iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** II **Month of publication:** February 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 4 Issue II, February 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Multi-Level Security Mechanism for Data Storage in Cloud Computing: A Review

Anamika Sirohi[1], Vishal Shrivastava[2]
[1,2]*Department of Computer Science and Engineering, Arya College of Engineering and IT, Jaipur, Rajasthan, India*

***Abstract*— Cloud computing is a highly-scalable distributing computing platform in which resources are offered as services. The security of data in cloud is one of the important issue which act as an obstacle in the implementation of cloud computing. This paper is proposing an efficient cloud security model in which the model is providing the multi-level encryption mechanism over the data to be uploaded at the cloud as well as role-based authentication for the users. The model is including four parties: Data owner, Private Cloud, Admin and User. The encryption mechanism is using the RSA algorithm first and further re-encrypts the data with MD5 to enhance the security of the data. The Message authentication Code is being generated before uploading the encrypted data which will be used after downloading of the data. The Message Authentication Code of downloaded data will be decrypted first by user and then send to Data owner for data integrity check. After that the user can decrypt the downloaded data if he get confirmation from Data owner. The model is using the best possible multiple techniques in a single approach.**

Keywords*— *Cloud Computing, Encryption, Message Authentication Code, Role-based Authentication.

I. INTRODUCTION

Cloud Computing is the biggest innovation in today's world of computing. It is tremendously gaining attention in scientific world and Information Technology sector. Cloud computing [1] will be forthcoming utility. Cloud computing utility will serve as the most basic level of computing service that will be needed to fulfil human daily needs. Basically, Cloud computing is anything whether it is about storage, hardware, software or full virtualized machine accessing from anywhere, anytime through internet. These storage, hardware or software which is delivered to the user remotely are maintained and monitored by the cloud service provider. The cloud seems [2] as:

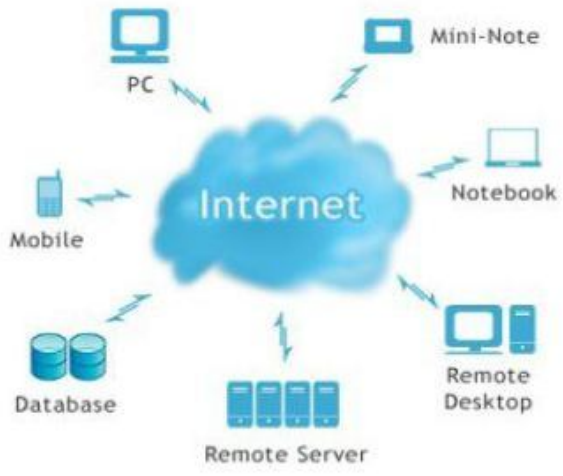


Fig 1. Cloud Computing

This aspect is also reflected as [3], Cloud computing refers to both the applications delivered as the services over Internet and the hardware, and the system software in the data-centres that provide those services." The three criteria[4] to recognize whether a service is delivered in the cloud computing form, are defined as: The service is accessible via a Web browser or a Web services application programming interface (API), Zero money is necessary to get started, Pay-per-use basis. The cloud computing services are freely available for the single users and for enterprise class; the services are delivered according to specific pricing scheme. In this case the user needs to subscribe the service and establish through the service provider, a service-level agreement defining the

quality-of-service parameters under which the services are going to be delivered. The utility-oriented nature of cloud computing is expressed as [5], a cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers.Security in the terms of confidentiality and protection of the data in a cloud environment is one of the important challenge. These are specifically tied to the ubiquitous nature of cloud computing, which spreads computing infrastructure across all the geographical locations. Cloud security is a highly complex issue. Especially the data owners of large organizations fear about data misuse by the cloud provider without their knowledge. There will be an issue for the data security in cloud environment which includes confidentiality, integrity, authentication and authorization. The cloud computing model contains three functional units as listed below:

A. Cloud Service Provider

It is an entity that manages Cloud Storage Server (CSS), which has significant storage space to store the client's data and has high computational power.

B. Client / Owner

It is an entity, which stores the large data files in the cloud and depends on the cloud for data maintenance and computation; it can be either single consumer or an organization.

C. User

It is a unit, which is registered with the owner and uses the data of the owner which is stored on the cloud. The user can be an owner as well.

II. MESSAGE AUTHENTICATION CODE

In cryptography, a hash message authentication code is a special construction for calculating a Message authentication Code (MAC)[6] containing a hash function combined with cryptographic secret key. MAC is using for data integrity and authentication. In the proposed cloud security model we are using MD5 as hash function for calculating MAC. The cryptographic strength is depends on the functionality of hash function and size of hash output and quality of the providing key.

A. Hash Message Authentication Code

Definition (from RFC 2104):

$$HMAC(K, m) = H\left((K \oplus opad) \mid\mid H\left((K \oplus ipad) \mid\mid m\right)\right)$$

where,

H is a cryptographic hash function,

K is a secret key padded to the right with extra zeroes to the input block size of the hash function, or the hash of the original key if it is longer than that block size,

m is the message to be authenticated,

|| denotes concatenation,

⊕ denotes exclusive or (XOR),

opad is the outer padding (0x5c5c5c…5c5c, one-block-long hexadecimal constant),

and ipad is the inner padding (0x363636…3636, one-block-long hexadecimal constant).

The algorithm we are using MD-5 (Message Digest)[7] is as follow: MD5 process a variable-length message into a fixed-length output of 128 bits. The input message is broken up into clump of 512-bit blocks (sixteen 32-bit words); the message is padded so that its length is divisible by 512. The padding works as follows: first a single bit, 1 is appended to the end of the message. This is followed by as many zeros as required to bring the length of the message up to 64 bits less than the multiple of 512. The remaining bits are filled with 64 bits representing the length of the original message, modulo 264. The main MD5 algorithm operates on the divided 128 bits into four 32-bit words.

III. LITERATURE SURVEY

In this paper, I have made a review on my topic i.e. providing data security in cloud using different techniques, by reading different

kinds of papers published by authors are discussed as follows:

Jing et.al. [8] describes the security of data in cloud using Hadoop Framework. They described to solve the security problem in the distributed network cloud disk. Based on the different confidentiality level of user data, it gave selective encryption scheme, which gave full following security issues, such as the security of the user data transmission in the network, no verification of the data before uploading; the user data privacy might be leaked etc. Combination of the rapid symmetric encryption algorithm and identity authentication of RSA, overtime checking and the performance of Hadoop, so that in the distributed network the cloud data security storage disk can be supply secured, effective and will have stable effect. But the scheme focuses only on data encryption technique like DES or AES not on the user authentication. Thilakanathan et.al. [9] proposed scheme using proxy re-encryption for security of data. They addressed the issues of privacy and security in the domain of mobile tele-care and cloud computing. Demonstrated a tele-care application that allowed doctors to remotely monitor patients via cloud and then use this system as a basis to showcase a model which allowed the patients to share their health information with other doctors, nurses or medical professionals in a secure manner. The scheme used in this model was proxy re-encryption for security of the data. In this scheme the data owner will encrypt the data using his key piece and then proxy-encrypt the data using his remaining key piece. Decryption is will be carried in similar fashion. However, if proxy is untrusted then data becomes insecure. Sharma et.al. [10] discusses the challenges and threats in deployment models and also discuss about obstacles in implementation of cloud computing. It highlights different service models of cloud computing, key security issues at cloud, the challenges and its solution at different layers of cloud. They highlighted deployment models, threats in security parameters, key security issues and challenges at each layer of cloud. They described the requirement of security at different service models and focused under developed areas. The anxiety of cloud can be easily expelled, saving enterprises time and investment. This service can be easily integrated by different organizations such as banking, search engines and enterprise applications. Li et.al. [11] discussed an efficient model for secure data sharing in cloud. They aimed at enabling efficient and secure data sharing in cloud computing by providing a generic construction for this purpose. The construction was full-featured: it enables the authorized users to perform keyword-based search directly on encrypted data without sharing the unique secret key; and it provides two-layered access control to limit unauthorized users access to the shared data. On the basis of their proposed generic construction, utilization of the existing techniques based on identity broadcast encryption and public-key searchable encryption to instantiate a detailed construction. The model has some issues like if authority is untrusted then the data will be insecure and it's costly to use the model on the basis of time. Sood et.al. [12] discusses the security which comes to cloud computing. The data owner cannot trust the cloud when it comes to possible misuse of data by the cloud provider. Their model proposed to keep the most critical data on the private cloud and the rest of the data on the public cloud. Also, the proposed model uses the hash codes to tackle the issues regarding the integrity of the data at the public cloud. Their cloud security model provides the arrangement of defining the user roles thereby determining the type of access the user exercises on the data. Hence, it consumes time and if the sensitive data is increased then this model will be expensive. The whitepapers [13] discusses that organizational policies or industry or government regulations, which may require the use of encryption to protect your data at rest. The flexible nature of Amazon Web Services (AWS) is to allow you to choose from the various options which meet your needs. This whitepaper provides an overview of today's available different methods for encrypting your data at rest. This whitepaper from many organizations describe three types of data security model in cloud. First model consists of key generation and encryption on data which is performed by data owner. However, this will result in high overhead for data owner. Second model describes the encryption will be performed by data owner and key generation by the cloud service provider. Unfortunately, if cloud service provider is untrusted then data is insecure. In third model the encryption and key generation was controlled by cloud service provider only. If service provider is untrusted then the data is endangered.

Hwang et.al. [14] proposed a business model for cloud computing situated on the concept of separating the encryption and decryption service from the storage service. Moreover, the party responsible for the data storage system must not store data in plain-form. And the party responsible for data encryption and decryption must delete all the data about the computation once the encryption or decryption is completed. The exemplary service utilizes three cloud systems, including an encryption and decryption system, a storage system, and a CRM (Customer Relationship Management) application system. One of the service provider performs the encryption and decryption services while other providers operate on the storage and application systems. It further includes suggestions for multi-party Service-Level Agreement (SLA) suitable for business model. This consumes time too. Varalakshmi et.al. [15] describes that the data integrity is essential to secure the data in a cloud environment. Their work creates theoretical cloud architecture by adopting an encryption algorithm with dynamic small sized key to ensure the security and doesn't compromise type of any information with the cloud server. It involves a third party who encrypts the client's information for

ensuring the security, partitioning into multiple segments based on the remaining dynamic storage capacity presented in the VMs of cloud storage servers. And store these encrypted segments of the client's file on the corresponding VM (Virtual Machine) of the cloud storage. Then it generates the hash value of the encrypted segment, store and manage these details for further verification purpose. Mohamed et.al [16] discuss about data security for both cloud computing and traditional desktop applications, to obtain best possible level of privacy. It presented an evaluation for selected eight modern encryption techniques namely: RC4, RC6, MARS, AES, DES, 3DES, Two-Fish, and Blowfish at two independent platforms namely; desktop computer and Amazon EC2 Micro Instance cloud computing environment. The evaluation was performed for these encryption algorithms according to random testing by using NIST (National Institute of Standards and Technology) statistical testing in the cloud computing environment. Xu et.al. [17] discuss an important issue such as efficient user revocation and key refreshing are not straight-forward, which constrains the approval of Cipher Attribute Based Encryption (CP-ABE) in cloud storage systems. They proposed a dynamic user revocation and key refreshing model for Cipher Attribute Based Encryption (CP-ABE) schemes. The key feature of their model was its generic possibility in general Cipher Attribute Based Encryption (CP-ABE) schemes which refresh the system keys or will remove the access from a user without issuing new keys to other users or will re-encrypt the existing cipher-text.

IV. PROPOSED MODEL

The proposed model is based on data owner, centric approach as data security is important concern and user cannot trust anyone like cloud service provider or other party. Proposed model has been organized in such a manner that it gives data security in cloud computing at different levels. The different threat levels are: user level, cloud service provider level and network intruder level. In proposed model data remains private during transmit as well as at cloud itself and from the untrusted users. The goals of proposed model are to provide security:

At user level: Data will remain secure from dishonest employees of the organization or intruder.

At cloud service provider: Data will remain private form untrusted cloud provider.

Network intruder: Data will remain secure during transmit or over the network from intruders.

Data confidentiality: Data secrecy will be maintained throughout the proposed model.

Data privacy: The authentication will keep the data privacy so that data cannot be leaked.

Data Integrity: To check data tampering over the network by the network intruder during transmit of data, data integrity will be maintained.

Proposed model has been designed in a way that issue related to data security in the cloud computing should be resolved and user feels free to adopt cloud. In order to secure data, encryption of data is carried out according to its sensitivity. The data is classified as: Data0 and Data1.

Data0 – Data is not sensitive i.e. no need to encrypt data. Data can be directly uploaded at cloud without encryption.

Data1 – Data is sensitive and need to be encrypted before uploading at cloud.

Data0 and Data1 are depending on the response of data owner. For Data1 type data follow Data Encryption Mechanism. This makes it efficient as well as a secure method.

A. Encryption Mechanism

Data encryption is handled by two entities: admin and data owner. Admin acts as Key Management Infrastructure (KMI) for the organization. Key Management Infrastructure handles the key generation and key storage. Main responsibility of admin is to generate asymmetric keys and give the required key to data owner for encrypting the data through secure channel. The keys will be generated using RSA algorithm using DES3 (Triple Data Encryption Standard). After data encryption the required key i.e. public key is returned back to key storage. Key storage protects, maintain, distribute and store the key securely. Data owner also acts as an admin as well as an access controller for the data to be accessed. Key maintenance and protection includes providing keys only after verification of required users. Login details are encrypted with by data owner which will only decrypted by the verified user when he/she will get verified. The user verification will be done by data owner as the verified users list of organization will be at admin. But for verification the data owner will do passwordless authentication. Then the private key will be passed to user. For the data encryption we will use firstly RSA encryption algorithm and for enhancing the security of data, we will use MD5 over the encrypted data. So, that more security will be provided and it will be hard to decrypt the data by unauthorized user. Other more complex algorithms could be used here but to propose a new approach and for easy implementation RSA and MD5 are used.

Volume 4 Issue II, February 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

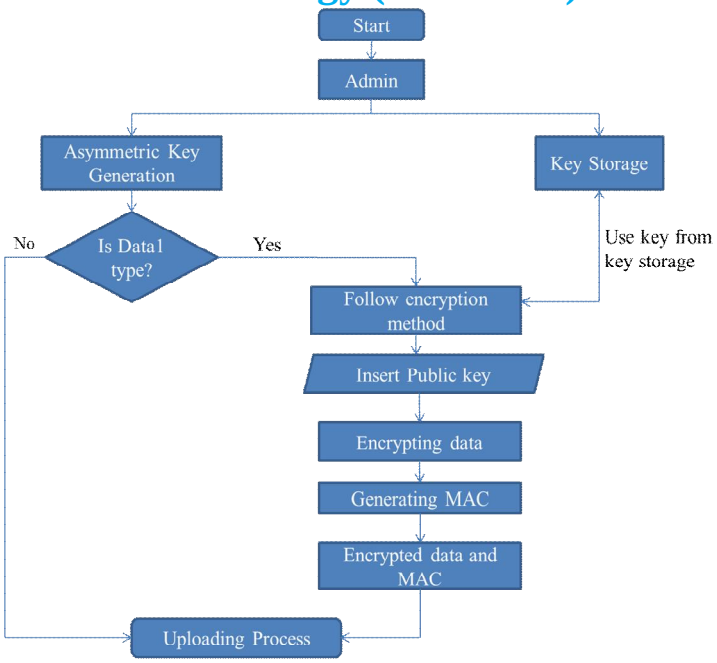


Fig 2. Data Encryption Mechanism

B. Uploading Data To Cloud

Now the encrypted data is ready to be uploaded on the cloud. Before uploading, Message Authentication Code (MAC) is generated on encrypted data for data integrity. Data Integrity verifies that the data has been tampered or not while passing through the network.

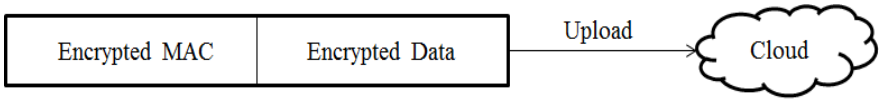


Fig 3. Uploading Data at Cloud

Message Authentication Code is also encrypted in the same manner as data by following the data encryption mechanism. Encrypted data and Message Authentication Code will be uploaded at cloud. The standard Message-Digest5 (MD5) algorithm is used for generating Message Authentication Code (MAC) for data integrity.

C. Role-Based Dual User Authentication

When the data is needed by data owner or user they have to download the data from the cloud. If the data is required by data owner then it gets direct access to cloud as an administrator of the cloud. Data owner have full privilege on cloud so it can add or revoke user and also give role-based access to its uploaded data. In Role-based authentication the data owner will create the group of users and after uploading the data, the data owner can provide the role over the data i.e. user can read, edit, share etc. If data is required by user then user have to undergo with dual verification which is carried by admin and further verified by data owner. Admin makes the database for user authentication. In this model it is assumed that organization have provided their users with login id and password and uniform resource locator (URL) or IP address where the data is residing. When user login to desire URL or IP address with user id and password as provided by the organization then admin will verify the user by checking its database. If user is an authorized user then admin issues private key without passcode and also notify data owner about user. Now further verification is performed by the data owner. Data owner verify user using passwordless authentication where after performing the data owner could direct login to user and if verified, then owner provide cloud login id, password, information about passcode of private key in encrypted format. This encrypted data is decrypted using after verification at user side. User sends the identity of user to cloud so that cloud service provider allows user to login to cloud to access the data. Now user will login to cloud to access data. Through role-based access to data i.e. user can update, read or delete etc. according to data owner's wish.

Volume 4 Issue II, February 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

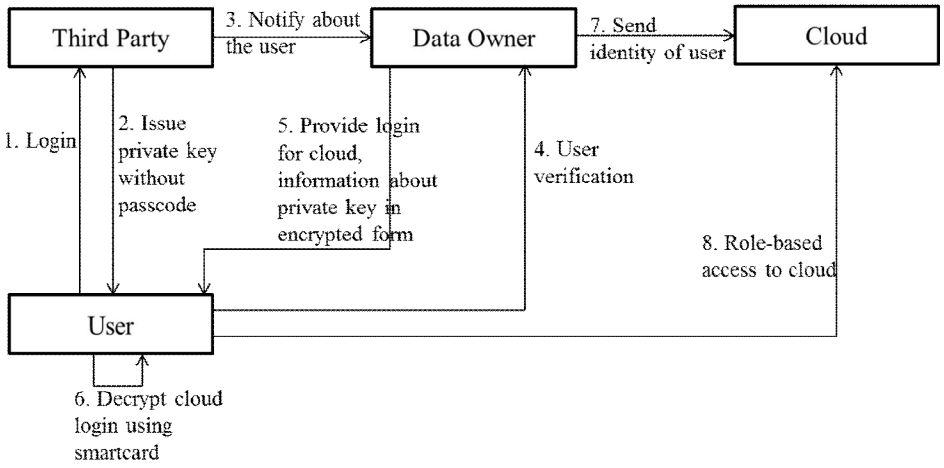


Fig 4. Role-Based Dual User Authentication

D. Message Authentication Code Verification

Now user has downloaded the encrypted data/file and Message Authentication Code. User will decrypt the Message Authentication Code first and then calculate Message Authentication Code on encrypted data. And then the user will send the calculated MAC to the data owner. Then data owner will check for the both the Message Authentication Code i.e. decrypted received Message Authentication Code and own calculated Message Authentication Code, if they are same then the data is not being misused by unauthorized user. And then the data owner will send the status to user. Now, the data can be decrypted by the further procedure i.e. by private key and then the data can be used otherwise user can report to data owner about Message Authentication Code mismatch.

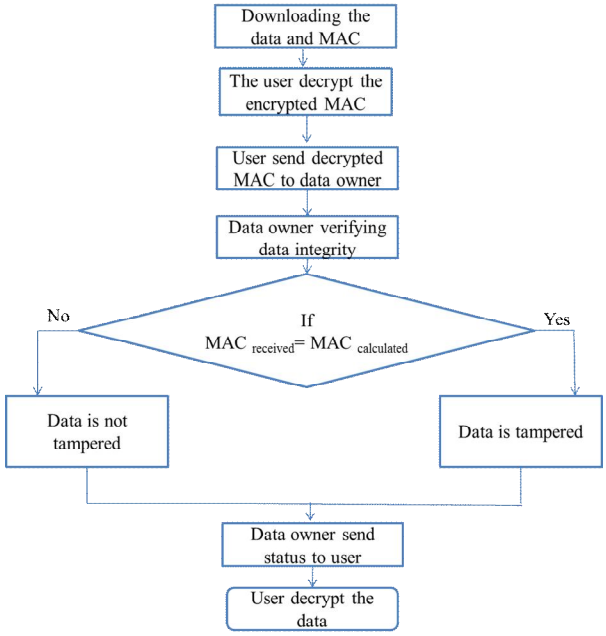


Fig 5. Verifying Data Integrity

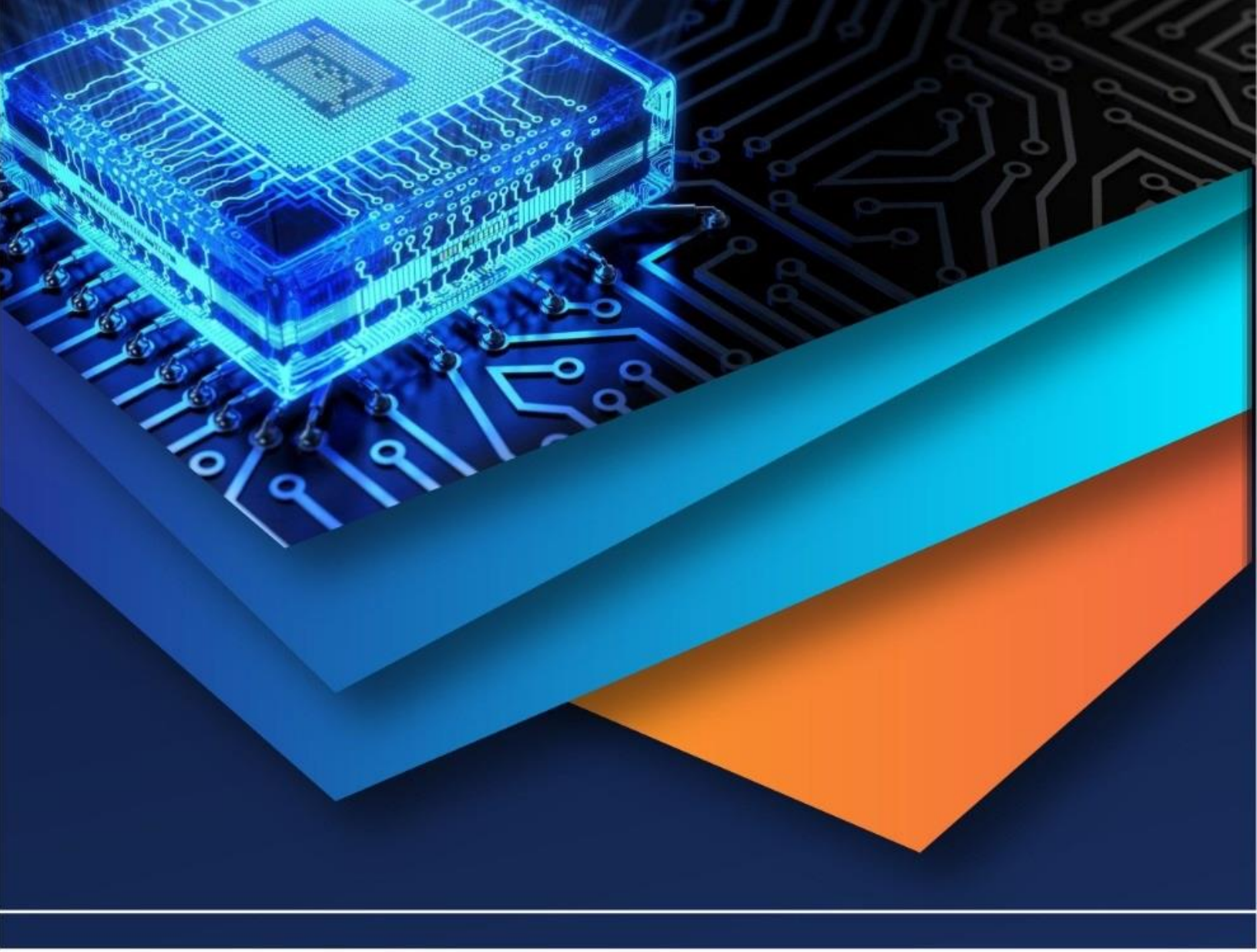
V. CONCLUSIONS

The proposed technique provides a multi-level encryption mechanism in a single model for data storage in cloud. It provides the role-based user authentication and data integrity through message authentication code. It provides the security at different levels such as cloud service provider, user, cloud and admin. Generally the main doubt occurs during uploading of data. Keeping this concern the proposed model is providing the security of data at cloud. The security is enhanced with the help of MD5. It is highly

secure and efficient model which can be used to upload the data without the fear of unauthorized user access.

REFERENCES

[1] Rajkumar Buyya, Christian Vecchiola,S. Thamarai Selvi: Mastering Cloud Computing Foundations and Applications Programming, Morgan Kaufmann, USA, pp. 3-27, 2013.
[2] Garima Mahajan, "Job Scheduling In Cloud Computing: A Review of Selected Techniques", Iunternational Journal of Emerging Trende & Technology in Computer Science, vol. 3, no. 3, p.p-254, 2014.
[3] Armbrust M, Fox A, Griffith R, Joseph A, Katz R, Konwinski A, Technical Report No. UCB/ EECS-2009-28 Above the clouds: a berkeley view of cloud computing. USA: University of California at Berkeley, pp. 1-10, 2009.
[4] Reese G. Cloud application architectures: building applications and infrastructure in the cloud. Sebastopol, CA, USA: O'Reilly Media Inc., pp. 1-50, 2009.
[5] Buyya R, Yeo CS, Venugopal S. , "Market oriented cloud computing: vision, hype, and reality for delivering IT services as computing utilities" , 10th conference on high perfor- mance computing and communications,Dalian, China, IEEE, pp. 5-13, 2008.
[6] Hash Message Authentication Code: https://en.wikipedia.org/wiki/HMAC.
[7] Message Digest: https://en.wikipedia.org/wiki/MD5.
[8] Jing Huang Jing, LI Renfa, TangZhuo, "The Research of the Data Security for Cloud Disk Based on the Hadoop Framework", Intelligent Control and Information Processing, pp. 293-298, IEEE, 2013.
[9] Danan Thilakanatha, Shiping Chen, Surya Nepal, Rafael A. Calvo, Leila Alem, "A platform for secure monitoring and sharing of generic health data in the Cloud", Elsevier Ltd, vol. 35, pp. 102-113, 2013.
[10] Pardeep Sharma, Sandeep K. Sood, Sumeet Kaur, "Cloud Implementation Issues and What to Compute on Cloud", International Journal of Advances in Computer Networks and its Security, vol.1, no. 1, pp. 130-135, 2011.
[11] Jingwei Li, Jin Li, Zheli Liu, Chunfu Jia,"Enabling efficient and secure data sharing in cloud computing" Concurrency Computat.: Pract Exper., John Wiley & Sons , Ltd., vol.26,no. 5, pp. 1052-1066, 2014.
[12] Sandeep K. Sood, "Hybrid Data Security model for Cloud ", Intternational Journal of Cloud Applications and Computing,vol. 3, no. 3, pp. 50-59, 2013.
[13] Amazon Web Services: "Encrypting Data at Rest in AWS", https://aws.amazon.com/ whitepapers, pp. 2-18, 2014.
[14] Jing-Jang Hwang, Hung-Kai Chuang, Yi-Chang Hsu, Chien-Hsing Wu, "A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service", International Conference on Information Science and Applications, IEEE, pp. 1-7, 2011.
[15] P.Varalakshmi, Hamsavardhini Deventhiran, "Integrity Checking for Cloud Environment Using Encryption Algorithm", IEEE, pp. 228-232, 2012.
[16] Eman M.Mohamed ,Sherif EI-Etriby, "Randomness Testing of Modern Encryption Techniques in Cloud Environment", 8th International Conference on Informatics and Systems, pp. 237-241, 2012.
[17] Zhiqian Xu, Keith M. Martin, "Dynamic User Revocation and Key Refreshing for Attribute-Based Encryption in Cloud Storage", International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, pp. 844-849, 2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY