Implementing Secure Data Storage and Sharing Techniques for advanced Protections in Cloud Environments

[1]Ms. Smita B. Zanke, [2]Prof. C. M. Mankar
[1]Student, Department of Computer Science and Engineering
[2] Assistant Professor, Department of Computer Science and Engineering,
[1] [2]Shri Sant Gajanan Maharaj College of Engineering, Shegaon.

Abstract:

Cloud computing has gained a lot of hype in the current world of I.T. Cloud computing is said to be the next big thing in the computer world after the internet. Cloud computing is the use of the Internet for the tasks performed on the computer and it is visualized as the next- generation architecture of IT Enterprise. The 'Cloud' represents the internet. Cloud computing is related to several technologies and the convergence of various technologies has emerged to be called cloud computing. In comparison to conventional ways Cloud Computing moves application software and databases to the large data centers, where the data and services will not be fully trustworthy. In this article, I focus on secure data storage in cloud; it is an important aspect of Quality of Service. To ensure the correctness of users' data in the cloud, I propose an effectual and adaptable scheme with salient qualities. This scheme achieves the data storage correctness, allow the authenticated user to access the data and data error localization, i.e., the identification of misbehaving servers.

Keywords: Computing, virtualization, grid, computations, applications

1. Introduction

The most popular advanced technology in use now is cloud computing. Being an Internet-based computer technology, cloud computing. The "CLOUD" has been deployed by some of the biggest companies, like Amazon, Microsoft, and Google, which have been employing it to accelerate their operations. The whole outsourcing industry (SaaS, PaaS, and IaaS) has taken on a new dimension thanks to cloud computing, which also offers ever-cheaper, more potent processors with various computing architectures. A computer's most basic function is to store information in the available space and retrieve it whenever the registered user requests it. Any type of data that we use every day may be stored, including basic pictures, our favourite tunes, saved movies, vast quantities of secret data, and even little amounts of data. The most fundamental service provided by cloud computing is the one just described.

Cloud is a pool of computing service on large scale. The increasing network bandwidth and reliable yet flexible network connections make it even possible that users can now subscribe high quality services from data and software that reside solely on remote data centers. The Cloud helps enterprises to have a dynamically scalable abstracted computing infrastructure that is available on-demand and on a pay-per-use basis. This model not only saves the IT teams from investing heavily on infrastructure, but also shields them from the intricacies involved in infrastructure setup and management. Presently, apart from providing the on-demand IT infrastructure, cloud service providers typically provide interfaces for other related IT management services. Cloud based flexible and on demand infrastructure enables a travel enterprise to offer mobility and social media channels without incurring any fixed cost. Using a cloud infrastructure, a travel enterprise can start in a small way and grow into these evolving markets with a lower risk and financial strain. From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons. At first, traditional cryptographic primitives for the purpose of data security protection can not be directly adopted due to the users' loss control of data under Cloud Computing. Therefore, we require verification of data storage in the cloud. Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of

verifying accuracy of data storage in the cloud becomes even more challenging. Secondly, Cloud Computing is not just a third party data warehouse.

The stored data in cloud may be frequently revised by the users, including operations like insertion, deletion, modification, affixing, reordering, etc. To ensure storage correctness under dynamic data revise is hence of paramount importance. However, this dynamic feature also makes traditional integrity insurance techniques futile and entails new solutions. The deployment of Cloud Computing is powered by data centers running in a simultaneous, cooperated and distributed manner. Individual user's data is redundantly stored in multiple physical locations to further reduce the data integrity threats.

Ensuring storage correctness without having users possessing data, cannot address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations. This is conquered using distributed protocols for ensuring storage correctness across multiple servers or peers. In this paper, we propose an effective and flexible scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud. We rely on erasure- correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability. This construction drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. By utilizing this token with distributed verification of erasure-coded data, our scheme achieves the storage correctness insurance as well as data error localization. Error Localization is the data corruption that has been detected during the storage correctness verification, our scheme can almost guarantee the simultaneous localization of data errors, i.e., the identification of the misbehaving server(s).

This is among first few ones in this field to consider distributed data storage in Cloud Computing. The main contribution can be recapitulated as the following aspects:

When compared to its predecessors they only provide binary results about the data storage status across the distributed servers, the protocol used in our work provides point of data error (i.e. Error Localization).

- We provide secure and efficient dynamic operations on data blocks.
- The security and performance analysis shows the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

In cloud data storage system, users store their data in the cloud and no longer possess the data locally. Thus, the correctness and availability of the data files being stored on the distributed cloud servers must be guaranteed. One of the key issues is to effectively detect any unauthorized data modification and corruption, possibly due to server compromise and/or random Byzantine failures. Besides, in the distributed case when such inconsistencies are successfully detected, to find which server the data error lies in is also of great significance, since it can be the first step to fast recover the storage errors. To address these problems, our main scheme for ensuring cloud data storage is presented in this section. The first part of the section is devoted to a review of basic tools from coding theory that are needed in our scheme for file distribution across cloud servers. Then, the homomorphic token is introduced. The token computation function we are considering belongs to a family of universal hash function, chosen to preserve the homomorphic properties, which can be perfectly integrated with the verification of erasure coded data.

2. Literature Survey

Mendonca S [1] stated that SaaS, PaaS, and IaaS are the three services that cloud computing offers to the customer. Different levels of security are offered in the cloud computing environment through these service models. Data security, data integrity, identity management, data location, data availability, and other factors need to be taken into consideration for better data security in cloud computing in order to have a secured cloud computing environment and to speed up cloud elements in SaaS service model.

- Data Security and Data Protection – Once the client uploads data to the cloud, there should be some assurance that access will only be permitted by those who have been given permission. Another risk that could potentially endanger cloud data is improper access to customer sensitive data by cloud staff.
- Data Integrity- Cloud service providers should put in place methods to assure data integrity and be able to explain what happened to a specific dataset and when. This is done by offering data security. It might be important to keep detailed records of the data that was stored in a public cloud. When such requirements for data integrity are present, it is necessary to retain the origin and custody of data or information in order to stop tampering with it or exposing it outside of the predetermined boundaries.
- Data localization and relocation are made possible via cloud computing. Consumers frequently have no idea where their data is located. An organisation may wish to know where their sensitive data is securely stored if it is kept on a cloud-based storage device. This calls for a contract between the cloud service provider and the client specifying the location or server where the data shall remain. on order to secure the data on the cloud, it is frequently moved from one location to another. SLAs (Service Level Agreements) are contracts between cloud service providers that allow them to share resources.
- Data Availability: Typically, customer data is stored in segments on various servers spread across various locations or on various clouds. As the availability of seamless and uninterruptible provision becomes more challenging in this situation, data availability becomes a serious problem. Therefore, it is crucial that the supplier give the authorised user proper access to the data.
- Identity Management – Each user must authenticate themselves in order to access cloud services. For the purpose of providing authentication and authorization, the provider should offer an identity management system. This is a significant concern in a cloud computing environment for both the provider and the user.[1]

Pan Yang [2] mentioned that as the Internet of Things (IoT) gains popularity, more information-sensing gadgets are becoming online in order to realise how interconnected people, gadgets, and "things" are. According to a recent forecast from IDC, there will be 41.6 billion internet of things (IoT) "things" in 2025, producing 79.4 zettabytes (ZB) of data. Additionally, people are still dedicated to enhancing the effectiveness of data collecting from IoT devices. The cloud service provider platform generates and hosts an unprecedented volume of data. Numerous smart city apps and services will be housed in the cloud due to its high performance, scalable, and stable datacenters. In order to host, develop, and/or launch their smart city services and apps, citizens of smart cities and service providers can rely on cloud services. Additionally, the benefit of pay-as-you-go forces the majority of conventional organisations to actively shift data to the cloud. The cloud not only hosts workloads but also offers effective operational procedures, enhancing the flexibility and agility of businesses. Both enterprise digital transformation and network modernization transformation have benefited from this. The United Nations' 2019 Digital Economy Report emphasises how the digital economy is evolving into a significant engine for economic growth. Statistics are not complete, however the digital economy makes up 4.5% to 15.5% of global GDP. Cloud computing is essential to expediting the development of the modern economic system and promotes the deep integration of the Internet, big data, artificial intelligence, and the real economy. The global market for public

cloud services will increase by 17% to $266.4 billion in 2020 from $227.8 billion in 2019, predicts Gartner, Inc.. Collectively, cloud applications continue to be popular. [2]

Salim et. Al [3] Cloud computing is a new technology often used virtualized with resources to provide dynamically scalable service via the internet. In the cloud computing, users can access to the resources by using a various devices, such as laptops, PCs, smart phone, etc. to access multiple service such as storage, programs, and application-development platforms, over service that provided by cloud providers via the internet. Through the last years, Cloud computing improved from simple web applications, such as Gmail and Hotmail, into business propositions like SalesForce.com, AmazonEC2, etc. Cloud computing may be supply service for reducing IT costs, business management, and maintenance costs of hardware and software are effective. At the same time, it makes the enterprises able to access to professional IT solutions. Data storage center in cloud computing can be reliable and secure, because the world's most advance data center is helping the users save the data. The users must not concern about virus attack, data loss, and other problems when they used the cloud in correct form. User with cloud computing can use the cloud services anywhere, everywhere, on-demand and based on pay per use principle. Cloud computing has two types of models: services models (SaaS, PaaS, and IaaS), and deployment models (Public, Private, Community, and Hybrid cloud). Also the cloud computing is contains five essential characteristics (On-Demand, BroadNetwork Access, Rapid Elasticity, Measured Service, and Resource pooling). There are many companies that provide cloud services such as Amazon, Google, Microsoft, and SalesForce.com, etc. There are many concerns about the data security in cloud computing should be taken into account such as violation of the confidentiality and privacy of customers' data via unauthorized parties. The major concern is if data secure when it save in cloud?. Therefore, we have dedicated our work to design a new architecture to improve data security in cloud computing by using modified Identity-Based Cryptography (MIBC) and Elliptic Curve Integrated Encryption Scheme (ECIES) Algorithm.

Vamsee k [4] proposed playfair and vigenere cipher techniques that were merged with structural aspects of Simplified Data Encryption Standard (SDES) and Data Encryption Standard (DES). In which 64 bit block size of plain text is taken which is fixed and this 64 bit plain text is divided into two halves by using the "black box" the right half have 2 bits whereas left half has 6 bits, then these 6 bits are feed into "superior function" block where these 6 bits are further separated in two halves where first two bits represent the rows and last four bits represent the column by identifying the rows and column the corresponding value can be selected. Then this function is apllied to all 8 octets of the output of vigenere block the resultant of black box is again of 64 bits then these bits are further divided into 4 new octants similarly right 4 bits are unified to formulate right halves. Finally left and right halves are XOR-ed to obtain left half of this arrangement. This process is repeated three times.

Shuai, H., & Jianchuan, X [5] worked with RSA algorithm to encrypt the data and Bilinear Diffie-Hellman to insure the security while exchanging the keys. In proposed method a message header is added in front of each data packet for direct and safe communication between client and cloud without any third party server. When user sends the request to the cloud server for data storage then cloud server creates the user public key, private key and user identification in certain server. Two tasks performed at user end before sending the file to cloud, first add message header to the data and secondly encrypt data including message header by using secret key. When user request for data to the cloud server then it will check the message header of received data and pick up the Unique Identification for Server in cloud (SID) information. If SID information is found it will respond the user request otherwise request will be discarded.

Sood, S. K. [6] used introduced a technique to ensure the availability, integrity and confidentiality of data in cloud by using Secure Socket Layer (SSL) 128 bit encryption that can also be raised to 256 bit encryption. The user who wishes to access the data from cloud is strictly required to provide valid user identity and password before access is given to the encrypted data.

Parsi Kalpana [7] worked with user module to send the data to the cloud then cloud service provider generate a key and encrypts the user data by using RSA algorithm and stored the data into its data centre. When user request the data from cloud then cloud service provider verify the authenticity of the user and give the encrypted data to the user that can be decrypted by calculating the private key.

Mohamed, E. M., Abdelkader [8] developed a three layered data security model is presented in which each layer performs different task to make the data secure in cloud. First layer is responsible for authentication, second layer performs the duty of data encryption and third layer performs the functionality of data recovery.

Singh, J., Kumar, B., & Khatri [9] used RC5 algorithm that is implemented to secure the data in cloud. An encrypted data is transmitted even if the data is stolen there will be no corresponding key to decrypt the data.

Lan, Z., Varadharajan [10] developed a Role Base Encryption (RBE) technique that is proposed to secure the data in cloud and role base access control (RBAC) cloud architecture was also proposed which allows organizations to store data securely in public cloud, while maintaining the secret information of organization's structure in private cloud.

3. Problem Statement

Future-generation technology for IT businesses is cloud computing. It offers several various qualities, including scalability, multi-user, virtualization, and many more. As well provides computational infrastructure that is available on demand, which has the ability to lower the cost of developing IT-based services. It is capable of offering a variety of services online. The ability for customers to store their data as needed is one of the key services offered by the cloud. The user has a difficult situation because all the data are stored in a global resource pool that is interconnected but dispersed among many locations. These data could be accessed by an unauthorised user via the virtual machines. This is the negative aspect of cloud data storage. Users face a serious difficulty as a result of this insecurity. As a result, a significant issue with cloud computing is data security. AES is currently thought to be the most well-liked symmetric cryptographic method[11-12]. It is crucial to create high-performance AES in order to increase the scope of its general use. And hence the further security of encrypted data is necessary to secured on cloud.

4. Objectives

- To implement two step of encryption procedure
- To Authenticate cloud environment with considering high risk assessment
- To resolve maximum issue related to data leakage while storing the data in cloud

5. Proposed Methodology

5.1 Two Level Cryptographic techniques using AES and ECC Algorithm

- **Input**:
  In this step, user can send the original data or message.
- **Encryption**:
  Step 1: Here, we can encrypt the original message or data by using AES algorithm.
  Step 2: Generate a secret key.
  Step 3: Second level, again we can encrypt the data by using ECC algorithm[13].
- **Storage**: Here, we can store the encrypted data in cloud for more security (Box cloud or cloudme)
- **Decryption**:
  Step 1: Here, we can decrypt the encrypted data by using generated key.
- **Performance**: Here, we can estimate some performance metrics such as
  - PSNR
  - MSE

7. Proposed flow of the system

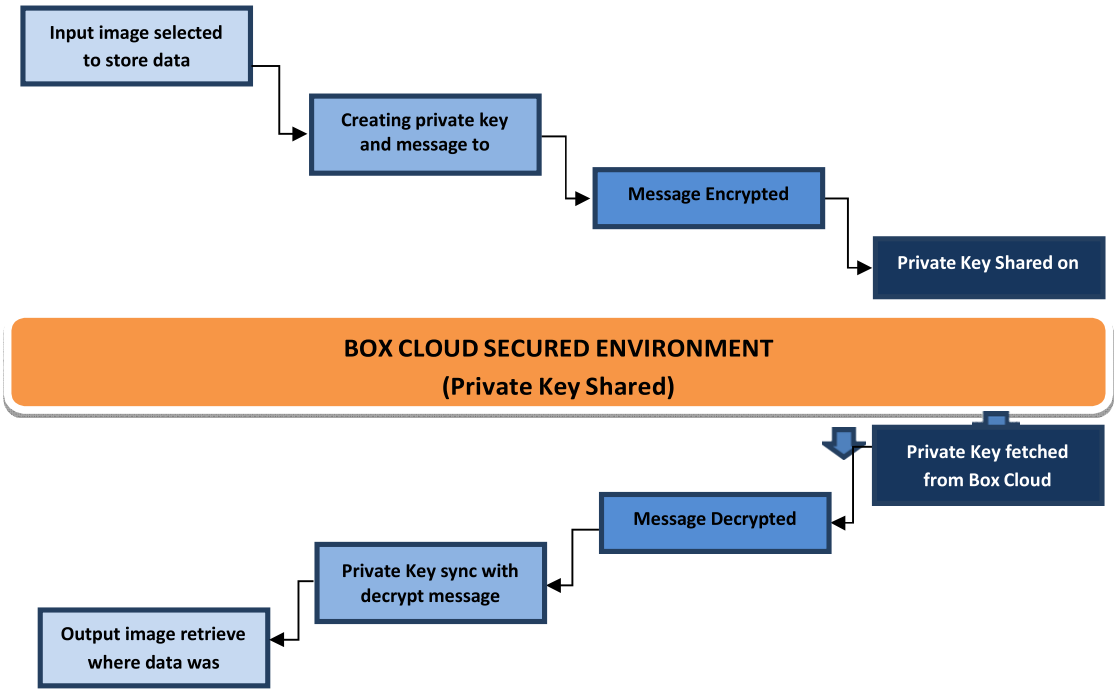

Fig. 1. Flow diagram of the proposed process

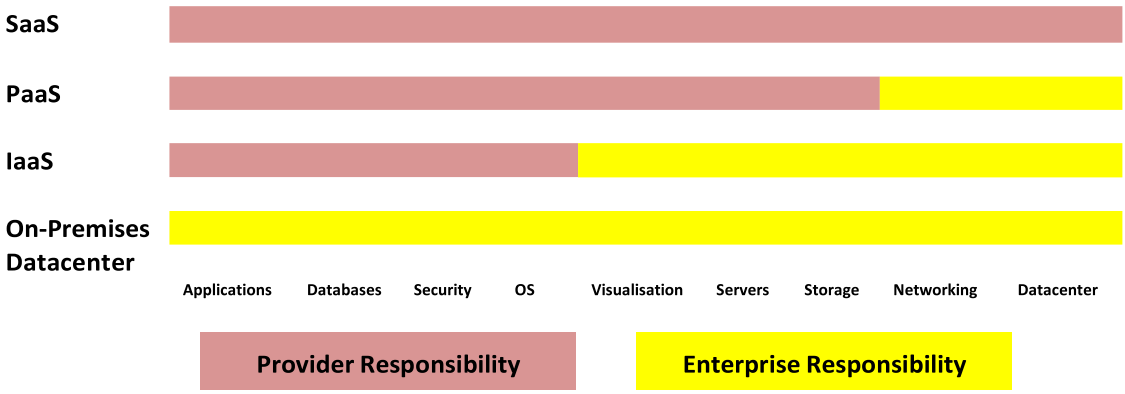

Fig. 2 Comparison of responsibilities of Cloud Computing environment in various fields

8. Implementation

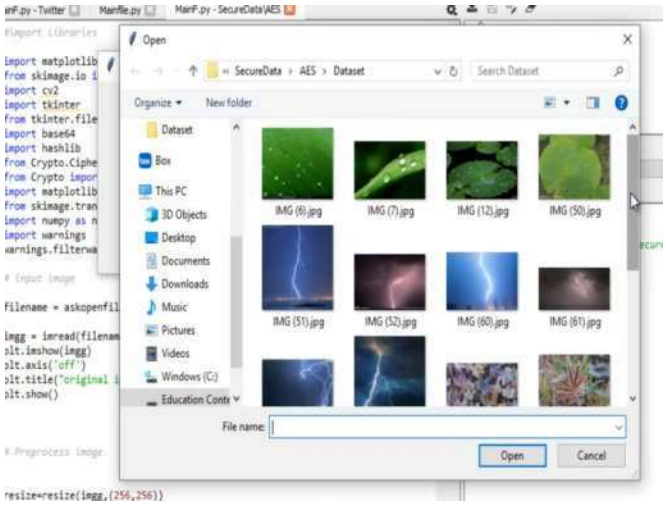

Fig. 3 Editor window and selection of data

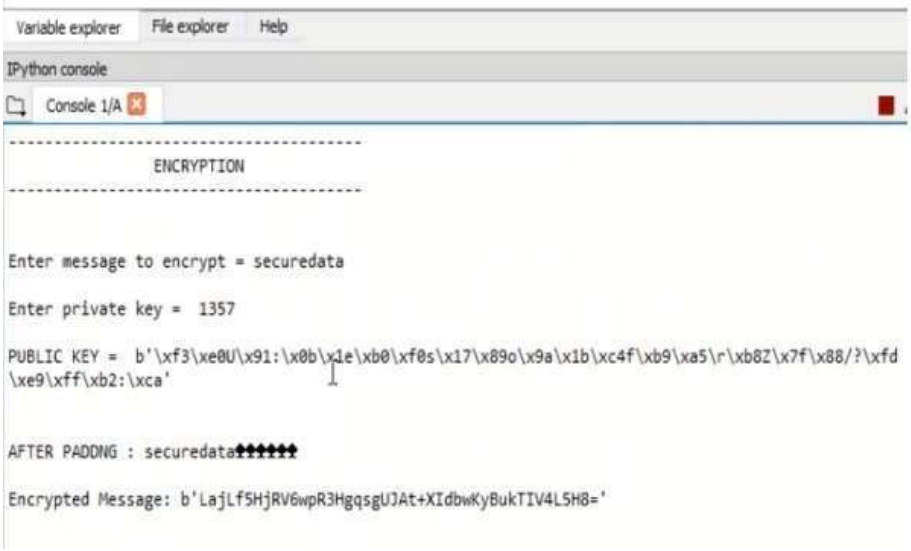

Fig. 4 Message to encrypt and private key saving on box cloud

Fig. 5. Decryption and fetching private key from box cloud

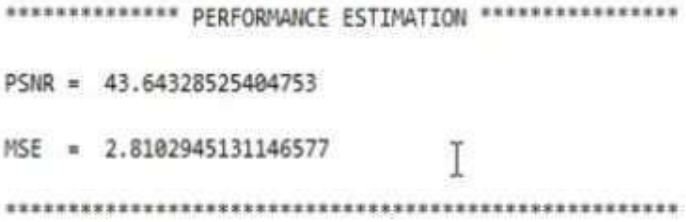

Fig. 6. Performance Estimation

9. Objective and various Technical Methods for Security Features in cloud

Objective 1

Collaborative access control

Proposed Schemes: Attribute-based controlled, collaborative access control scheme

Technical Methods: Translation nodes insertion, Data confidentiality[14]

Objective 2

Self-adaptive access control

Proposed Schemes: Self-adaptive access control with smart deduplication[15]

Technical Methods: Break-glass access, Secure deduplication, Data confidentiality, Secure deduplication

Objective 3

Group-oriented access control

Proposed Schemes: Attribute-based privacy-preserving data sharing for dynamic groups

Technical Methods: Broadcast encryption, Re-encryption algorithms, Data confidentiality, Fine-grained access control, Dynamic groups data sharing

10.Conclusion

A literature review of the works in the area of cloud computing data security is conducted and the results of review are presented in this paper. The results show that the majority of approaches are based on encryption (45%) out of which 71% encryption techniques results are validated. 67% of encryption techniques used experimentation to validate the results. These results point towards the fact that most of researchers show their interest in encryption technique to enhance the security of

data in cloud computing environment. The results also reveals the fact of lack of validation in proposed approaches as 42% of the studies provide no validation of the results out of which 67% are guidelines. Only few studies have used statistical analysis for validation. This area (validation) needs the attention of the research community to gain the trust and confidence of cloud computing users.

References:

[1] Smitha Nisha Mendonca," Data Security in Cloud using AES", International Journal of Engineering Research & Technology (IJERT) http://www.ijert.org ISSN: 2278-0181 IJERTV7IS010104 Vol. 7 Issue 01, January-2018

[2] Pan Yang1, Neal N. Xiong2, And Jingli Ren1," Data Security and Privacy Protection for Cloud Storage: A Survey", 10.1109/ACCESS.2020.3009876, IEEE Access, Volume 4, 2016

[3] Salim Ali Abbas, Amal Abdul Baqi Maryoosh," Data Security for Cloud Computing based on Elliptic Curve Integrated Encryption Scheme (ECIES) and Modified Identity based Cryptography (MIBC)", International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 10 – No.6, March 2016

[4] Vamsee k and sriram r,(2011) "Data Security in Cloud Computing,"in Journal of Computer and Mathematical Sciences Vol. 2, pp.1-169

[5] Shuai, H., & Jianchuan, X. (2011, 15-17 Sept. 2011). Ensuring data storage security through a novel third party auditor scheme in cloud computing. Paper presented at the Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on.

[6] Sood, S. K. (2012). A combined approach to ensure data security in cloud computing. Journal of Network and Computer Applications, 35(6), 1831- 1838

[7] Parsi Kalpana & Sudha Singaraju (2012).Data Security in Cloud Computing using RSA Algorithm. International Journal of Research in Computer and Communication technology(IJRCCT), vol 1, Issue 4.

[8] Mohamed, E. M., Abdelkader, H. S., & El-Etriby, S. (2012,14-16 May 2012). Enhanced data security model for cloud computing. Paper presented at the Informatics and Systems (INFOS), 2012 8th International Conference on.

[9] Singh, J., Kumar, B., & Khatri, A. (2012, 6-8 Dec. 2012). Improving stored data security in Cloud using Rc5 algorithm. Paper presented at the Engineering (NUiCONE), 2012 Nirma University International Conference on.

[10] Lan, Z., Varadharajan, V., & Hitchens, M. (2013). Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage. Information Forensics and Security, IEEE Transactions on, 8(12), 1947-1960.

[11] Taeho, J., Xiang-Yang, L., Zhiguo, W., & Meng, W. (2013, 14-19 April 2013). Privacy preserving cloud data access with multi-authorities. Paper presented at the INFOCOM, 2013 Proceedings IEEE

[12] Ravindra Changala, "Secured Activity Based Authentication System", Journal of innovations in computer science and engineering (JICSE), Volume 6, Issue 1,Pages 1-4, September 2016.ISSN: 2455-3506.

[13] Ishu Gupta, "Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis, and Future Directions", VOLUME 10, 2022,IEEE Access.

[14] Mazhar Ali, "SeDaSC: Secure data sharing in clouds",1932-8184 © 2015 IEEE.

[15] Cloud security Alliance, "Security guidelines for critical areas of focus in cloud computing v3.0,"2011.