JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 214-224
https://publishoa.com
ISSN: 1309-3452

A New Approach for Maintaining Data Security using Cryptography in a Hybrid Cloud Environment

Dr. Nisha Jebaseli[1], A. Fairose Banu[2*]

[1]Assistant Professor , P.G and Research Department of Computer Science ,Government Arts and Science College, Kumulur, Lalgudi, Affiliated to Bharathidasan University, Trichy

[2]Research Scholar, P.G and Research Department of Computer Science, Science ,Government Arts and Science College, Kumulur, Lalgudi, Affiliated to Bharathidasan University, Trichy

Abstract

A smart and intelligent cloud system virtually provides computing resources to enhance the user computing requirement. Computing resources are provided to the user based on their demand. A hybrid cloud is most effective for using and maintaining user data in the cloud deployment. However, no matter what kind of cloud technology the user adopts, it is open to security vulnerability. It's tedious to keep security in the hybrid cloud environment. Maintaining the user's data with a proper security mechanism, this paper proposes a new approach to maintaining data security in the hybrid cloud. The proposed approach uses cryptography techniques to secure the user's data in a hybrid cloud. The solid purpose of proposing this approach is to protect users' data in a public and private cloud using different encryption techniques. The proposed data security model provides users and suppliers with many benefits concerning the security of the data. Three encryption techniques are proposed and provided as Symmetric Encryption as a service from the cloud. Three techniques are measured for their efficiency by implementing the proposal as a cloud-based application hosted in the cloud. The proposed techniques are measured for performance and security strength. The results show that the proposed encryption techniques are more efficient for a hybrid cloud environment to secure data.

Key words- Cryptography, Encryption, Symmetric cryptosystem, Block cipher, Data security

I. INTRODUCTION

Cloud computing is a modern technology that makes sophisticated computing easier for users and providers. Cloud computing is a technology where users can compute for unlimited resources. The computing resources are delivered from the cloud data centre. The data centre is where many computers and servers are connected in a pool, and they are up and running 24X7 to provide the resources. The small and medium scale industries mainly use the cloud to leverage their business. The cloud resources are delivered in software, platform and infrastructure. More importantly, infrastructure as a Service (IaaS) is the primary provider of cloud-based services. Amazon is the first provider of IaaS, and now it can be serviced by Google, Microsoft and so on. The cloud provides reliably stored data, which means the data given to the cloud is returned whenever required to the user. Cloud provide maximum protection on data from damaging data physically. But, the most noted point about the cloud is that it is more vulnerable to data security issues on the data stored in the cloud. For example, does the cloud protect data against piracy? Abuse, tapping, and so on [1].

The cloud can be public and private or hybrid. A hybrid cloud is more efficient for maintaining the data in public and private. A hybrid cloud is a high-end cloud configuration type. The NIST (National Institute of Standards and Technology) describes that "a hybrid cloud combines two categories of clouds like public and private cloud technology consistent or exclusive computing enabling data and application portability. There are several reasons why companies can migrate to a hybrid cloud. Nevertheless, they are likely inspired by the desire to achieve one or more benefits: elasticity, virtualized resources, metered service and load balancing management. Most businesses adopt the hybrid cloud because of its user-friendliness. It provides

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 214-224
https://publishoa.com
ISSN: 1309-3452

a high degree of data recovery and high availability of cloud services[3]. Using the hybrid cloud model in the business, they can keep their sensitive data in the private cloud and store their general and insensitive data in the public cloud. The advantage of using both clouds in the business gives profit in spending costs on securing the data. The model of a disaster recovery system in the hybrid cloud helps the business save substantially while increasing the accessibility of their applications. This would make this a standard primary phase for companies that accept hybrid cloud solutions.
Along with the above-said benefits of hybrid cloud, it provides speedy delivery of services, easy migration from CAPEX to OPEX, reduces the admins' burden, provides group collaboration, and makes global scope, low cost and easiness [4]. The latest study denotes that [5] 55% of businesses use a hybrid cloud model for their business requirement. Furthermore, 45% of business deals are performed in the private cloud model and 32% of business deals that companies perform in the public cloud model[6]. The hybrid cloud model architecture is shown in Figure 1.

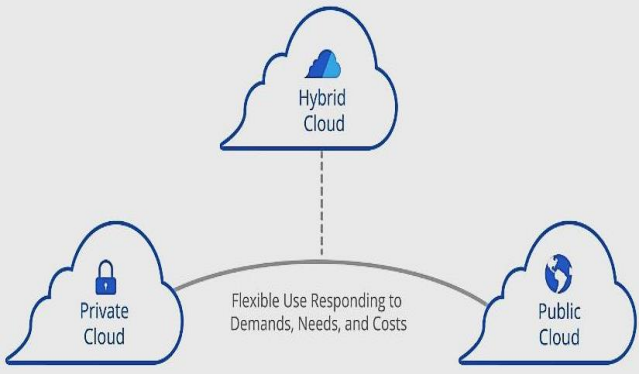


Figure 1 Architecture of Hybrid Cloud

User wonders about the benefits of the cloud, but the darkest part of the cloud is data security. Data security is the biggest challenge in the cloud, and it keeps on increasing day by day [7]. Data lost to businesses suffer a lot to leverage their business and general users. Keeping data safe is the most concern in the cloud [8]. The cloud infrastructure is a huge computer network, and it requires better and greater data security design[9]. Data security is given by cryptography techniques[10][11]. However, not all cryptography techniques are efficient in the cloud environment[12]. Instead of using a single security technique to secure the data in the hybrid cloud, this paper proposes a new approach to secure the hybrid cloud data using two different cryptography encryption techniques.

The rest of the paper is organized as follows. The next section discusses the related research work in the same data security field. Section 3 describes the problem considered in the paper. Section 4 discusses the methodology used in the proposed approach. Section 6 explains the proposed security model and its procedures. Section 7 describes the implementation setup and result of the discussion. Finally, section 8 concludes the paper.

II. RELATED WORKS

The related works are summarized in the section. Data security is an open research topic for researchers to provide the solution to secure the data. Most of the researchers tried to address the data security issues in the cloud. Generally, data security can be provided using cryptography techniques[13]. There are different cryptography services to secure the data in the cloud environment, such as Authentication, Confidentiality, integrity, etc. Most of the authors tried to implement the traditional cryptography encryption techniques to address the data security issues in the cloud [14], [15], [16], [17].

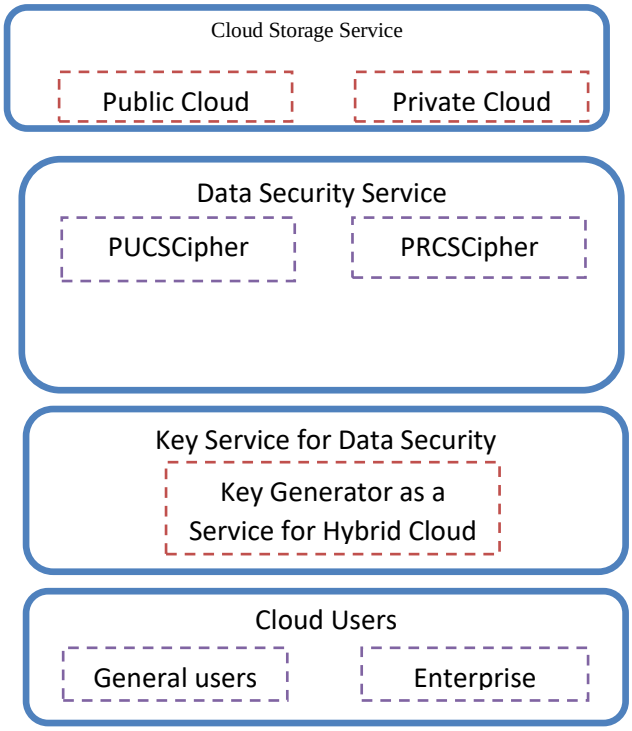
In addition, many authors in [18], [19], [20], [21] have proposed a new cryptographic algorithm to secure the data. But, in their proposal, most of them are integrated with any two existing encryption techniques. Simply, integrating two encryption techniques is not given an efficient result. The cloud data are hacked by two different internal and external attacks. The authors [22],[23] suggested attack mitigation techniques. The internal attack is more difficult to track because the authorized

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 214-224
https://publishoa.com
ISSN: 1309-3452

cloud maintenance engineers in the cloud data centre [24] carry out this attack. The external attack may easily be tracked because the outside cloud users tried to access the data without permission. Researchers already suggest some security approaches deal with data security in [25], [26], [27], [28], [29]. The literature suggested a security framework is expected to be more efficient in mitigating data security attacks. This is not expected to create more workload for cloud users. There is a great deal of related work in cloud security. This section summarizes the work already completed by the individual researchers. In addition to all this work, data security remains more susceptible to cloud-based attacks.

III. PROBLEM DEFINITION

The safety of data in the cloud becomes very important. Cloud offers outsourcing information technology. There are many cloud security challenges associated with data outsourcing. The main security problem in the cloud is data security. The outsourced data is maintained and controlled by the cloud providers. Cloud providers are third parties not known in person to



the user. Users don't know where and in which location or the address their data are stored and don't know who all the maintenance engineers look after the data. User data is formatted according to the styles of cloud providers. Providers may have greater opportunities to know about the data uploaded to the cloud. The data security in the cloud is provided to the data in two forms, the data is in transit, and the data is at rest, which means stored data. External users can attack the data when it travels through the network, and internal and external users can attack data at rest. Protecting data in the hybrid cloud is a critical and tedious task. To avoid these problems in the cloud, the data is encrypted by the user, and it is stored in the cloud.

IV. METHODOLOGY

Figure 2 Proposed framework with its entities

The proposed methodology mainly considers data security in cloud storage. The hybrid cloud model is used to store the data. The data are stored in a hybrid cloud based on the user's wish. Users should decide whether the data is stored in the public or private cloud. According to the sensitive nature of the data, users can select the cloud type. The proposed approach

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 214-224
https://publishoa.com
ISSN: 1309-3452

separates the cloud for encryption, key, and storage services. Because if all these services are received from the same cloud provider, then the provider can know everything about the data stored in their storage. By separating the service providers, they don't know which encryption method is used to encrypt the data, which key is used for encryption and where the encrypted data is stored. Two encryption techniques are proposed for storing the data in public and private separately. The encryption techniques used for securing the data stored in a public and private cloud are symmetric encryption. The key to encryption is to get from the key service provider from the cloud. Once the key is received from the cloud, the user can encrypt the data from their location, and the encrypted data is uploaded to the public or private cloud. When the user uploads the data to the public and private cloud simultaneously, the data are encrypted parallelly using the proposed two encryption techniques. Figure 2 shows the proposed framework design with entities used to secure the data.

V. DATA ENCRYPTION TECHNIQUES FOR HYBRID CLOUD MODEL

The data encryption techniques are proposed for securing the data stored in the cloud. The encryption approach is provided as a service from the cloud called Symmetrical Encryption as a Service (SEaaS). SEaaS comprises three symmetrical security encryption approaches; all three encryption approaches are proposed for public and private, and hybrid cloud environments. Cryptographic techniques are methods to secure the data. A symmetrical cryptographic system is more appropriate and efficient for storing data in the cloud. However, asymmetry is not recommended to encrypt a massive amount of cloud-based data. The proposed framework consists of various cloud and cloud services. Primarily, the scope of our proposal includes the security services provided by SEaaS. Other types of services are also included in the framework called KPMaaS. They are key-provider services and storage services from the public and private clouds. The user doesn't have the burden to generate and maintain the key. Instead, the KPMaaS generates the key requested by the user from SEaaS. SEaaS is the main focus of our research. Users request the SEaaS for encryption. The SEaaS provides the requested encryption approach to the user for doing encryption.

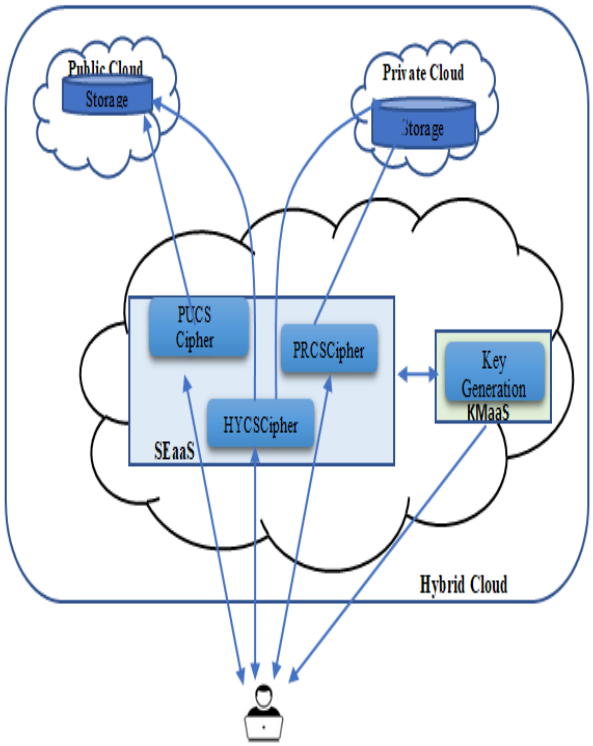


Figure3 Proposed Data Security Model for Hybrid Cloud

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 214-224
https://publishoa.com
ISSN: 1309-3452

Further, SEaaS also forwards the user's details and selected encryption approach to the KPMaaS to generate the key. KPMaaS generates the key and forwards it to the user directly, not by the SEaaS. So SEaaS doesn't know the key used for encryption. The KPMaaS knows the key and encryption method, but they don't know the location of the data stored in the cloud. The data is encrypted by the user and uploaded to the cloud. The storage provider can store the data; they don't know about the key and the encryption method used on the data for encryption. The framework efficiently separates the cloud service providers for each service, and it avoid the provider to know the details about the data stored in the cloud storage. Figure 3 depicts the hybrid cloud environment's proposed data security model diagram.

The framework proposed in this paper improves data security in the cloud. The services used in the frameworks are independent. The users have to follow the proposed procedure to get their data encrypted. The followings are proposed procedural steps designed for data security.

Table-I Notation and Description

Acronym	Description
PUCSCipher	Public Cloud Service Cipher
PRCSCipher	Private Cloud Service Cipher
HYCSCipher	Hybrid Cloud Service Cipher
KPMaaS	Key Provider Maintainence as a Service
SE	Symmetric Encryption

The proposed hybrid cloud workflow procedure:

1. First, Users have to decide which cloud storage they store their data.
2. Users contact the SEaaS for knowing the security approaches available.
3. Users generate requests matching symmetrical encryption from SEaaS.
4. The SEaaS provides the user with the requested SE.
5. The SEaaS also instruct the KPMaaS to generate the key for the selected SE.
6. According to the SEaaS, KPMaaS generates a symmetric key, and the key is directly forwarded to the cloud users.
7. The keys generated by the KPMaaS are not communicated to SEaaS. It only forwarded the user to their IP address.
8. The users now can able to encrypt the data.
9. The data encrypted from the user machine is uploaded to public or private cloud storage.

VI. SEAAS (SYMMETRIC ENCRYPTION AS A SERVICE)

The hybrid cloud with SEaaS cloud service is developed to ensure data security in the cloud. SEaaS comprises three security models for different cloud deployment models. There are three symmetric encryptions: PUCSCipher for public cloud, PRCSCipher for private cloud, and HYCSCipher for hybrid cloud. The execution of the proposed symmetric encryption is given below.

6.1 PUCSCipher(Public Cloud Service Cipher)

It is a symmetric encryption mainly developed to provide security to the data stored in the public cloud. The execution procedure of the PRCSCipher is given below.

Algorithm-1 PUCSCipher

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 214-224
https://publishoa.com
ISSN: 1309-3452

Step 1: Users' data are taken as Input Plain Text(P_{TEXT})
Step 2: Consider the binaries of P_{TEXT}
Step 3: Input PT is divided into 64 bits blocks. PUCSCipher encrypts 64-bit blocks at a time.
Step 4: Get a 196-bit key K_{EY} for PUCSCipher from KPMaaS.
Step 5: Last four bits in the key K_{EY} denote the number of rounds to be executed for encrypting the data.
Step 6: The round function starts. Form the P_{TEXT} into an 8_X8 Matrix M_{AT}.
Step 7: Get the first 64-bit subkey SK_{EY1} from the 196-bit key.
Step 8: Convert the SK_{EY1} 64-bit into corresponding eight decimal values.
Step 9: Arrange the eight decimals on the top of each eight-column of the M_{AT}.

Step 10: Read the bits from the M_{AT} by column based on the ascending order of the eight decimal values placed on the top of each column.
Step 11: The 64-bit is split into two equal half of 32-bit blocks by reading even and odd positional bits separately.
Step 12: Get the second 64-bit Subkey SK_{EY2} from 196-bit $K_{EY.}$
Step 13: Split the SK_{EY2} into two 32-bit keys.
Step 14: Find the XoR of two 32-bit plaintexts with two 32-bit keys and get the result of two 32-bits blocks.
Step 15: 32-bit swap is carried out.
Step 16: Merge the resulting two 32-bit blocks into 64-bit by alternatively placing bits from both blocks.
Step 17: The round function is completed. Steps from step 6 to step 15 are repeated in several rounds based on the encryption rounds. The result from the first round is given as the input to the next round.
Step 18: After all rounds, a 64-bit output is derived. It is XoR with the third subkey SK_{EY3} from the key K.
Step 19: The resulting 64 bits from Step 17 is the ciphertext C_{TEXT}.

6.2 PRCSCipher

PRCSCipher is a block cipher symmetric encryption method used to secure the user's data stored in the private cloud. The encryption procedure of the proposed PRCSCipher is given below.

Algorithm-2 PRCSCipher

Step 1: Users' data are taken as input Plain Text(P_{TEXT})
Step 2: Find the length of P_{TEXT} binaries.
Step 3: Convert the P_{TEXT} into corresponding ASCII decimal values and binaries.
Step 4: Generate 128 bits Key K_{EY} from the KPMaaS.
Step 5: The plain text binaries are split into 8 bits.
Step 6: Get the first eight bits from the K_{EY}. A subkey S_{KEY} denotes the number of rotations carried out for every 8 bits left to right.
Step 7: Rotate every 8-bits according to the key. The S_{KEY} is incremented by 1 for each next 8 bits.
Step 8: Read each 8 bits binaries in reverse order.
Step 9: Convert the binaries into decimal.
Step 10: A Matrix is formed for the P_{TEXT} decimal values. Calculate the nearest and greatest square value based on the length N of the P_{TEXT}.
Step 11: Find the square root value of the chosen square value.
Step 12: Form a matrix with rows and columns equal to square value.
Step 13: Maximum size of a matrix is 25x25. If the P_{TEXT} length is greater than 625, then a new matrix is formed for the remaining length of the P_{TEXT}.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 214-224
https://publishoa.com
ISSN: 1309-3452

Step 14: Do Row Shifting on each row of the matrix according to the row number. For Ex, the first row shifts one time, the second row shifts two times and so on.
Step 15: Split the matrix into three submatrices: Upper Matrix U_{MATRIX}, Lower Matrix L_{MATRIX} and Diagonal Matrix D_{MATRIX}.
Step 16: Interchange the matrix values from U_{MATRIX} to L_{MATRIX}, L_{MATRIX} to $U_{MATRIX,}$ and reverse the D_{MATRIX} values from top to bottom.
Step 17: Find the transpose of the entire matrix.
Step 18: Read the even column from bottom to top and from left to right, then read the odd column from top to bottom from right to left.
Step 19: Convert the decimal value in the matrix into binaries.
Step 20: Find XoR of 128 bits K_{EY} with the binaries. The K_{EY} is repeated for the length of the binaries.
Step 21: The binaries are converted into decimal and corresponding ASCII character code.
Step 22: The Result of Step 21 is the Cipher Text

6.3 HYCSCipher

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 below.

Algorithm-3 HYCSCipher

Step 1. User data is submitted for storing in the public and private clouds.
Step 2. Users have to mention the data for public and private clouds.
Step 3. HYCSCipher enabled with both PUCSCipher and PRCSCipher.
Step 4. PUCSCipher is applied to data stored in the public cloud, and PRCSCipher is applied to the data stored in the private cloud.
Step 5. Both procedures are executed in parallel to generate the encrypted data.
Step 6. The encrypted data are forwarded to the corresponding from the user's machine.

VII. IMPLEMENTATION

7.1 Experimental Setup

The proposed research work is implemented in the real-time cloud environment. The research work comprises three security techniques. All these techniques are implemented in C#.Net program coding and developed as a cloud-based application. The application is developed in Visual studio 2012. The developed application is hosted in the cloud-based platform as MyASP.Net. MyASP.Net is an environment to provides a platform to host the user's application. The entire research work is implemented and hosted in the MyASP.Net platform. The developed and hosted application is provisioned to upload the plaintext. The user can encrypt the data using three types of encryption and

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 214-224
https://publishoa.com
ISSN: 1309-3452

decrypt the data accordingly. The application is coded to find the time taken for encryption and decryption. The proposed techniques are measured for their performance efficiency according to the time taken for encrypting and decrypting the data. The performance is compared with existing similar security techniques. Table 1 shows the time taken for encryption by the three proposed and existing techniques.

Table-2 **Performance Comparison by Encryption Time**

Size	**DES**	**Blowfish**	**PUCSCipher**	**PRCSCipher**	**HYCSCipher**
100 KB	72	44	37	31	41
200 KB	141	85	75	69	79
300 KB	213	132	112	106	119
400 KB	282	177	150	143	157
500 KB	355	223	188	181	195

Similarly, the techniques are compared for the decryption time. The developed application is efficiently coded to analyze the decryption time taken to decrypt the data. Table 3 shows the decryption time comparison of proposed and existing techniques

Table 3. Performance Comparison by Decryption Time

Size	**DES**	**Blowfish**	**PUCSCipher**	**PRCSCipher**	**HYCSCipher**
100 KB	69	42	31	28	33
200 KB	139	81	64	62	67
300 KB	207	128	103	99	108
400 KB	276	173	138	134	142
500 KB	350	219	169	163	173

7.2 Security Analysis

The scrambled data is stored in the cloud server rented in the Amazon cloud EC2. The encrypted data is an analyst for the security strength of the proposed techniques. The ABC Hackman tool is used to analyze the security of the encryption techniques. First, the tool is installed on the Amazon cloud server. Next, the Hackman tool [30] gives the encrypted data to get the analysis report. Then, the tool hacks the encrypted data and tries to get the original data. Based on the percentage of hacking by the Hackman tool, the security strength is measured for the encryption techniques. Table 3 shows the security strength of the proposed and existing techniques.

Table 3. Security Strength

Techniques	**Security Strength (%)**

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 214-224
https://publishoa.com
ISSN: 1309-3452

Blowfish	87
DES	81
PUCSCipher	89
PRCSCipher	91
HYCSCipher	89

VIII. Conclusion

Cloud-based data security is a more complex task. Cloud is an enormous infrastructure that maintains virtually everything. User requirements provide virtual resources and services. Cloud-based data security vulnerability reduces the usage of the cloud among users. The data security model proposed in this article provides effective data protection in the hybrid cloud. The approach separates the cloud service for encryption, key generation and storage. The encryption service comprises three algorithms for storing public, private, and hybrid cloud data. All the proposed techniques are symmetrical encryption in nature. The efficiency of the techniques is measured by implementing the techniques in the cloud environment. The results are shown in the tables. The results show that the proposed techniques are more efficient for storing data in the hybrid cloud environment.

References

[1] Wei Wu, Qi Zhang, Yue Wang, "Public Cloud Security Protection, Research," IEEE International Conference on Signal Processing, Communications and Computing, (2019), pp. 1-4.

[2] S.M.Barhate, M.P.Dhore, "Hybrid Cloud: A Cost Optimised Solution To Cloud Interoperability," IEEE International Conference on Advanced Trends in Information Technology, 2020, pp. 1-5.

[3] B. Pushpa, "Hybrid Data Encryption Algorithm for Secure Medical Data Transmission in Cloud Environment," IEEE International Conference on Computing Methodologies and Communication, 2020, pp.329-334.

[5] Kaspersky Lab, "Threat Landscape for Industrial Computerization Systems in the Second Half of 2016," March 2017.

[4] "Hybrid Clouds Transport the Best of Both Worlds," https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/solutions/cloud/white-paper-hybrid-cloud-model.pdf, accessed on May 2020.

[6] Right Scale, "2018 State of the Cloud Report," 2018.

[7] C. Myeonggil, "The Security Risks of Cloud Computing," IEEE International Conference on Computational Science and Engineering (CSE), (2019), pp. 330-330.

[8] Maurizio Colombo, Rasool Asal, Quang Hieu, Fadi Ali El-Moussa, Ali Sajjad and Theo Dimitrakos, "Data Protection-as-a-Service in the Multi-cloud Environment," IEEE International Conference on Cloud Computing, (2019), pp.81-85.

[9] Enrico Bacis, Sabrina De Capitani di Vimercatiy, Sara Forestry, Stefano Paraboschi, Marco Rosa, Pierangela Samarati, "Securing Resources in Decentralized Cloud Storage," IEEE Transactions on Information Forensics and Security, Volume 15, (2019), pp. 286 – 298.

[10] H. Song, J. Li and H. Li, "A Cloud Secure Storage Mechanism Based on Data Dispersion and Encryption," in IEEE Access, vol. 9, 2021, pp. 63745-63751.

[11] Md. Abu Musa and Md. Ashiq Mahmood, Client-side Cryptography Based Security for Cloud Computing System, IEEE International Conference on Artificial Intelligence and Smart Systems, 2021, pp. 594-600.

[12] Megha Vashishtha, Dr Pradeep Chouksey, "A Hybrid Data Security And Identification Mechanism in Cloud Computing," International Journal Of Scientific and Technological Research, Volume 8, Issue 09, (2019), pp. 1565-1571.

[13] Adee, R.; Mouratidis, H. A, Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography, Sensors, 22, 1109, 2022, pp. 1-23.

[14] Riddhi Doshi, Vivek Kute, "A Review Paper on Security Concerns in Cloud Computing and Proposed Security Models," IEEE International Conference on Emerging Trends in Information Technology and Engineering, (2020), pp. 1-4

[15] A. V. Deorankar, Khushboo T. Khobragade, "A Review on Various Data Sharing Strategies for Privacy of Cloud Storage," IEEE International Conference on Computing Methodologies and Communication, (2020), pp. 98-101.

[16] Anagha Markandey, Prajakta Dhamdhere, Yogesh Gajmal, "Data Access Security in Cloud Computing: A Review," IEEE International Conference on Computing, Power and Communication Technologies, (2018), pp. 633-636.

[17] Surbhi Singla, Anju Bala, "A Review: Cryptography and Steganography Algorithm for Cloud Computing," IEEE International Conference on Inventive Communication and Computational Technologies, (2020), pp. 953-957.

[18] Manikandasaran, S. S., Lawrence Arockiam, and PD Sheba Kezia Malarchelvi. "MONcrypt- a Technique to Ensure the Confidentiality of Outsourced Data in Cloud Storage" International Journal of Information and Computer Security, Inder Science Journal, Volume 11, Issue 1, (2019), pp. 1-16.

[19] T. A. Mohanaprakash, Dr J. Andrews, "Novel Privacy-Preserving System for Cloud Data security using Signature Hashing Algorithm," IEEE International Carnahan Conference on Security Technology, (2019), pp. 1-6.

[20] Bablu Kumar Das, Ritu Garg, "Security of Cloud Storage based on Extended Hill Cipher and Homomorphic Encryption," IEEE International Conference on Communication and Electronics Systems, (2019), pp. 515-520.

[21] Arockiam, L., and S. Monikandan, "Data security and privacy in cloud storage using a hybrid symmetric encryption algorithm," IJARCCE, Volume 2, Issue 8, (2013), pp. 3064-3070.

[22] Manikandasaran, S. S. "Security Attacks and Cryptography Solutions for Data Stored in Public Cloud Storage", IJCSITS, 2016, pp. 498 -508.

[23] Hossein Abroshan, A Hybrid Encryption Solution to Improve Cloud Computing Security using Symmetric and Asymmetric Cryptography Algorithms, IJACSA, Vol. 12, No. 6, 2021, pp. 31-37.

[24] Roshan Jahan, Preetam Suman, Deepak Kumar Singh, An Algorithm To Secure Data For Cloud Storage, IT in Industry, Vol. 9, No.1, 2021, pp. 1382-1387.

[25] Folasade Mercy Okikiola, Abiodun Muyideen Mustapha, Adeniyi Foluso Akinsola, Michael Adio Sokunbi, "A New Framework for Detecting Insider Attacks in Cloud-Based E-Health Care System," IEEE International Conference in Mathematics, Computer Engineering and Computer Science, (2020), pp. 1-6.

[26] Vanaja Malgieri, Raman Dugyala, Ashwani Kumar, "A Novel Data Security Framework in Distributed Cloud Computing," IEEE International Conference on Image Information Processing, (2019), pp. 373-378.

[27] Shangping Wang, Xu Wang, and Yaling Zhang, "A Secure Cloud Storage Framework with Access Control based on Blockchain," IEEE Access, Volume 7, (2019), pp. 112713-112725.

[28] Yoshita Sharma, Himanshu Gupta, Sunil Kumar Khatri, "Security Model for the Enhancement of Data Privacy in Cloud Computing," IEEE International Conference on Artificial Intelligence, (2019), pp. 898-902.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 214-224
https://publishoa.com
ISSN: 1309-3452

[29] M. Repetto, A. Carrega, G. Lamanna, “An Architecture to Manage Security Services for Cloud Applications,” IEEE International Conference on Computing, Communications and Security, (2019), pp. 1-8.

[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(24),2015.pp.88-97.

[31] .http://www.huffingtonpost.com/young-entrepreneur-council/the-cloud-and-your-busine_b_13751184.html.