using two different encryption methods. Symmetric encryption protects data stored in both public and private clouds. The cloud-based key service provider is where you'll find the encryption key. Encryption may be done on-site or in the cloud, and the encrypted data is uploaded to the desired place. While concurrently uploading data to both the public and private cloud, the data is encrypted using the suggested encryption methods.

3.1. Techniques for encryption of data in hybrid cloud models

Cloud data storage may be made more secure by using the data encryption solutions that have been developed. Symmetrical encryption as a service (SEaaS) is a cloud-based service that provides symmetrical encryption. A data security model diagram for the hybrid cloud environment is shown in Figure 5. Symmetrical security encryption techniques are offered for both public and private and hybrid cloud settings in the SEaaS framework. Data may be protected via the use of cryptographic procedures. For cloud storage, a symmetrical cryptographic scheme is more suited.

Asymmetric encryption isn't a good idea when dealing with large amounts of cloud-based data. Various cloud and cloud services are part of the proposed architecture. SEaaS's security services are the primary

focus of our proposal. KPMAaS is a framework that also includes other kinds of services. These are cloud services from both public and private cloud providers. Creating and maintaining a key is not a burden on the user's shoulders. Rather, the user requests the key from SEaaS, which is generated by the KPMAaS service. That's why we're here: to learn all we can about SAAS. Encryption is requested from the SEaaS by users. The SEaaS complies with the user's request for encryption by implementing the desired encryption method.

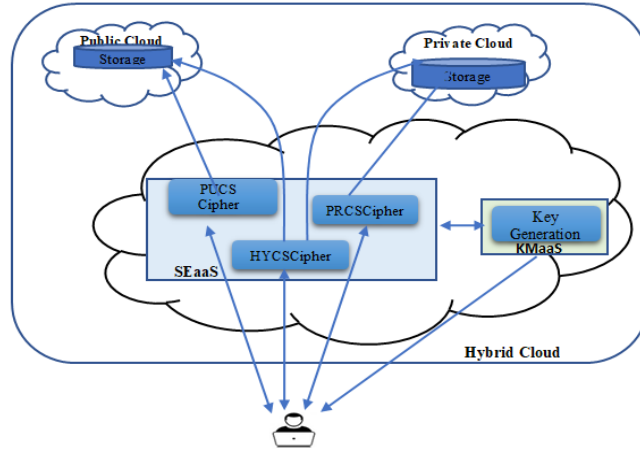


Figure 4. A conceptual framework and its constituent elements

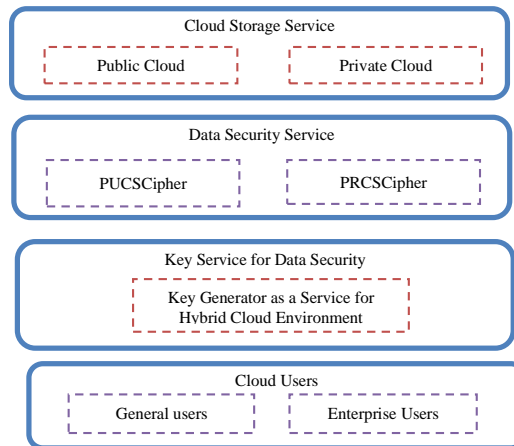


Figure 5. Proposed hybrid cloud data security model

To produce the key, SEaaS sends the user's information and the encryption method they want to KPMAaS. In contrast to the SEaaS, the KPMAaS produces the key and delivers it directly to the user. It's possible that SEaaS doesn't know the encryption key used. The KPMAaS is aware of the encryption key and mechanism but is unaware of where the cloud-based data resides. Encrypted data is uploaded to the cloud and decrypted by the user. Only the data storage provider can access it, and they don't know how the data was encrypted. With the framework in place, a single provider can't get access to sensitive data housed in a cloud storage facility. This study proposes a methodology for enhancing cloud data security. The frameworks make use of services that are decoupled from one another. To encrypt their data, users must follow the instructions provided. The procedures outlined below are aimed at ensuring the safety of sensitive data. Table 1 depicts the notations and descriptions used in this work.

Table 1. Notation and description

Acronym	Description
PUCSCipher	Cryptographic ciphers for public clouds
RCSCipher	Cipher for private cloud service
KPMAaS	Maintaining a key provider as a service
SE	Secure encryption methods

3.2. Workflow method for a hybrid cloud

The HYCSCipher encrypts the user's data forwarded to the public and private cloud. The HYCScipher invokes both previous ciphers for encryption and decryption simultaneously. The execution procedures of the proposed HYCSCipher are given as:

- The first step is to choose a cloud storage provider
- The SEaaS helps users learn about the various security options
- SEaaS responds to symmetrical encryption demands from users
- The SEaaS delivers the SE required by the user
- It is also possible to specify the SE to produce a key for using the SEaaS
- For users, the symmetric key is generated and sent straight to their cloud accounts through KPMAaS
- The KPMAaS does not share the keys it generates with SEaaS. The user was just redirected to their IP address
- Encryption is now an option for the users
- Encrypted data from a user's computer is sent to a cloud storage service

3.3. Symmetric encryption as a service

The SEaaS cloud service is a hybrid cloud designed to assure cloud data security. SEaaS is made up of three distinct security models to accommodate various kinds of cloud deployments. Public cloud encryption is available in PUCSCipher, private cloud encryption is available in PRCSipher, and the third is HYCSCipher for hybrid cloud encryption. This symmetric encryption method's implementation is described in subsection 3.4.

3.4. Implementation

The real-time cloud environment is used for the suggested study. Among the approaches studied are three. Using C#.Net programme coding, these strategies are turned into cloud-based software. Visual Studio 2012 is used to create the application. MyASP.Net, a cloud-based platform, hosts the built application. MyASP.Net is a platform for hosting user-created applications. MyASP.Net is used to implement and host all of the research. Provision has been made to upload plaintext using the created and hosted software application.

4. RESULTS AND DISCUSSION

The user may encrypt and decode data using three different forms of encryption. The programme tracks encryption and decryption times. The suggested methods are evaluated based on the time it takes to encrypt and decode the same amount of data. Existing equivalent security measures are used to evaluate the system's performance. As seen in Table 2, the three suggested and current encryption methods require different amounts of time to decrypt. It is also compared in terms of the decryption time. The application's efficient coding analyses the decryption time of the encrypted data. Decryption times for proposed and current algorithms are shown in Table 3.

Table 2. Compares the encryption times of several encryption algorithms

Size (KB)	DES	Blowfish	PUCS Cipher [35]	PRCS Cipher	HYCS Cipher
100	72	44	37	31	41
200	141	85	75	69	79
300	213	132	112	106	119
400	282	177	150	143	157
500	355	223	188	181	195

Table 3. Performance comparison by decryption time

Size (KB)	DES	Blowfish	PUCS cipher [35]	PRCS cipher	HYCS cipher
100	69	42	31	28	33
200	139	81	64	62	67
300	207	128	103	99	108
400	276	173	138	134	142
500	350	219	169	163	173

4.1. Analyzing security risks

In the Amazon cloud, EC2 leased server, the scrambled data is saved. Encrypted data is used to test the suggested approaches' security. Analyzing the safety of encryption methods is made possible by the ABC Hackman tool. The first step is to deploy the programme on Amazon's cloud servers. After that, the data is decrypted using the Hackman tool [30]. It then hacks the encrypted data and attempts to recover the original data.

For encryption approaches, the percentage of hacking by the Hackman tool is used to determine the level of security they provide. As shown in Table 4, the proposed and current approaches have different levels of security.

Table 4. Strength in security

Techniques	Security strength (%)
Blowfish	87
DES	81
PUCS Cipher	89
PRCS Cipher	91
HYCS Cipher	89

5. CONCLUSION

It is more difficult to maintain data security on the cloud. There is no limit to what can be done with this massive infrastructure when it comes to cloud computing. Virtual resources and services are created based on the needs of users. Users' willingness to utilise the cloud is being curtailed because of concerns about data security in the cloud. As a result of this paper, a hybrid cloud security paradigm has been suggested that is successful. The cloud service for encryption, key creation, and storage is isolated from the rest of the service. Three methods are included in the encryption service for storing data in the public, private, and hybrid clouds. Symmetric encryption is used in all of the described methods. Cloud computing is used to evaluate the effectiveness of the strategies. A hybrid cloud system is more efficient when data is stored using the described strategies.




REFERENCES

- [1] W. Wu, Q. Zhang, and Y. Wang, "Public cloud security protection research," in *2019 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, Sep. 2019, pp. 1–4, doi: 10.1109/icspcc46631.2019.8960734.
- [2] S. M. Barhate and M. P. Dhore, "Hybrid cloud: a cost optimised solution to cloud interoperability," *2020 International Conference on Innovative Trends in Information Technology (ICITIT)*, pp. 1-5, Feb. 2020, doi: 10.1109/icitit49094.2020.9071563.
- [3] B. Pushpa, "Hybrid data encryption algorithm for secure medical data transmission in cloud environment," *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)*, Mar. 2020, doi: 10.1109/iccmc48092.2020.iccmc-00062.
- [4] "Threat landscape for industrial automation systems in the second half of 2016," *Kaspersky ICS CERT*, Mar. 2017, [Online]. Available: <https://ics-cert.kaspersky.com/publications/threat-landscape-for-industrial-automation-systems-in-the-second-half-of-2016/>.
- [5] "Hybrid clouds deliver the best of both worlds," [Online]. Available: <https://webojects.cdw.com/webojects/media/pdf/CDWCA/white-paper-hybrid-cloud-model.pdf>.
- [6] R. Inc, "RightScale 2018 state of the cloud report uncovers cloud adoption trends," *GlobeNewswire News Room*, Feb. 13, 2018, [Online]. Available: <https://www.globenewswire.com/en/news-release/2018/02/13/1339982/0/en/RightScale-2018-State-of-the-Cloud-Report-Uncovers-Cloud-Adoption-Trends.html> (accessed Aug. 13, 2022).
- [7] J. Zhang, D. Sun, and D. Zhai, "A research on the indicator system of cloud computing security risk assessment," *2012 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering*, pp. 121–123, Jun. 2012, doi: 10.1109/icqr2mse.2012.6246200.
- [8] M. Colombo, R. Asal, Q. H. Hieu, F. A. El-Moussa, A. Sajjad, and T. Dimitrakos, "Data protection as a service in the multi-cloud environment," *2019 IEEE 12th International Conference on Cloud Computing*, pp. 81-85, Jul. 2019, doi: 10.1109/cloud.2019.00025.
- [9] E. Bacis, S. D. C. di Vimercati, S. Foresti, S. Paraboschi, M. Rosa, and P. Samarati, "Securing resources in decentralized cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 286–298, 2020, doi: 10.1109/tifs.2019.2916673.
- [10] H. Song, J. Li, and H. Li, "A cloud secure storage mechanism based on data dispersion and encryption," *IEEE Access*, vol. 9, pp. 63745–63751, 2021, doi: 10.1109/access.2021.3075340.
- [11] A. Musa and A. Mahmood, "Client-side cryptography based security for cloud computing system," *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*, pp. 594-600, Mar. 2021, doi: 10.1109/icaiss50930.2021.9395890.
- [12] M. Vashishtha and P. Chouksey, "A hybrid data security and identification mechanism in cloud computing," *International Journal Of Scientific and Technological Research*, vol. 8, no. 9, pp. 1565–1571, 2019.
- [13] R. Adeed and H. Mouratidis, "A dynamic four-step data security model for data in cloud computing based on cryptography and steganography," *Sensors*, vol. 22, no. 3, p. 1109, Feb. 2022, doi: 10.3390/s22031109.
- [14] R. Doshi and V. Kute, "A review paper on security concerns in cloud computing and proposed security models," *2020 International Conference on Emerging Trends in Information Technology and Engineering*, pp. 1-4, Feb. 2020, doi: 10.1109/ic-etite47903.2020.37.
- [15] A. V. Deorankar and K. T. Khobragade, "A review on various data sharing strategies for privacy of cloud storage," *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)*, pp. 98-101, 2020, doi: 10.1109/iccmc48092.2020.iccmc-00019.
- [16] A. Markandey, P. Dhamdhare, and Y. Gajmal, "Data access security in cloud computing: a review," *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*, pp. 633-636, Sep. 2018, doi: 10.1109/gucon.2018.8675033.
- [17] S. Singla and A. Bala, "A review: cryptography and steganography algorithm for cloud computing," *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, pp. 953-957, Apr. 2018, doi: 10.1109/icicct.2018.8473109.
- [18] P. D. S. K. Malarchelvi, S. S. Manikandasaran, and L. Arockiam, "MONCrypt: a technique to ensure the confidentiality of outsourced data in cloud storage," *International Journal of Information and Computer Security*, vol. 11, no. 1, p. 1, 2019, doi: 10.1504/ijics.2019.10014390.




- [19] T. A. Mohanaprakash and J. Andrews, "Novel privacy preserving system for cloud data security using signature hashing algorithm," *2019 International Conference on Security Technology (ICCST)*, pp. 1-6, 2019, doi: 10.1109/ccst.2019.8888420.
- [20] B. K. Das and R. Garg, "Security of cloud storage based on extended hill cipher and homomorphic encryption," *2019 International Conference on Communication and Electronics Systems (ICCES)*, pp. 515-520, Jul. 2019, doi: 10.1109/iccce45898.2019.9002549.
- [21] L. Arockiam and S. Monikandan, "Data security and privacy in cloud storage using hybrid symmetric encryption algorithm," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2, no. 8, pp. 3064-3070, Aug. 2013.
- [22] S. S. Manikandasaran, "Security attacks and cryptography solutions for data stored in public cloud storage," *International Journal of Computer Science and Information Technology & Security*, vol. 6, no. 1, pp. 498-503, 2016.
- [23] H. Abroshan, "A hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography algorithms," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 6, 2021, doi: 10.14569/ijacsa.2021.0120604.
- [24] R. Jahan, P. Suman, and D. K. Singh, "An algorithm to secure data for cloud storage," *Information Technology In Industry*, vol. 9, no. 1, pp. 1382-1387, Mar. 2021, doi: 10.17762/itii.v9i1.281.
- [25] F. M. Okikiola, A. M. Mustapha, A. F. Akinsola, and M. A. Sokunbi, "A new framework for detecting insider attacks in cloud-based E-health care system," *2020 International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS)*, pp. 1-6, Mar. 2020, doi: 10.1109/icmcecs47690.2020.240889.
- [26] V. Malgari, R. Dugyala, and A. Kumar, "A novel data security framework in distributed cloud computing," *2019 Fifth International Conference on Image Information Processing (ICIIP)*, pp. 373-378, 2019, doi: 10.1109/iciip47207.2019.8985941.
- [27] S. Wang, X. Wang, and Y. Zhang, "A secure cloud storage framework with access control based on blockchain," *IEEE Access*, vol. 7, pp. 112713-112725, 2019, doi: 10.1109/access.2019.2929205.
- [28] Y. Sharma, H. Gupta, and S. K. Khatri, "A security model for the enhancement of data privacy in cloud computing," *2019 Amity International Conference on Artificial Intelligence (AICAI)*, pp. 898-902, Feb. 2019, doi: 10.1109/aicai.2019.8701398.
- [29] A. K. Talukder and H. A. Prahald, "Security and scalability architecture for next generation internet services," in *2009 IEEE International Conference on Internet Multimedia Services Architecture and Applications (IMSAA)*, Dec. 2009, pp. 1-4, doi: 10.1109/imsaa.2009.5439441.
- [30] S. Monikandan and L. Arockiam, "Confidentiality technique to enhance security of data in public cloud storage using data obfuscation," *Indian Journal of Science and Technology*, vol. 8, no. 24, Sep. 2015, doi: 10.17485/ijst/2015/v8i24/80032.
- [31] M. Tahir, M. Sardaraz, Z. Mehmood, and S. Muhammad, "CryptoGA: a cryptosystem based on genetic algorithm for cloud data security," *Cluster Computing*, vol. 24, no. 2, pp. 739-752, Jul. 2020, doi: 10.1007/s10586-020-03157-4.
- [32] P. Chinnasamy, S. Padmavathi, R. Swathy, and S. Rakesh, "Efficient data security using hybrid cryptography on cloud computing," in *Lecture Notes in Networks and Systems*, Springer Singapore, 2020, pp. 537-547, doi: 10.1007/978-981-15-7345-3_46.
- [33] M. Joshi, S. Budhani, N. Tewari, and S. Prakash, "Analytical review of data security in cloud computing," *2021 2nd International Conference on Intelligent Engineering and Management (ICIEM)*, pp. 362-366, Apr. 2021, doi: 10.1109/iciem51511.2021.9445355.
- [34] L. Zhang, H. Xiong, Q. Huang, K.-K. R. Choo, and J. Li, "Cryptographic solutions for cloud storage: challenges and research opportunities," *IEEE Transactions on Services Computing*, vol. 15, no. 1, pp. 567-587, Jan. 2022, doi: 10.1109/tsc.2019.2937764.
- [35] A. Fairosebanu and A. N. Jebaseeli, "Enhanced symmetric encryption technique for securing users' data in public cloud environment," *IJCSNS International Journal of Computer Science and Network Security*, vol. 22, no. 4, pp. 785-791, Apr. 2022, doi: 10.22937/IJCSNS.2022.22.4.93.

BIOGRAPHIES OF AUTHORS



Abdul Azis Fairosebanu    received her M.Sc., (CS) degree in Government Arts College (Autonomous), Kumbakonam, India, in 2012. She also received her M.Phil. (CS) degree in the Jamal Mohammed College (Autonomous), Trichy, India, in 2013. Now she is employed as an Assistant Professor in PG & Research Department of Computer Science, Idhaya College for Women, Kumbakonam, India. In addition, she is pursuing a Ph.D (Computer Science) in Government Arts and Science College, Kumulur, Lalgudi, Trichy, India. She can be contacted at email: rschlrfairosebanu@outlook.com.



Dr Antony Cruz Nisha Jebaseeli    completed her Ph.D (Computer Science) at Bharathidasan University in 2014. Now she is employed as an Assistant Professor and Head, PG and Research, Department of Computer Science, Government Arts and Science College, Kumulur, Lalgudi. Now she is guiding 5 Ph.D scholars. She has completed her M.Sc in Bishop Heber College, Trichy, India and M. Tech in Bharathidasan University, Trichy, India. She has 18 years of experience in teaching and 5 years of experience in research. She can be contacted at email: drnishajeba@outlook.com.