International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/CSEIT228659

A Security Frame work for Data Storage in Cloud Computing by Using Cryptographic Approaches

Mangalampalli Sesha Sai Lakshmi Lavanya[1], T Virajitha[2], A Divya Reddy[3], B. Sree Saranya[4]

[1,2]Assistant Professor, CSE (DS) Department, CMR Engineering College, Hyderabad, India

[3]Assistant Professor, CSE Department, CMR Engineering College, Hyderabad, India

[4]Assistant professor, CSE(AI&ML), CMR Engineering College, Hyderabad, India

ARTICLEINFO

Article History:

Accepted: 01 July 2023

Published: 14 July 2023

Publication Issue

Volume 9, Issue 4

July-August-2023

Page Number

110-120

ABSTRACT

Cloud computing has revolutionized the way data is stored, processed, and accessed. However, with the widespread adoption of cloud services, ensuring the security and privacy of data has become a paramount concern. This paper presents a comprehensive security framework for data storage in cloud computing, leveraging cryptographic approaches. The proposed framework aims to protect data confidentiality, integrity, and availability throughout its lifecycle in the cloud. It explores various cryptographic techniques, including encryption, access control mechanisms, and key management protocols. Additionally, the paper discusses the challenges and considerations associated with implementing cryptographic security measures in cloud storage and provides recommendations for a robust and efficient security framework.

Keywords: Data security, Privacy, Integrity, Trust, Secure data storage, Cloud Computing, Cryptography, Hybrid model.

I. INTRODUCTION

For offering convenient, on-demand network access to pooled computer resources, cloud computing is regarded as the future or the next generation of computing paradigms. The technologies that have made cloud computing successful include virtualization, service-oriented computing, utility computing, load balancing, multi-tenant environments, and the ability to pay for computer resources on a per-use basis, which lowers significant upfront costs and administrative overhead [1]. Despite the fact that cloud computing has many advantages, data security, privacy, integrity, and trust are some of the main barriers to its widespread adoption [2]. Users of the cloud need to ensure that their sensitive data is protected from alteration or unauthorised access.

The cloud computing platform occasionally encounters internal and external security risks, as well as many outages and security risks to the cloud services. The alliance mentioned the incident of Mat Honan, a wired magazine journalist, who discovered in the summer of 2012 that someone had accessed his Gmail, Twitter, and Apple accounts and destroyed all of the baby images of his 18-month-old daughter [4]. In order to maintain the data integrity, privacy, and trust in the cloud environment, it is imperative to solve the data security challenges.[2].

To preserve the concerns connected to data privacy, integrity, and trust, a number of algorithms and protocols (including MD5, RSA, PDP, and PoR) have been developed in the past and are now being used[2. The goal of the study is to safeguard data against numerous risks to data security, including those posed by cloud environments, which raise concerns about data privacy, data integrity, and data trust. The document offers sensitive data encryption, which deters potential customers and businesses from using cloud computing services for their sensitive data.

The report will assist and encourage researchers to look into security solutions that will support a reliable cloud environment [4]. A methodology for data security is put out that will provide cloud users' data improved protection. More data security will result from multiple levels of data authentication. The employment of forensic virtual machines, real-time monitoring, and different encryption mechanisms will result in data security, privacy, integrity, and trust.

II. RELATED WORK

Cloud computing is the on-demand commercial distribution of computing resources through the internet, including database, storage, applications, computational power, and a limited number of IT resources. With the service provider's pay-as-you-go policy [5]. Because of the enormous volume of data being sent and the resulting danger of data assault, privacy and security are particularly crucial in cloud computing [6]. Because of these security worries, customers still have some difficulty trusting service providers to build secure cloud storage on top of public clouds [7]. Several high-level designs are merged with current non-standard cryptographic primitives to overcome this difficulty.

Cryptographic algorithms are created to function against computers and are straightforward, unadulterated, and pure maths. Cryptographic algorithms become more vulnerable as computers become smarter, which increases assaults for gaining access to a person's sensitive data. But when it comes to delivering information across an unreliable medium like the internet, these cryptographic techniques are essential [6]. A cryptography algorithm performs the following five main tasks:

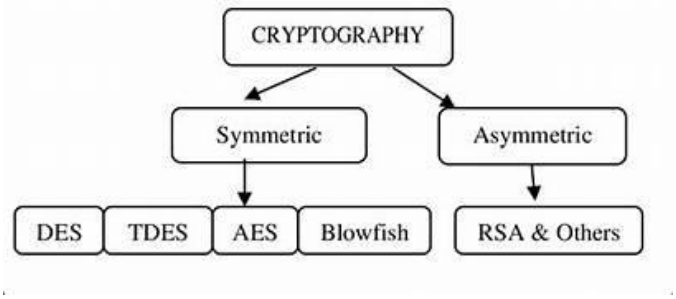

Fig 1. Types of cryptographic approaches.

Confidentiality: Data must be viewed by the intended, authorised recipient or user in order to prevent assaults in everyday life.

Authentication: In order to access the correct data, one must demonstrate their identity.

Integrity: The data that the receiver receives after it has been transmitted across an unreliable

medium must be accurate and unaltered from the original.

Non-repudiation: This feature stipulates that only authorised senders are allowed to convey information to the recipient.

Key-Exchange: This is the most vital operation since exchanging cryptographic keys is essential for both encrypting and decrypting data.

According to Fig. 1, there are two types of cryptography: classical and contemporary. Transposition and substitution cyphers are the two types of traditional cryptography.

Transposition cyphers: To encrypt data, a mathematical function that repositions the characters is employed. To decrypt data, the opposite mathematical function is used. Permutations of plaintext are frequently used in transposition cypher text.

Substitution cyphers: During encryption, each character or unit of data is swapped out for a different character or unit of data, and the opposite is done during decryption.

According to the keys used to encrypt and decode the data, modern cryptographic algorithms may be split into two categories [6]. Secret Key Cryptography: Symmetric Key Cryptography also goes by the name of Secret Key Cryptography. These cyphers employ a single key for both data encryption and decryption. The main purposes of these cyphers are secrecy and privacy. Block and stream cyphers can both be symmetric cyphers.

Public key encryption Asymmetric Key Cryptography is the term used to describe Public Key Cryptography. These cyphers employ two keys. Both encryption and decryption require different keys.

Key exchange, authentication, and non-repudiation are the main applications for these cyphers.

The process of putting into practise the two cryptographic methods that accept a key and change plain text into cypher text is known as the Crypto System. Basic elements of the cryptosystem include sensitive information that must be encrypted is in plain text, Cypher text is the disarmament of plain text created by the encryption process, while the decryption algorithm is the mathematical operations that reverse the encryption algorithm. Decryption Key is used as input to the decryption method using cypher text to recover the plain text after the encryption key has been used to generate the cypher text. Key space is the collection of decryption keys.

III.LITERATURE WORK

Certainly! Here are a few notable existing works on cloud security:

"Securing the Cloud: Cloud Computer Security Techniques and Tactics" by Vic (J.R.) Winkler. This book provides an overview of cloud security concepts, including threats, vulnerabilities, and best practices for securing cloud environments.

"Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance" by Tim Mather, Subra Kumaraswamy, and Shahed Latif. This publication explores cloud security and privacy issues from an enterprise perspective, covering risk management, compliance, and incident response.

"Cloud Computing Security: Foundations and Challenges" by John R. Vacca. This book presents an in-depth examination of cloud security foundations, technologies, risks, and challenges,

providing insights into securing cloud environments.

"A Survey of Security Issues in Cloud Computing" by Mariana Gerber and Isaac Woungang. This survey paper discusses the various security issues in cloud computing, including data security, privacy, access control, and virtual machine security.

"Cloud Security: A Comprehensive Guide to Secure Cloud Computing" edited by Ronald L. Krutz and Russell Dean Vines. This comprehensive guide covers various aspects of cloud security, including risk assessment, compliance, governance, and secure cloud deployment.

"Security Issues and Solutions in Cloud Computing" by Prof. B. B. Gupta, S. Mishra, and G. B. Singh. This research paper addresses security concerns in cloud computing and proposes solutions for data confidentiality, integrity, and availability.

"A Systematic Literature Review of Cloud Computing Security" by Kaoutar El-Maghraoui, Abderrahim Sekkaki, and Mohamed El Marraki. This systematic literature review examines recent research on cloud computing security, including threat modeling, authentication, encryption, and secure data storage.

"A Survey of Cloud Computing Security Issues and Solutions" by Meiko Jensen, Jorg Schwenk, Nils Gruschka, and Luigi Lo Iacono. This survey paper presents an overview of cloud computing security challenges, such as data protection, trust management, and secure virtualization.

A Hard Decisional Composite Residuosity Assumption scheme which is an enhanced function of the Pailler encryption algorithm was proposed by El Makkaoui et al. [9] to ensure the confidentiality of data on the cloud. Their proposed algorithm's execution time was high. Jain and Kumar proposed a homomorphic cryptographic scheme to boost customers' conviction regarding the confidentiality of data. Their system allowed for data updates even in the encrypted form without the need for a security key from the cloud service provider. Their system resulted in a high execution time.

The work of Zhang et al. [10] proposed the use of a cryptographic scheme using a pairing based algorithm based on blockchain that generates records that can resist tampering with records of patients to attain data privacy. Their system allowed all auditors on the system to verify the validity of the records but their contents were encapsulated. On the other hand, their approach failed to consider the security of e-health records under a cloud-assisted project and also depicted a high execution time in the data processing stages.

Zhang et al. [11] again proposed an attribute-based access control scheme that is decentralized to achieve data confidentiality on the cloud. Their scheme helped to ensure repudiation which allowed for the generation of a secret key without an idea from the users of the system. However, due to the non-uniqueness of the attribute key, unauthorized users can decipher plaintext which increased the execution time as a result of complicity, which has a serious effect on the security of data.

Huang et al in achieving the same objective as Zhang et al. [12] proposed the use of a Lagrange interpolation-based control system to achieve data confidentiality of patient records on the cloud. Their system achieved this through the use of an

authority-based scheme to access health records which increased the struggle in breaking the security of the database and accessing et health information. However, their approach had compatibility of systems and management of access problems as a result employed a lot of iteration which increased its execution time.

Rizwan et al. [13] proposed the use of Modular Encryption Standards (MES) integrated with the augmentation of condition-centric risk monitoring aiming to achieve confidentiality of health records. The confidentiality of data was attained by providing layered architecture of the health records. Making any decision regarding risk strategies of the MES is aided by a machine learning algorithm grounded using a Fuzzy Inference System integrated with Neural Networks. This system provides security against insider and outsider attacks by providing five variant keys for encryption. Their system however was not tested on other data types like image, audio, and video. Again there was proportionality between the data size and the execution time when textual data files were used.

Jain et al. [14] proposed the use of Secured Map Reduce to ensure the privacy of data on the cloud by introducing a layered interface between Hadoop Distributed File System as well as Map-Reduce Layer. Their architecture provided privacy, solved expansion concerns in privacy, and ensured data mining tradeoff based on privacy utility but the iteration of the processes influenced the execution time negatively.

Al-Balasmeh et al. [15] also ensured data privacy and information over vehicular cloud networks (VCNs) through the use of the data and location privacy (DLP) framework which secured the anonymity of personal data by providing location aided by obfuscation technique. In their work, much concentration was not given to securing loaded geo-fence storage infrastructure because it required many iterations to execute the process which has a negative influence on execution time.

These works provide a good starting point for understanding cloud security and the challenges associated with it. It's important to note that new research is continually being published in this rapidly evolving field, so staying updated with recent publications is crucial for a comprehensive understanding of cloud security.

IV. PROPOSED WORK

In order to prevent hackers from seeing or altering a person's personal data, secure data storage provides security across all layers of a storage system. Hybrid algorithms are used to safeguard data in the cloud to boost security. A hybrid algorithm combines at least two cryptographic algorithms. For secure data storage, one such hybrid strategy utilising the RSA and AES algorithms has been utilised in [7]. Here, the data is supplied to the RSA asymmetric algorithm, which encrypts the plain text using a public key, before the encrypted cypher text is passed to the AES method for a second layer of encryption.

The same keys are used for encryption and decryption when the user wants to access the data. The AES algorithm must first be used to decrypt the cypher text during the decryption process before the RSA algorithm is given the plain text. Utilising the AES technique takes time since

symmetric keys must be generated. Therefore, this framework does not provide the best answer. One Time Password, or OTP, is an alternative to the AES algorithm [8]. OTP is a contemporary technique that uses a randomly generated private key to encrypt data by executing an XOR operation [9]. The fact that OTP encrypts the data with random keys has the benefit of making the code impossible to crack theoretically.

If the data is 1024 bytes, the OTP method will produce a key that is 1024 bytes long, matching the length of the data that has to be encrypted. In this study, OTP with variants have been presented to address this drawback. This study examines the data on Drive HQ, a public cloud storage, and illustrates these variances. Here, a tiny key is repeatedly encrypted with the plain text using a small, randomly generated key. To explain, let's say we have 1024 bytes of data. A key of 16 bytes is produced at random, and the first 16 bytes are subjected to an XOR operation. The same key is then applied to the following 16 bytes, and so on until the plain text is completed. The procedure is described in more depth in the next section.

In this study, three hybrid models are proposed, and the temporal and spatial complexity of their implementations are compared. Every model adheres to the same flow of the hybrid method is used to encrypt the material, the encrypted text is then stored in a public cloud. DriveHQ has been chosen as the public cloud storage to test this work [10]. The cloud storage solution from DriveHQ boasts a tonne of top-notch features and is designed with corporations in mind. DriveHQ's Online Backup is incredibly simple to use when compared to other online backup programmes or services. Its primary use is cloud storage, whereby a free 1GB of space is made available upon initial login. Additionally, it provides a wide range of capabilities, including the DriveHQ file organiser, online backup, hosting for FTP servers, hosting for email and files, group accounts, web hosting, drive mapping, and more [11]. The following subsections provide an explanation of the hybrid models' implementation specifics.

Implementation of RSA and AES:

The first kind of hybrid model uses the AES and RSA algorithms together, as seen in Fig 2. This strategy has been thoroughly described in [7] and contrasted with the suggested strategy utilising OTP.

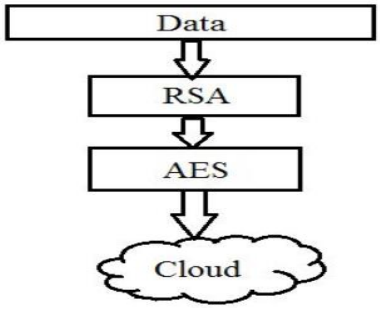

Fig 2. Fig 2: Working mechanism of models.

The RSA algorithm is given data in the model of Fig. 2. The public key RSA algorithm is used to encrypt data before transferring it to the AES method. AES encryption is carried out in rounds using various keys, after which the encrypted data is stored in the cloud. The same calculations are carried out in reverse when a user wishes to access data stored in the cloud. The RSA algorithm's overall time complexity for encryption and decryption is O (N3), while the time required to produce the key is O(N2) [12]. 10, 12, or 14 rounds of encryption are used by the AES algorithm [13]. The number of rounds depends on the key length;

for example, AES does 10 rounds of encryption for keys with a 128-bit length, 12 rounds for keys with a 192-bit length, and 14 rounds for keys with a 256-bit length. Time complexity therefore varies on input and key length [14].

Implementation of RSA and OTP

The second approach, as seen in Fig. 3, involves merging the RSA technique with OTP. This suggested course of action and the application of Fig 2 have been contrasted. In this paradigm, the RSA algorithm is initially given the data as shown in Fig 2. The OTP algorithm receives the RSA algorithm's final encrypted data as input. The OTP algorithm determines the length of the cypher text provided by the RSA method before generating the key of that same length. Following key creation, the OTP algorithm XORs the provided cypher text with the generated keys before storing the result in the cloud. The calculations are repeated in reverse order when the user requests access to the data. The RSA algorithm's overall time complexity for encryption and decryption is O(N3), and as was already noted, the time required to produce the key is O(N2). One Time Pad employs a straightforward XOR technique, hence its time complexity is O(N)ss [15].

Implementation of RSA and OTP with variations

The third strategy is to improve the strategy mentioned in Fig 3. The first two phases of this implementation are identical to those in the prior method. The OTP algorithm is employed in a variety of ways, as will be detailed below. Figure 4 depicts the approach's flow diagram.

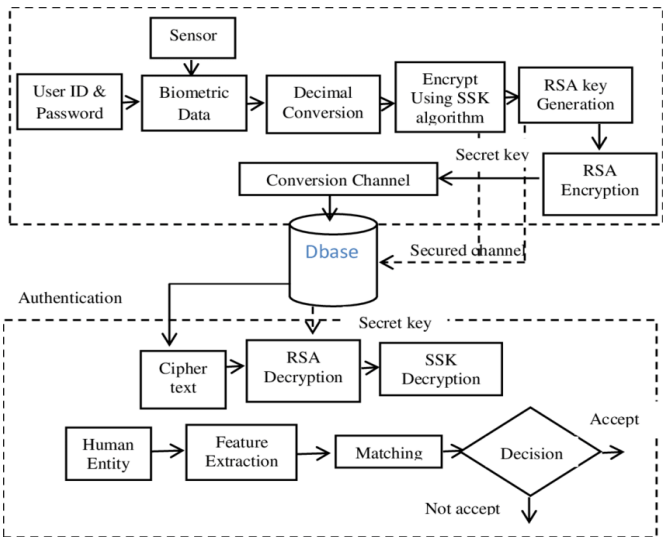

Fig 3.Work Flow of RSA and OTP hybrid model

Data is encrypted using a public key and the RSA method. The OTP algorithm receives the cypher text after encryption. The OTP method creates a tiny random key and then uses that same key to encrypt all of the data.

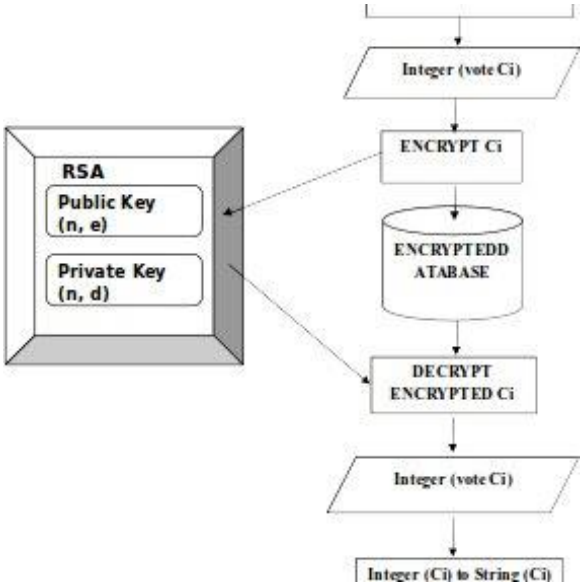

Fig 4. Work Flow of RSA and OTP with variations in hybrid model.

The same calculations are carried out in reverse order when a user requests access to the data. With the exception of how less time-consuming key creation is in OTP, the approach's overall time complexity is the same as that discussed in the previous section. Since the same key is used for

every continuous occurrence of the cypher text, an OTP method that uses O(N) for key generation instead uses OTP with variant described here, which uses only O(X), where X is the length of the key used for XOR operation.

V. CLOUD DATA SECURITY

Different methods were employed in conventional data security to process and safeguard sensitive data. Encryption was a widely used data security solution to protect outsourced data. It is not particularly cost-effective to download all the data and decrypt it locally because the procedure involves using a lot of bandwidth locally. When data is outsourced, the evidence of ownership that shields the user from exposure to his own data also poses a serious security risk. The remote service provider receives the data that has been outsourced, but the owner is unaware that the data is being stored there.

The catastrophe recovery issue is another difficult security issue. It depends on how the service provider handles the data in the event of a disaster, which may happen in the event that a remote hard drive fails owing to flaws in the cloud [2]. The old security procedures are not very effective since the amount of data that has to be kept is growing daily, reducing the effectiveness of the security mechanism. Critical and sensitive consumer data are handled by the supplier, although data integrity, privacy, and trust are not always guaranteed.

The main hazards to cloud computing, according to the paper's author [4], are misuse and criminal use of the technology, unsecured interfaces and APIs, malevolent insiders, problems with shared technology, data loss or leakage, account or service hijacking, and unclear risk profiles.

Data privacy: is one of the security challenges connected with cloud computing. As data grows every day, there are a number of security risks that arise. The complexity of risk assessment, the demands of a growing market for timely delivery of new business models and their implications for consumer privacy, various regulatory compliance, data privacy issues in design that result in poor data quality, and a lack of transparency are the privacy threats faced by cloud computing [13]. The Information Commissioner Office (ICO), which is in charge of applying norms and standards for accessing and using personal information in the cloud, conducts a Privacy Impact Assessment (PIA) for cloud users. Data processing methods have an impact on data privacy in the cloud, which is connected to data and software transfer protocols.

Data Integrity: Data validity as well as data dependability and consistency are both assured by data integrity. In the cloud environment, a key vulnerability is the lack of integrity; this leads to several security vulnerabilities and assaults. The user is given the assurance that the data won't be altered without their knowledge via data integrity.

When an outsider or anonymous person acquires access to the stored data, the data's integrity is put at jeopardy. Attacks on user data include attacks on data alteration, attacks on data leakage, and attacks on tags. In order to prevent data corruption and data crashes in the data centres, data integrity monitoring is crucial.

The architectural layout of cloud computing can occasionally cause an integrity problem. For example, cooperative provable data possession (CPDP), which combines a hash indexing hierarchy with homomorphic verifiable response, is one of the strategies used to avoid data integrity threats in the cloud context.

Data Trust: When two issues—a lack of transparency and a security or privacy breach—are not addressed effectively, trust, which is a big worry, is broken. Customers of cloud computing are drawn to the service's flexibility in resource utilisation, which encourages them to take use of it by putting their sensitive data at danger. Because they only rely on contracts and trust mechanisms, users are uninformed of the technology involved and who controls the data.

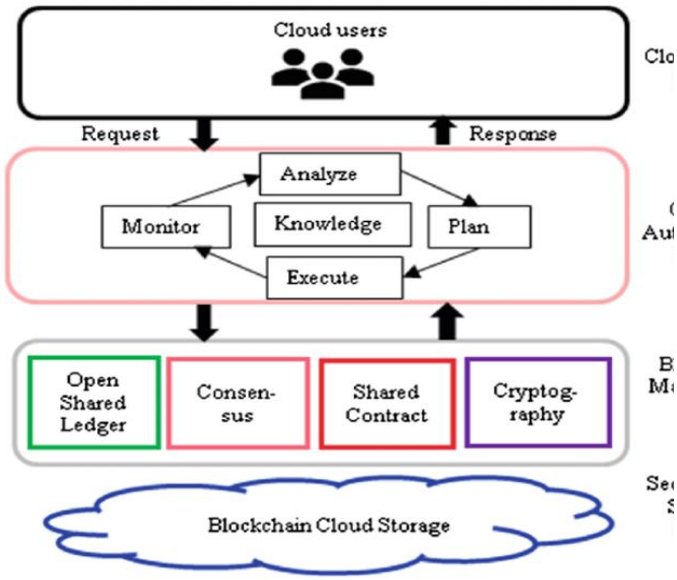

Fig 4. Data security framework in cloud environment.

Trust is a complicated concept that depends on another person's attitude or behaviour. The level of security provided by the cloud service provider to its clients is the foundation for trust. Building trust in the relationship between the cloud vendor and the cloud user also heavily relies on reputation. Additionally, trust-building practises must be spread across the whole service delivery chain [12]. If the cloud provider isolates the data while upholding integrity and privacy concerns in a multi tenant environment, trust can be improved. A degree of trust and understanding between the cloud provider and the user will be developed by being transparent while keeping data and disclosing any superfluous information to them.

VI. CONCLUSION

Three hybrid models have been applied on the sample text to determine which cloud storage technique performs better. The three techniques' time complexities have been examined, and it is possible to draw the conclusion that RSA and One Time Pad (with variation) are less difficult than the other two hybrid models. AES uses more storage since it creates a different key for the encryption process with each cycle. The One Time Pad approach uses a key that is the same length as plain text, therefore the difficulty of the storing relies on the size of the plain text selected. As it utilises the same key repeatedly and only requires a tiny key, the One Time Pad that has been presented with modifications has a lower spatial complexity. The conclusion drawn from the data is that the hybrid model based on RSA and One Time Pad (with variants) is efficient in terms of time and space complexity and the cypher text thus produced cannot be readily attacked.

Integrity and Trust are two benchmarks in data security and privacy that aid in the assessment of the secured system. The suggested approach is beneficial for creating a well-designed, highly secure data security system. The suggested

approach relates specifically to the data security across all three tiers of cloud services that the cloud provider makes available to cloud users. Cloud computing's prospective problem with data security presents new difficulties such data locks by cloud providers, fault tolerance, and disaster recovery systems.

VII. REFERENCES

[1]. A. Jaberi , M.F Data integrity and Privacy model in cloud computing, Biometrics and Security Technologies(ISBAST)2014, PP 280-284.

[2]. N. Jose and C. Kanmani, Data Security Model enhancement in Cloud Environment, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 10, Issue 2 , PP 01-06.

[3]. B. Goswami, and Dr..S.N. Singh, Enhance security in cloud computing using public key cryptography with matrices, International Journal of Engineering Research and Applications,vol.2,issu.4,pp.339-344,2012.

[4]. D W. Chadwick and K. Fatema, A privacy preserving authorization system for the cloud, Journal of Computer and System Sciences , 2012,PP 1359-1373.

[5]. C. Mont, and Pearson, An Adaptive Privacy Management System for Data Repositories, Trust, Privacy and Security in digital business,Volume 3592, 2005, pp 236-245.

[6]. Khan, S.M. and K.W. Hamlen., Anonymous Cloud: A Data Ownership Privacy Provider Framework in Cloud Computing. in Trust, Security andPrivacy, Computing and Communications (TrustCom), 2012 IEEE 11thInternational Conference on. 2012.

[7]. S. Subashini and V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, 2011. 34(1): p. 1-11.

[8]. C. Ning., et al. Privacy-preserving multi-keyword ranked search over encrypted cloud data, INFOCOM, 2011 Proceedings IEEE. 2011.

[9]. S. Pearson, Taking Account of Privacy when Designing CloudComputingServices," ICSE'09 workshop,Vancouver,canada,978-1-4244-3713-9-09,IEEE,Page no 44-52 (2009)

[10]. C.Saravanakumar and C.Arun, Survey on Interoperability, Security,Trust, Privacy Standardization of Cloud Computing, ContemporaryComputing and Informatics (IC3I), 2014, pp 997- 982.

[11]. Supriya, M., Sangeeta, K., & Patra, G. K. (2016). "A fuzzy based hierarchical trust framework to rate the cloud serviceproviders based on infrastructure facilities". International Journal of Performability Engineering, 12(1), 55-62.

[12]. Supriya, M., Sangeeta, K., & Patra, G. K. (2014). "Estimation of trust values for varying levels of trustworthiness based on infrastructure as a service". Paper presented at the ACM International Conference Proceeding Series, 10-11-October-201410.1145/2660859.2660921.

[13]. William Stallings. "Cryptography and Network Security Principles and, Pearson Education", Inc., publishing asprentice Hall.

[14]. Santhanalakshmi, S., Sangeeta, K., & Patra, G. K. (2017)."Design of secure cryptographic hash function using softcomputing techniques". International Journal of Advances in Soft Computing and its Applications, 9(2), 188-203.

[15]. Jonathan Katz & Yehuda Lindell (2015). "Introduction to Cryptography Modern". [7] Nasrin Khanezaei, Zurina Mohd Hanapi, (2014). "AFramework Based on RSA and AES Encryption Algorithms for Cloud Computing Services" in 2014 IEEE Conference on Systems, Process and Control (ICSPC 2014), 12 – 14 December 2014, Kuala Lumpur, Malaysia.

[16]. Hamza Ali Olwan ,Mohammed Khalifa Musa, (2017)."Hybrid Model Based on RSA Algorithm Combines with OneTime Pad Algorithm to

Improve Security and performance" in Imperial Journal of Interdisciplinary Research (IJIR) Vol-3, Issue-5, 2017 ISSN: 2454-1362.

[17]. Yun Huang , Zheng Huang , Haoran Zhao , Xuejia Lai, (2013). "A new One-time Password Method" in 2013 International Conference on Electronic Engineering and Computer Science..

[18]. AL.Jeeva, V.Palanisamy & K.Kanagaram, P.(2012). "Comparative Analysis of Performance Efficiency and security Measures of some Encryption Algorithm".

[19]. Chia-Long Wu; Chen-Hao Hu. (2012). "Computational Complexity Theoretical Analyses on Cryptographic Algorithms for Computer Security Application", 2012 Third International Conference on Innovations in Bio-Inspired Computing and Applications, Pages: 307 – 311.

Cite this article as :

Mangalampalli Sesha Sai Lakshmi Lavanya, T Virajitha, A Divya Reddy, B. Sree Saranya, "A Security Frame work for Data Storage in Cloud Computing by Using Cryptographic Approaches", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 4, pp.110-120, July-August-2023. Available at doi : https://doi.org/10.32628/CSEIT228659
Journal URL : https://ijsrcseit.com/CSEIT228659