Cryptographic Hybrid Model-An advancement in Cloud Computing Security: A survey

Reena Saini[1]
Department of Computer Science & Engineering
BK Birla Institute of Engineering & Technology
Pilani, India

Nachiket Sainis[2]
Department of Computer Science & Engineering
BK Birla Institute of Engineering & Technology
Pilani, India

Abstract: **Cloud computing deals by providing computing and storage services via the internet on demand and pay per use access to the shared pool of configurable resources like networks, storage, servers, services and applications, without physically acquiring them. It enable computing resources as IT service which promotes various configurable resources in which the data is stored and managed with high efficiency and effectiveness in a decentralized manner. Information security is an essential topic in every area. In past few years, cloud computing security is the major issues in an organizations. However dealing with cloud, the data is out of the owner's control, concerns appear regarding data confidentiality. Security is the major concern when the sensitive information is stored (at rest) and transferred (in transit) across the internet. Cryptography ensures the confidentiality, authentication, availability, and integrity of the data. Information storage and transmission such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), RSA, MD5 and Blowfish.**

Keywords—Cloud security, Encryption, Hybrid Model, Cryptography

I. INTRODUCTION

Cloud computing is a model for providing on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be quickly supplied and released with minimal administration effort or service provider interaction.

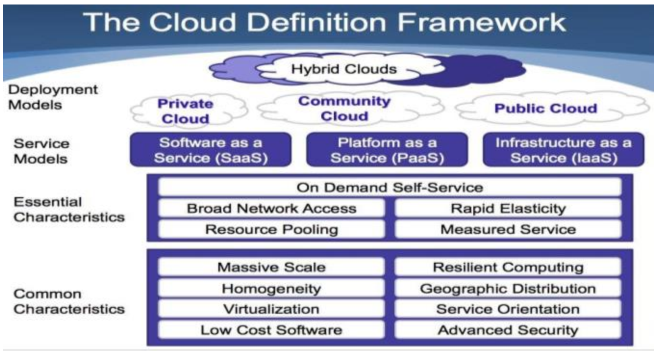

Fig 1. Cloud computing service models, deployment models, and Characteristics [3]

Cloud computing has five essential characteristics, according to the National Institute of Standards and Technology (NIST) definition: on-demand self-service, broad network access, resource pooling, quick elasticity or expansion, and measured service. As shown in Figure 1, cloud computing encompasses three service models and four deployment models, according to a NIST definition. The four "deployment models" (private cloud, community cloud, public cloud, and hybrid cloud) and three "service models" (software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS)) that together categorize ways to deliver cloud services [1].

Cloud computing is a distributed computing paradigm that focuses on providing a wide range of users with IT resources on a large scale by using existing technologies such as virtualization, service orientation, and grid computing [2].

Security and privacy are key concerns when using the cloud for data [4]. It is necessary for the cloud service to maintain data integrity, privacy, and security. Several service providers use various policies and mechanisms for this purpose, depending on the nature, type, and size of the data. Data may be shared among different businesses, which is one of the benefits of Cloud Computing. However, this benefit in itself poses a data security concern. Data repositories must be protected in order to avoid potential damage to the data.

When using the cloud to store data, one of the most important decisions to make is whether to employ a third-party cloud provider or build an internal organizational cloud. National security data or highly confidential future product details are sometimes too sensitive to be maintained on a public cloud. This type of data can be highly sensitive, and putting it to the public cloud can have catastrophic effects. In such instances, storing data in an internal organizational cloud is highly recommended. By imposing on-premises data usage policies, this strategy can help in data security. However, many organizations are not equipped to provide all layers of protection to sensitive data, therefore it still does not ensure complete data security and privacy [5].

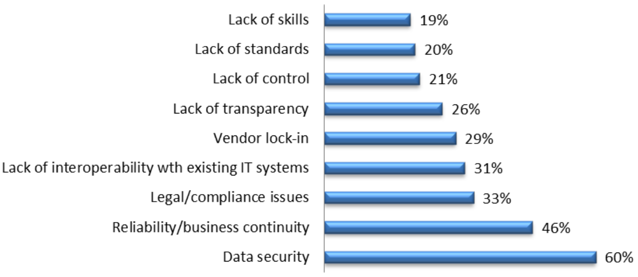

Fig 2. Significant concern with cloud computing

Confidential and critical information is stored across the cloud in the cloud context. Data loss and leakage are among the top security issues in the cloud, according to a recent survey by the Cloud Security Alliance. Recent laws, regulations, and compliance frameworks have increased the risks; offending firms may be held liable for the loss of sensitive data and face significant fines if data breaches occur. According to a survey conducted by Right Scale in 2018, security is a big concern in both enterprise and small and medium organizations.

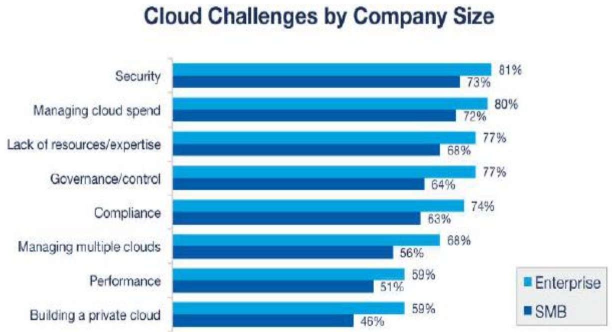

Fig 3. Cloud Right scale survey 2018

When all of these concerns about data security are taken into account, cloud computing becomes a major concern. Cryptography is a widely accepted method for assuring the security of information. This technique will encrypt the data by converting it to an unreadable format.

Cryptographic algorithms are divided into two categories. The symmetric key algorithm and the asymmetric key algorithm are the two types of algorithms. In a symmetric key cryptographic algorithm, one key, known as the private key, is used for both encryption and decryption of the data, whereas in an asymmetric key cryptographic algorithm, two keys, known as the private key and the public key, are used [6]. The information is encrypted using the public key, and the user information is decrypted using the private key. Asymmetric key cryptography is considered more secure than symmetric key cryptography since it uses two separate keys, which means that if one key is revealed, the encrypted data will not be harmed.

II. INFORMATION SECURITY

Information security is the term used to define the ability to secure a computer system against unauthorized access, use, disclosure, harassment, alteration, or destruction in order to maintain confidentiality, integrity, and availability [7]. The C.I.A Triad [8], which comprises of features of Confidentiality, Integrity, and Availability [9], is an important aspect of information security. Confidentiality (C) indicates that data and the information it represents must be protected in such a way that only authorized people can use it. Integrity (I) refers to the ability to safeguard users from unauthorized data modification. Guarantee that data will not be altered without authorization. Availability (A) refers to safeguarding users from unauthorized denial of service attacks.

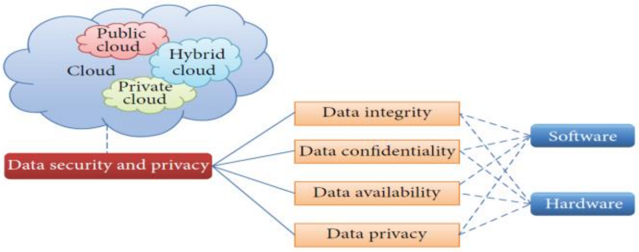

Fig 4. Information security aspect in cloud

A Security in Cloud Computing

Security and privacy issues in cloud computing have received a lot of attention in past few years [10]. The cloud divided into two categories: (1) cloud storage security and (2) cloud computation security. Cloud storage security refers to ensuring the integrity of data stored on cloud servers, whereas cloud computation security refers to ensuring the accuracy of cloud servers' computations [10].

B Data security in cloud computing

Data security in cloud computing encompasses more than just data encryption. As information is used, it frequently passes through multiple states, each with its own set of vulnerabilities. To keep your data safe at all times, you must understand the three states of digital data [11].

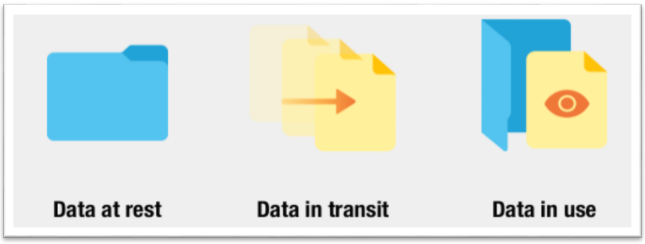

Fig 5. The three states of data

Data at Rest and Data in Transit are two types of data that can pose a security risk in the cloud. The nature of data protection mechanisms, procedures, and processes determines data confidentiality and integrity. The most important issue is the exposure of data in the two states mentioned.

- **Data at Rest:** Data at rest refers to data that is stored in the cloud or that may be accessed via the Internet. This includes both backup and live data. As previously stated, enterprises who do not maintain a private cloud may find it challenging to protect data at rest since they do not have physical control over the data. This problem can be resolved, by keeping a private cloud with strictly regulated access [5].

- **Data in Transit:** The term "data in transit" refers to data that is being moved in and out of the cloud. This data can be in the form of a cloud-based file or database that can be requested for use at a different location. When data is uploaded to the cloud, it is referred to as data in transit at the time of upload. Data in transit is intrinsically more risky than data at rest since it can move across the internet and around enterprise networks. It's also more likely to be exposed to third parties. [12].

- **Data in use:** Individuals can easily view or edit data that is in use because it is usually unencrypted. Once a file has been decrypted and opened, it is vulnerable to targeted attacks. Because of these factors, data is most susceptible when it is being used. Using identity management tools to detect anomalies in user behavior and verify that no one is attempting identity theft to gain access to company information [11].

III. PROTECTING DATA IN CLOUD USING CRYPTOGRAPHY

Cryptography is a method of data protection and communications by encoding it in a way that only the people who need to know can interpret and process it. As a result, unwanted access to information is prevented. The practise encompasses a variety of aspects of information security, including data confidentiality, integrity, and authentication (CIA) as well as non-repudiation, which are two of the most important features of modern cryptography [13].

Encryption in the cloud computing industry is a substantial problem that has been the subject of various research [14]. Jaber and Bin argue that an example of a significant focus area of encryption in cloud computing is identification based on encryption [15].

Encryption Algorithm for Cloud Security

Encryption algorithms are important in addressing the issue of cloud security. It's a mathematical method for converting plain text to cipher text. It utilises an algorithm to convert text into cipher text, which is meaningless text that requires a key to translate into understandable text.

In cryptography, encryption is used to provide data confidentiality, integrity, availability, and authentication. Encryption algorithms are divided into two types, symmetric and asymmetric [16].

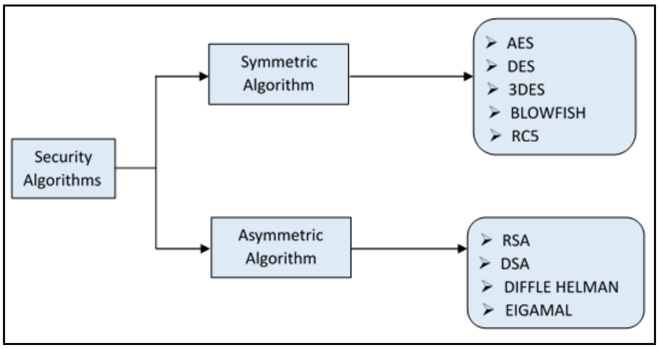

Fig 6. Security Algorithms

Symmetric Algorithms

In symmetric key encryption, only a single secret key is used to encrypt and decrypt data. It employs a secret key that can be a number, a word, or a string of random letters [17].

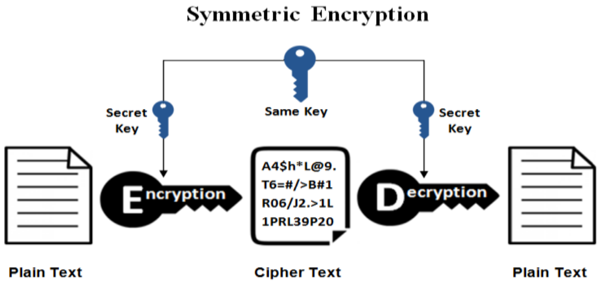

Fig 7. Symmetric Encryption

Block ciphers and stream ciphers are two separate methods of encrypting data with symmetric encryption algorithms:

Block Cipher: A block cipher divides plaintext messages into fixed-size blocks before converting them to cipher text with the help of a key, i.e. Encrypting data in chunks [17]. If the plaintext is longer than the block length, it is divided into many chunks for encryption.

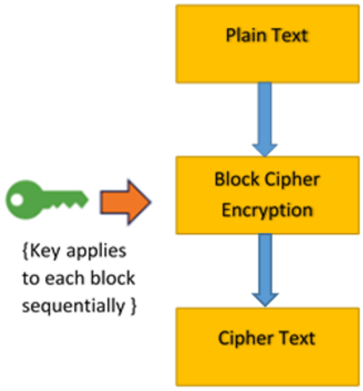

Fig 8. Block Cipher

Block Encryption Algorithm

- Data Encryption Standard (DES),
- Triple DES (3DES or TDEA),
- Advanced Encryption Standard (AES),
- International Data Encryption Algorithm (IDEA),
- Blowfish,
- Twofish,
- RC5

Stream Cipher: A stream cypher breaks down a plaintext message into single bits, which are subsequently converted into cipher text separately using key bits, i.e. encrypting data bit by bit [17]. Stream ciphers use long, pseudorandom streams to encrypt data. Generally, this procedure works one bit of data at a time.

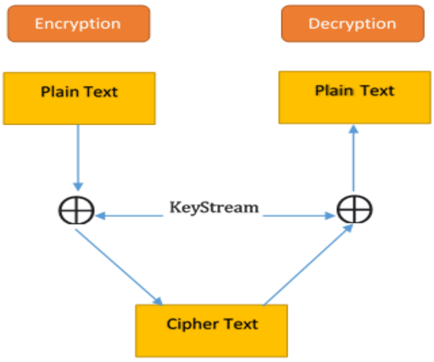

Fig 9. Stream Cipher

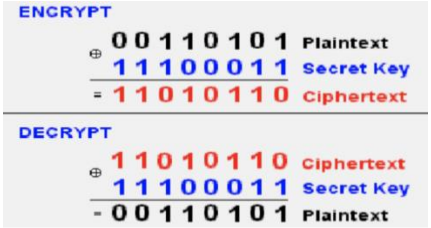
ENCRYPT
0 0 1 1 0 1 0 1 Plaintext
⊕ 1 1 1 0 0 0 1 1 Secret Key
= 1 1 0 1 0 1 1 0 Ciphertext
DECRYPT
1 1 0 1 0 1 1 0 Ciphertext
⊕ 1 1 1 0 0 0 1 1 Secret Key
= 0 0 1 1 0 1 0 1 Plaintext

Fig 10. Stream Cipher data process

Some Symmetric encryption algorithms are discussed here.

AES: (Advanced Encryption Standard) is a text encryption method that uses a symmetric block cipher. AES is a set of three algorithms that use a key size of 128, 192, or 256 bits to encrypt data. These algorithms are broken into a key schedule and an encryption algorithm [18]. The key size used by an AES cipher [20] specifies the number of transformation rounds that translate the input, known as plaintext, into the final output, known as ciphertext. It's divided into rounds, each of which consists of a collection of mathematical operations. The number of rounds used in the various AES variants differs the most: 10, 12, and 14. Each phase has several processing stages, one of which is based on the encryption key [20]. The key schedule differs between AES versions because they use various length secret keys and generate varying quantities of 128-bit round keys [19]. The ciphertext is then converted to plaintext by a number of reverse rounds.

DES: (Data Encryption Standard) is a block cypher that encrypts and decrypts using a shared secret key. Davis R. defines the DES cryptography technique. Get a fixed-length string by performing a series of complex operations on the bits of the encrypted text string [16]. The full block size in the case of DES is 64 bits. Because DES encrypts data with a 56-bit key, the decryption method can only be completed by someone who knows the key used to encrypt the data. The Feistel cipher, which consists of 16 Feistel rounds, is implemented using DES. The 48 bit round keys that apply to plain text are used in each round. Out of 56 cipher keys, these round keys generate sixteen 48 bit keys. It produces a 64-bit ciphertext as output.

3DES: The Triple Data encryption standard was created in 1998 as an advancement to DES. This 3DESEncryption technique is similar to the original DES, but it always employs three keys to increase the encryption level. The DES cypher is used in triplicate by encrypting with the first key (k1), decrypting with the second key (k2), and encrypting with the third key (k3). There also exist a two-key variant in which k1 and k3 are the same [21]. However, 3DES is a little slower than other block cypher methods. Because of its triple phase encryption, it takes more time than DES.

BLOWFISH: Blowfish is a 64-bit symmetric variable-length block cipher. Bruce Schneier designed it in 1993 as a "general-purpose algorithm." It is much faster than DES and has a higher encryption rate [22]. The survey found that the Blowfish algorithm outperformed other algorithms in terms of computation time. Blowfish has a 64-bit block size and accepts keys ranging in length from 32 to 448 bits. It is made up of 16 Feistel-like iterations, with each iteration operating on a 64-bit block divided into two 32-bit words. Blowfish encrypts and decrypts data with a single encryption key.

RC5: Ronald Rivest designed RC5 in 1994 as a symmetric block cypher that uses the same key for encryption and decryption. It is Hardware and software compatible. It only operates computational primitive operations found on standard microprocessors. It is notable for being simple, fast, and memory efficient. It works on two word blocks at once. Various instances of RC5 can be defined based on the input plain text block size, number of rounds, and key size, and each instance is denoted as RC5-w/r/b, where w=word size in bits, r=number of rounds, and b=key size in bytes. Choosing a larger number of rounds increases the level of security [23].

Asymmetric Algorithms

Two keys are used in Asymmetric Encryption. One key is public key which used for encryption and other key is private key which used for decryption. Some Asymmetric encryption algorithms are discussed here.

RSA: One of the most widely used encryption and decryption techniques is RSA (Rivest–Shamir–Adleman). RSA encryption is widely used in conjunction with other encryption techniques and digital signatures to verify the validity and legitimacy of a transmission [24]. It is not generally used to encrypt complete communications or data since it is less reliable and resource-intensive than symmetric-key encryption. As a result, engineers integrate RSA with other encryption algorithms to improve security and performance. This approach can only be used to decode the symmetric key by someone who has access to the RSA private key. Message decryption is nearly difficult without the symmetric key. As a result, combining two or more encryption and decryption methods is an elegant and conventional solution for improving security and efficiency [18]. The public key in RSA is made up of two numbers, one of which is the result of multiplying two large prime numbers. The same two prime numbers are also used to create the private key. So if the huge number can be factored, the private key is compromised. Encryption strength is entirely dependent on key size, and if key size is doubled or tripled, encryption strength increases exponentially. The length of an RSA key is usually 1024 or 2048 bits.

DSA: The DSA stands for Digital Signature Algorithm, which was created by the US government for digital signatures. The Digital Signature Algorithm was created specifically for signing, and as a result, it is well-known in the world of virtual signatures. A sequence of calculations based on a chosen prime number are used to execute the DSA signing process. Longer key sizes are now supported, despite the fact that the maximum key size was designed to be 1,024 bits. The process of creating a digital signature is faster than validating when DSA is used. When RSA is used, validating a digital signature takes less time than creating one. Similarly, DSA is faster to decrypt but slower to encrypt; on the other hand, RSA is the contrary [25].

Diffie-Hellman Key Agreement (D-H): It's a way of transferring cryptographic keys by creating a shared secret key that'll only be used for communication, not encryption or decryption. This key exchange procedure assures that neither party has previous knowledge of the creation of a shared secret key across a public channel [26, 27]. The key transformations are exchanged, and they both end up with the same session key, which appears to be a secret key. For public key cryptography, SSL, SSH, PGP, and other PKI systems, the Diffie – Hellman algorithm is utilised. Diffie–Hellman is used by many web services for secure communication and encryption [28].

El Gamal: El Gamal is a digital signature and key exchange transmission algorithm. Calculating logarithms is the foundation of the procedure. El Gamal's approach is based on the mathematical properties of logarithmic numbers. El

Gamal is the base for the Digital Signature Algorithm (DSA). El-Gamal is an asymmetric key algorithm for public key cryptography that is based on Diffie-Hellman key exchange. Taher El-Gamal described this algorithm in 1985. It consists of discrete logarithm problems as well as signature and encryption algorithms. The difference between El-Gamal and RSA algorithms is that RSA is based on the difficulty of determining factors of large integer, whereas El-Gamal is based on the difficulty of computing the discrete logs of a large prime modulus. Another feature of the El-Gamal cryptosystem is that each time the same message or plaintext is encrypted, a different cipher text is obtained [29, 30].

IV. LITERATURE SURVEY

In order to ensure strong security, the hybrid cryptography technique combines symmetric and asymmetric algorithms. Different encryption and decryption mechanisms are used by different cryptographic techniques. During the encryption process, the original data is converted into cypher data, which cannot be read. The ciphertext is turned into plaintext during the decryption process. The following are the various techniques and algorithms used to provide data security:

Adee1 et al,. 2022 [31] According to the author, the proposed artifacts can be classified as a four-step data security paradigm. In the first step, encryption algorithms are used to protect and secure data; in the second stage, steganography is used; in the third stage, data backup and recovery are performed; and in the fourth stage, data exchange is performed. The process begins with a sender and a receiver who wants to securely communicate files with one other. The sender generates an RSA key pair, consisting of a private and public key. The private key is subsequently distributed to the receiver using key management by a trustworthy third party. Following the key pair distribution, an AES key is generated. The plain text is then encrypted and decrypted using the AES key. The ciphertext and the AES key are then encrypted with the RSA public key to ensure security. The encrypted AES key is provided to the recipient along with the ciphertext, and the receiver decrypts the AES key and data using their private RSA key. As a result, the output is the plain text that was encrypted in the first place. The AES-256 keys are all encrypted in this method before data exchange, and cloud administrators can allocate access rights to users appropriately.

Bindu et al., 2018 [32] created hybrid cryptography algorithm for safe file storage in cloud environment using four symmetric encryption algorithms (AES, RC6, BLOWFISH, and BRA). The file is divided into 8 equal sections and encrypted using the preceding algorithms simultaneously with multithreading. The secret key was sent over email and is hidden inside the image using the LSB stegnography technique.

Batra et al., 2018 [33] designed a hybrid encryption for secure file storage in the cloud system that uses three separate symmetric encryption algorithms. Hybrid encryption technique use of all three encryption algorithms to make cloud storage more secure. The data is divided into three equal portions and encrypted using the following three algorithms: RC4, DES, and AES. Stegnography was used to share the key to the receiver.

L. Kumar and Badal, 2019 [34], analysed several hybrid cryptography models and recommended using AES and FHE to address security concerns such as data confidentiality, privacy, and integrity. Data Confidentiality, Authenticity, Integrity, Authorization, Freshness, and Non-repudiation are among the primary security challenges in the cloud, according to the authors.

Zhang et al., 2019 [35] used a hybrid security strategy to protect medical patient data in the cloud. P-AES, a modified version of the AES algorithm, is used in conjunction with RSA to give privacy and security to medical data stored in the cloud. Their hybrid solution can only be used to secure text and cannot be used to secure images or videos.

Viswanath & Krishna, 2020 [36] developed a Hybrid encryption framework consist of modules like Data slicing, encryption, distribution, uploading, indexing, retrieval, and merging. AES and Fiestel network block encryption and decryption are used in their hybrid framework. In a multi-cloud scenario, the sliced data is encrypted, indexed, and saved.

Pravin Soni et.al, (2021) [37] developed the hybrid security model for cloud computing in which the authentication module uses cryptographic techniques to ensure message integrity and non-repudiation that the data retrieved from the cloud is correct. To ensure the integrity of cloud data, the SHA256 and DSA algorithms are used. The AES and RSA hybrid technique is used to manage confidentiality in the cloud during data at transit and at rest.

Moshira A. Ebrahim et al. (2017) [38] established a cloud data security model that encrypts file data with AES-256, encrypts hash code and a new session key with RSA, and embeds the AES-256 and RSA outputs into an image using the advanced LSB method. The LSB algorithm is a data-hiding stegnography algorithm.

V. HYBRID CRYPTOGRAPHY MODEL COMPARATIVE ANALYSIS

Table I. Summary of Hybrid Security Model

References	*Algorithms used*	*Features Achieve*	*Applications*
31	AES, RSA	Data Integrity and Availability	Cloud Storage, Data backup and Recovery
32	AES, RC6, Blowfish and BRA	Data Integrity and confidentiality	Cloud storage
33	AES, DES and RC4	Data Integrity, confidentiality, authentication	Cloud storage
34	AES, TEA	Data Integrity, confidentiality, privacy	IoT data on cloud
35	P-AES, RSA	Confidentiality, privacy	Cloud database
36	AES and Feistal Network	Data Integrity, availability, confidentiality	Multi-cloud storage
37	SHA-256, DSA	Confidentiality, access control, authentication,	Cloud storage

38	SHA-256, RSA, AES	Data integrity	Cloud storage
39	MD5, Blowfish, EC	Data Integrity	Cloud Storage

In our analysis we have found that, AES is the popular symmetric key cryptography algorithm, which is frequently used encryption algorithm in cloud security.

VI. CONCLUSION

After reviewing all of the popular hybrid cryptographic models, we concluded that data security is the most important concern in cloud computing technology. Integration of symmetric and asymmetric cryptosystems is used to overcome security restrictions. We would attempt to secure sensitive data in the cloud by combining several encryption algorithms such as DES, 3DES, AES, Blowfish, RSA, RC4, MD5, and SHA. The study also suggests that hybrid cryptography improves performance and adds more security layers to data when compared to using these techniques separately.

VII. REFERENCES

[1] NIST. “Final Version of NIST Cloud Computing Definition Published | NIST.” *NIST*, www.nist.gov, 25 Oct.2011, https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published.

[2] Lewis, Grace. “SEI Digital Library.” *SEI Digital Library*, www.sei.cmu.edu, Sept. 2010, https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=28873.

[3] ESDS. “Cloud-Computing-Framework - ESDS Official Knowledgebase.” *ESDS Official Knowledgebase*, www.esds.co.in, 21 Dec. 2001, https://www.esds.co.in/kb/a-framework-for-cloud-computing/cloud-computing-framework/.

[4] Alharthi, Abdulrahman, Yahya, Fara, Walters, Robert John and Wills, Gary (2015) An overview of cloud services adoption challenges in higher education institutions. *Emerging Software as a Service and Analytics 2015 Workshop (ESaaSA 2015), in conjunction with CLOSER 2015. 19 - 21 May 2015.* pp. 102-109

[5] Albugmi, Ahmed, Nammas, Alassafi, Madini, Obad, Walters, Robert and Wills, Gary (2016) Data security in cloud computing. In *Future Generation Communication Technologies (FGCT), 2016 Fifth International Conference on : (FGCT 2016).* IEEE. pp. 55-59 . (doi:10.1109/FGCT.2016.7605062).

[6] A. Singh and M. Malhotra, "Hybrid two-tier framework for improved security in cloud environment," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), 2016, pp. 955-960.

[7] Force Transformation Initiative, Joint Task. “SP 800-30 Rev. 1, Guide for Conducting Risk Assessments | CSRC.” *SP 800-30 Rev. 1, Guide for Conducting Risk Assessments | CSRC*, csrc.nist.gov, 1 Sept. 2012, https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

[8] Perrin C. “The CIA Triad | TechRepublic.”, 30 June 2008, https://www.techrepublic.com/article/the-cia-triad/.

[9] Samonas Spyridon and David Coss. “The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security.” *Journal of Information System Security Volume 10, Number 3 (2014) Pages 21–45*.

[10] Lifei Wei, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, Weiwei Jia, Yunlu Chen, Athanasios V. Vasilakos, “*Security and Privacy for Storage and Computation in Cloud Computing” – ScienceDirect, Elsevier*. Vol. 258, 27 Apr. 2013, pp. 371–86, https://doi.org/http://dx.doi.org/10.1016/j.ins.2013.04.028.

[11] Waksman, Michael. “How to Protect All 3 States of Data: In Use, in Transit, and at Rest | Jetico.”, 26 Oct. 2021, https://www.jetico.com/blog/how-protect-all-3-states-data-use-transit-and-rest.

[12] F. Yahya, V. Chang, R. J. Walters and G. B. Wills, "Security Challenges in Cloud Storages," 2014 IEEE 6th International Conference on Cloud Computing Technology and Science, 2014, pp. 1051-1056, doi: 10.1109/CloudCom.2014.171.

[13] Pant, V.K.; Prakash, J.; Asthana, A. Three step data security model for cloud computing based on RSA and steganography. In Proceedings of the 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Greater Noida, India, 8–10 October 2015; pp. 490–494.

[14] Timothy, D.P.; Santra, A.K. A hybrid cryptography algorithm for cloud computing security. In Proceedings of the 2017 International Conference on Microelectronic Devices, Circuits and Systems (ICMDCS), Vellore, India, 10–12 August 2017; pp. 1–5.

[15] Jaber, A.N.; Zolkipli, M.F.B. Use of cryptography in cloud computing. In Proceedings of the 2013 IEEE International Conference on Control System, Computing and Engineering, Penang, Malaysia, 29 November–1 December 2013; pp. 179–184.

[16] JoonsangBaek, QuangHieu Vu, Joseph K. Liu and Yang Xiang"A secure cloud computing based framework for big data information management of smart grid," IEEE transactions on cloud computing 3.2, 233-244, 2015.

[17] “Symmetric vs. Asymmetric Encryption - What Are Differences?” *SSL2BUY*, www.ssl2buy.com, 14 June 2021, https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences.

[18] Pant, V.K.; Prakash, J.; Asthana, A. Three step data security model for cloud computing based on RSA and steganography. In Proceedings of the 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Greater Noida, India, 8–10 October 2015; pp. 490–494.

[19] Sandeep K. Sood, “A combined approach to ensure data security in cloud computing”, Journal of Network and Computer Applications, Volume 35, Issue 6, 2012, Pages 1831-1838, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2012.07.007.

[20] Chachapara, K.; Bhadlawala, S. Secure sharing with cryptography in cloud computing. In Proceedings of the 2013 Nirma University International Conference on Engineering (NUiCONE), Ahmedabad, India, 28–30 November 2013; pp. 28–30.

[21] Mehdi Sookhak, Abdullah Gani, Muhammad Khurram Khan, Rajkumar Buyya, “Dynamic remote data auditing for securing big data storage in cloud computing”, Information Sciences, Elsevier Volume 380, 2017, Pages 101-116, ISSN 0020-0255, https://doi.org/10.1016/j.ins.2015.09.004.

[22] KekeGai, MeikangQiu, Hui Zhao and JianXiong (2016) "Privacy-aware adaptive data encryption strategy of big data in cloud computing," Cyber Security and Cloud Computing (CSCloud), 2016 IEEE 3rd International Conference on. IEEE.

[23] Ronald L. Rivest (1994) “The RC5 Encryption Algorithm” International Workshop on Fast Software Encryption Springer

[24] Islam, S.M.J.; Chaudhury, Z.H.; Islam, S. (2019) A Simple and Secured Cryptography System of Cloud Computing. In Proceedings of the IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Edmonton, AB, Canada; pp. 1–3.

[25] Brintha Rajakumari S., Nalini C. (2014), An efficient data mining dataset preparation using aggregation in relational database, Indian Journal of Science and Technology, v-7, i-, pp-44-46

[26] Vincent P M D R and Sathiyamoorthy E (2014) A Secured and Time Efficient Electronic Business Framework based on Public Key Cryptography in International Review on Computers and Software 9(10) 1791-1798

[27] Koziel, Brian, et al. (2016) Neon-Sidh: efficient implementation of supersingular isogeny DiffieHellman key exchange protocol on ARM International Conference on Cryptology and Network Security Springer International Publishing

[28] Yao, Andrew C and Yunlei Zhao (2013) Method and structure for self-sealed joint proof-ofknowledge and diffie-hellman key-exchange protocols U.S. Patent No. 8,464,060

[29] Sonia Rani, and Harpreet Kaur. (2017) “Technical Review on Symmetric and Asymmetric Cryptography Algorithms” International Journal of Advanced Research in Computer Science 8 (4): 182-186.

[30] S. Sathish Kumar, S. R. Akshay Prabhu, R. Durga, and S. Jeevitha. (2016). “A survey on various asymmetric algorithms” International Research Journal of Advanced Engineering and Science 1(4): 117-119.

[31] Rose Adee1 and Haralambos Mouratidis (2022) “A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography” Sensors 1109. https://doi.org/10.3390/s22031109

[32] B. Bindu, L. Kamboj, and P. Luthra, (2018) “Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm,” Int. J. Adv. Res. Comput. Sci., vol. 9, no. 2, pp. 773–776, doi:10.26483/ijarcs.v9i2.5916.

[33] M. Batra, P. Dixit, L. Rawat, and R. Khalkar, (2018) “Secure File Storage In Cloud Computing Using Hybrid Encryption Algorithm,” International Journal Computer Eng. Appl., vol. XII, no. VI, pp. 30–36

[34] L. Kumar and N. Badal, (2019) “A Review on Hybrid Encryption in Cloud Computing,” 4th International Conference Internet Things Smart Innovation Usages, IoT-SIU, pp. 1–6, doi:10.1109/IoT-SIU.2019.8777503.

[35] F. Zhang, Y. Chen, W. Meng, and Q. Wu, (2019) “Hybrid Encryption Algorithms for Medical Data Storage Security in Cloud Database,” International Journal of Database Management System, vol. 11, no. 01, pp. 57–73, doi: 10.5121/ijdms.2019.11104.

[36] G. Viswanath and P. V. Krishna, (2020) “Hybrid encryption framework for securing big data storage in multi-cloud environment,” Evol. Intell., no. 0123456789,doi: 10.1007/s12065-020-00404-w.

[37] Pravin Soni, Rahul Malik (2021) “A Hybrid Cloud Security Model for Securing Data on Cloud” WCNC-2021: Workshop on Computer Networks & Communications, Chennai, India. pp. 118-125.

[38] M. A. Ebrahim, I. A. M. El-Maddah and H. K. Mohamed, "Hybrid model for cloud data security using steganography," 2017 12th International Conference on Computer Engineering and Systems (ICCES), 2017, pp. 135-140, doi: 10.1109/ICCES.2017.8275292.

[39] Hossein 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 pp. 31-37