RESEARCH ARTICLE OPEN ACCESS

Securing Cloud by Enhancing Privacy Preservation and User Based Access Control Mechanism

Shubham S. Chourasiya, A.R.Bhagat Patil
Department of Computer Science Yashwantrao Chavhan College of Engg Nagpur, India
Department of Computer Science Yashwantrao Chavhan College of Engg Nagpur, India
Corresponding Author; Shubham S. Chourasiya

ABSTRACT: Cloud has Done away with Physical Barrier to record our data. Cloud computing is evolving as a widespread data access paradigm.However security and privacy complications regarding the storing of the data in the cloud and access through the Internet have been most important concerns for several organizations. The data and also the human resources region unit the life blood of some organization. Hence, they should be intensely protected as cloud owner can exploit the security we need to protect cloud by encryption as well as security keys for accessIn this review paper, we identify the security concerns related with cloud computing and plan a system that will protect public cloud by encryption as well as security keys to access and help the user to enjoy all the benefits of hosting their data in the cloud whereas at the identical time supporting fine-grained and flexible access control for common data presented in the cloud.
Keyword: Cloud, SHA-1,AES Algorithm and Blowfish Algorithm

Date of Submission: 17-02-2019 Date of acceptance: 03-03-2019

I. INTODUCTION

Cloud Computing is the developing technology where we can get platform, software and infrastructure as a service. While comes to storage as a service, data utilization and data privacy are the main issues.To keep the cloud data secure we implement the more advanced encryption and decryption algorithms by which public and private user's data will remain secure in cloud. To enhance user's privacy we putted user's details on third party server so cloud admin will not be able to violate user's privacy.This system providing service for public users and private users. Public user can able to upload data in the cloud without disclosing his or her personal details and user's

uploaded data will remain secure in the cloud. Private user is an authenticated user able to share data among private users and upload and download file in cloud. A vast quantity of data is being saved in the cloud, and more of this is sensitive information. This application can be use in day to day life likeprivate information in secure cloud.keeping personaldetails, medical history details and other.To care for a Cloud Third Party security server (to store user info OTP Key generation Server).It Deliver OTP to access Cloud. Third party Server will decide the Encryption Logic to record data on the cloud. As Cloud having only data but not having users personal info (Privacy preserving).OTP can't be guessed because its one time generated key for one transaction dynamically by security server. Cloud Don't have decryption logic of Encrypted data. User based control access mechanism to access process cloud data.

II. RELATED WORK

The Single Key Distribution Centre architecture (KDC) with no anonymous verification makes it extra complicated and it also raises the storage overhead at the single KDC. The pictographic overview of the decentralized KDC is depicted. The projected decentralized architecture, also authenticate users, who want to remain unidentified while accessing the cloud. We offered a distributed access control mechanism in clouds. In the introductory version of this review paper, we cover the previous work with added features which permits to authenticate the validity of the message without revealing the identity of user who has kept information in the cloud. In this review paper, we correspondingly address user revocation. We use attribute based signature scheme to complete authenticity and privacy. Our scheme is unaffected to replay attacks, in which user can interchange fresh data with stale data from prior write, even if it no elongated has valid claim policy. This is a significant property for a user, repealed of its attributes, might no longer be able to write to the cloud. The projected architecture consists of the following modules. The decentralized KDC architecture here considers two Key Distribution Centre's KDCs. The illustrative representation of the overall flow of the proposed architecture is depicted in Fig. 1. The user who is the file owner has a group of files stores the files in cloud

server in the way of coded files and indexing. The cloud checks the user even without knowing the original identity of the user; relatively two steps authentications takes place with the benefit of the (TPA) Trusted Party Authenticator and (KDC) Key Distribution Centre.

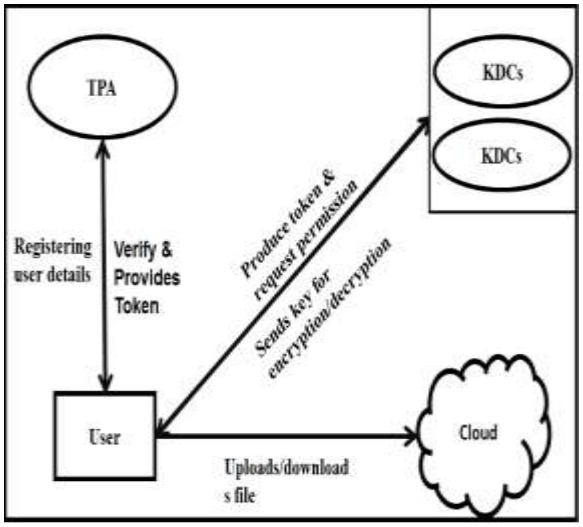

Figure 1: An illustration of Single KDC Architecture[7]

1)Service Request to Third Party Authenticator TPA: The user registers with the original identity and sign up with the TPA .The user directs request to the Third Party Authenticator for registration.

2)Third Party Authenticator Policy Creation: The Third Party Authenticator along with token offers the rules and regulation to be monitored by Creator, Reader and Writer.

3) User File Upload: The file initiator after receiving proper authentication encodes the file and uploads his/her files into the cloud.

4) Key Distribution Centers (KDC) Key Generation: The KDC which are decentralized make different keys to different types of users after receiving tokens from users.

5) Key Revocation: When there is misconduct detected upon a user his/her key is canceled and that specific user can neither use nor re-enter the cloud environment.

6)Cloud Admin: Cloud admin has the list of KDCs and Third Party Authenticator. The cloud admin sets the rules to be followed by Third Party Authenticator (TPA) and Key Distribution Center (KDC). It monitors the key generation policies and notifies abnormal behaviors.

III. LITERATURE REVIEW

In the past several other works are implemented for the cloud data security. The literature reviews of some of these works are described below:

InIn 2012, Amazon data center size [1] the features of cloud computing describe in subsequent way, first of all its huge environment which contains numerous number of host and virtual machines. Amazon EC2 cloud provide facility closely too countless cloud, this can be potential as a result of each host are going to be helpful to several virtual machine.

In 2012, AL.Jeeva, Dr.V.Palanisamy and K.Kanagaram [2] In Cloud Storage any entity's or organization's data is kept in and accessible from several distributed and linked resources that comprise a cloud. To deliver protected communication over connected resources and distributed secret writing formula plays a significant role.

In 2013, RachnaArora, AnshuParashar [3] discussed some of the security issues and challenges about cloud security. Further, some security algorithms are also discussed by describing various features of them and making a comparison of all these encryption schemes and suggestions are made to make it more suitable for the area of usability of each algorithm to make it more effective.

In 2013,MandeepKaur, Manish Mahajan [4] has proposed a system by first highlighting the cloud types, its characteristics, background of cloud environment and also addresses some of cloud issues and challenges that are faced nowadays. Bearing in mind all these things author discuss symmetric and asymmetric encryption algorithms and then proposed a system that forms a cipher cloud to which user will not need any of the resources or software to encrypt the data. Keys are generated instantly and choice of encryption algorithm is also provided to the user to which they want. This makes the cloud environment more efficient.

In 2014, Kan Yang and XiaohuaJia [5] Cloud storage is a significant service of cloud computing, which deals services for data vendors to host their data in the cloud. This different standard information of knowledge of information hosting and access services presents a good challenge to data access organization. As the cloud server cannot be completely trusted by data owners, this has been resolved by using the attribute based encryption in the prior methods

In 2014, S DivyaBharathy et al, [6] The Single Key Distribution Centers (KDC) architecture with no unidentified authentication makes it additional complicated and it also raises the storage overhead at the single Key Distribution Centers. We projected a distributed access control mechanism in clouds.

In 2014, R.Ranjith, S.Murugaanandam Department of IT, [7] in the initial version of this review paper, we cover the previous work with added features which permits to authenticate the validity of

the message without revealing the identity of user who has kept information in the cloud.

In 2015, RachanaChavda, Rajanikanth Aluvalu [8] has conducted a survey on various attribute based encryption techniques and also provide the limitations of all the schemes and then provide its own solution of the encryption based access control model in which the use of hierarchical set based encryption is used to enhance the security which makes the system more flexible, scalable, expressive, effective user revocation and fine grained access control.

In 2015, PriyankaOra, P.R.Pal [9] has proposed a system to maintain data integrity and data confidentiality. To provide its finest level of security, combination of 2 cryptography theme is enforced to get a brand new coding pattern before uploading it to the server. In addition to take care of its integrity and confidentiality, knowledge backups area unit performed that additionally serves the aim of security also by creating checks on this knowledge backup.

In 2016, AnirudhaPratap Singh, Syam Kumar Pasupuleti [10] the problem of data integrity authentication for the client's data residing on a (CSS) Cloud Storage Server was defined. The authors offered an improved Chameleon Authentication Tree to implement effective fine-grained and fine-grained dynamic-data update tasks on the data kept on cloud.

In 2017, Muhamed Jasim TK, Mitha Raj, Pinky Mohan, Janeeba Sherin [11] Steganography, Cryptography and Watermarking methods can be used to gain secrecy, security, authenticity and privacy of data. Steganography hides the data in a medium such as audio, video, text file, image etc., and conceals the very existence of the message in the medium. QR code is a two dimensional bar code capable of encrypting different types of data like alphanumeric, Kanji, binary, numeric and control code. Cryptography encodes the message and creates it unintelligent and unreadable form called "cipher". A portion of long multilingual text, an automated SMS message, a linked URL, just about any information can be embedded into the QR code or a business card.

In 2017, Dr.Ramalingam Sugumar, K.Arul Marie Joycee [12] Cloud computing has been proposed as the following generation of utility / distributed computing. It is defined as a model for permitting convenient, on- demand network access to a mutual pool of configurable computing resources examples are networks, servers, storage, applications, and services that can be quickly provisioned and or unrestricted with minimal management effort service provider interaction.

In 2017, IhssanAlkadi, Sarah Robert, [13] Steganography has been considered to be a standard way of sending secret data to the receiver without others being able to identify its immediate presence. Cloud computing has been competitive in fields like cost reduction, flexibility and optimal resource utilization. there is an effort taken to embed Steganography and Cloud Computing, so that, the security level of both can hold together and create a greater safety standard. The pixels are inverted and sent to Five Modulus Method (FMM) or Genetic Algorithm based mostly Steganography exploitation separate Cosine function Transformation (GASDCT) formula supported its size and complexity; Steganography the steganography image is then transmitted to the receiver using the SaaS infrastructure. Using the Software as a Service (SaaS) Document Management, the image is stored, and shared to the receiver, which reduces the extra steps of upload and download, sending via email or any other meaning of communication. SaaS is Cost-efficient, secure, and scalable. Hence an efficient usage of its security and resources to create a system that can handle them in Cloud without any necessity to download an application to the network.

In 2017, Dr. R. Sugumar, K. Arul Marie Joycee, [14] DSCESEA Technique to improve the classical encryption procedures by adding transposition cipher and substitution cipher. It's used first stage the plain text is converted into corresponding ASCII code i.e. Hexa value of each alphabet, key value range among 1 to 256. This algorithm is used in order to encode the data of the user in the clouds. Users can store data on demand or for the applications without keeping any local copy of the data on their machine. Since the user has no control over the data after his/her session is logged out, the encryption key play the very significant role and its primary authentication for the user.

In 2018 A Venkatesh, Marrynal S Eastaff, [15] Cloud computing is the mixture of many preexisting technologies that have matured at dissimilar rates and in dissimilar contexts. The objective of cloud computing is to permit users to take advantage from all these technologies.

III. PROPOSED WORK

1. The project aim is a Decentralized server to deal with the user based control access mechanism to access process cloud data.The system mainly deals with the third party security server to achieve a fully secured cloud computing for virtualization. The third party server to decide the encryption logic to record data on the cloud to provide OTP (One time password) to access cloudPublic user and private user able to upload data in cloud.User based authentication Means that public user can upload and download the file and private user is authenticated user able to upload download file and share file among private users

Public User

- To upload data (Files) in cloud. Choose file, it will be in plain text format. After choosing file converting pain text file into cipher text using AES or Blowfish Algorithm.
- To download data (file) from cloud user will choose the file name. OTP will send on user's email to download chosen file from the cloud.
- OTP will generate using SHA-1 random key generation Algorithm.
- User will enter OTP.
- If OTP match then file will download from the cloud in plain text. (Original format).

Private User
Registration

- Private user will register. To verify authentication of private user send OTP on email. OTP match the able to process further to access the service of cloud.
- Able to share file in cloud with authenticated user. While sharing file with authenticated user. It will also send OTP as well as color code image on file receiver's email for downloading that shared file.

Color Code Image

COLOR-CODE	
RED/red	0
YELLOW/yellow	1
GREEN/green	2
SKYBLUE/skyblue	3
VIOLET/violet	4
PURPLE/purple	5
BLUE/blue	6
ORANGE/orange	7
NEVYBLUE/nevyblue	8
WHITE/white	9

Figure. 2: Color Code Combination

For Example to download share file receiver will receive color code number: 220146 Then to download that file user need to insert color code First letter and generate code GGRYVB and enter that code if it matches then file download.

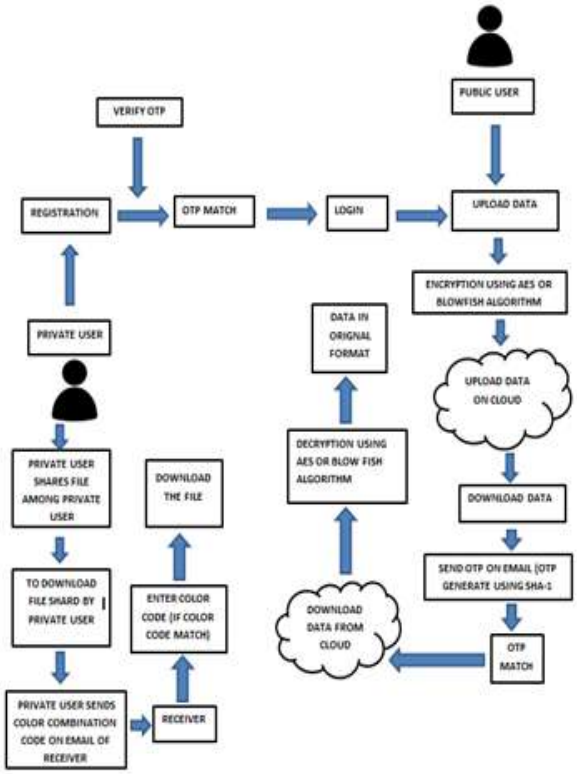

Figure. 3: Architecture of Private User and Public User Models Using AES or BLOW FISH Encryption and Decryption

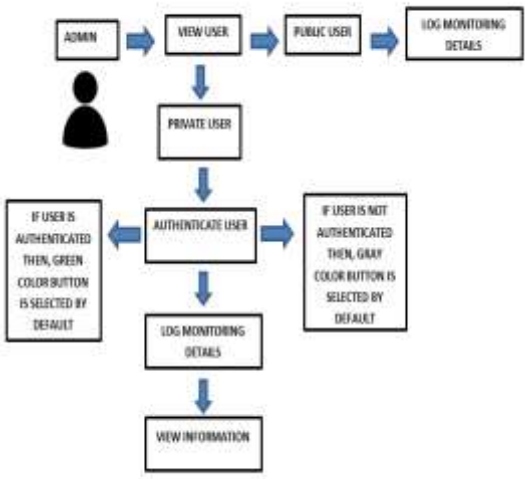

Figure. 4: Architecture of Admin Model Using AES or BLOW FISH Encryption and Decryption.

Algorithm & Techniques
1.SAH-1

- SHA-1 random key generation algorithm is generating random key OTP (one time password) for accessing (downloading) file from the server.

2.AES Algorithm (Public User)

- Applied AES encryption algorithm to upload file on cloud in encrypted format.
- AED Description algorithm applied while downloading file from the cloud so content will be visible in the original format.

3.Blowfish Algorithm (Private User)

- Applied Blowfish encryption algorithm to upload file on cloud in encrypted format.
- Blowfish Description algorithm applied while downloading file from the cloud so content will be visible in the original format.

Comparison of Algorithm:

● **lgorithms Parameters**	● **AE S**	● **B lowfish**
● ey length(Bit)	● 128 /192/256 bits	● V ariable key length i.e., 33-448 bits
● ounds	● 10/ 12/14	● 1 6
● lock size (Bits)	● 18	● 6 4
● ncryption speed	● Fas ter	● V ery fast
● ower consumption	● Hig her than Blowfish	● V ery low
● evel of security	● Exc ellent	● H ighly secure
● hrough put	● Lo wer than Blow fish	● V ery high
● omplexity	● Les s	● L ess than AES
● ecurity against	● Ch osen plain, known plain text	● D ictionary attacks ●

Table 1 : Comparison of Algorithm.

IV. ADVANTAGES:

1) The main advantage of cloud computing for health care is that the clouds create it far easier to record and use patient records and his/her medical images.
2) The data also befits more accessible from numerous locations, and though something occurs on-site, the data is still conserved.
3) Several business management applications like client relationship management and enterprise resource coming up with are supported a cloud service supplier.
4) Software as a Service has become a popular approach for deploying enterprise level software system. Sales force, Hub spot, Market are popular examples of this model. It ensures trouble free management, Maintenance and security of your organization's crucial business resources and permits you to access these applications handily via an internet browser.
5) The cloud conjointly delivers extra flexibility within the sense that you just will relish huge storage and on demand backups.
6) Recovery is also implemented faster in the cloud because the data is kept over a network of physical servers afore at one on-site data centre. Amazon S3, Google Drive and Drop box are widespread examples of cloud backup solutions.
7) Using cloud, you will be able to modestly create scalable cross-platform experiences for your users. Amazon work may be a shared mobile game development tool utilized in the cloud.
8) These platforms embrace several pre-coded tools and libraries like directory, search, services and security. This can get faster and modified the event process.
9) This protects the technical team from securing budgets and disbursal crucial project resources and time.
10) It is that the preferred and sometimes unnoted application of cloud computing. LinkedIn, Myspace, Twitter, Facebook and lots of alternative social networking sites use cloud computing.

V. CONCLUSION

We present Securing Cloud for Enhancing Privacy, User Based Access Control Mechanism. Our approach is to provide secure cloud for the users to upload and download data from the cloud. To download data from the could authenticated user will be getting OTP. User need to enter the OTP and after that able to download the file. User base access control and we are preserving user's privacy. Set privileges for public users and private users. To keep data secure on cloud we use AES and Blowfish algorithm.

REFERENCES

[1]. Amazon data center size.http:// huanliu.wordpress.com/2012/03//amazon-data-center-size.

[2]. AL.Jeeva,Dr.V.PalanisamyandK.Kanagaram "Comparative Analysis Of Performance potency And Security Measures Of Some coding Algorithms" International Journal Of Engineering analysis And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, pp.3033- 3037, May-Jun 2012.

[3]. RachnaArora, AnshuParashar, " Secure User Data in Cloud Computing Using Encryption Algorithms,"

In International Journal of Engineering Research and Applications, Vol 3, No. 4, pp.1922- 1926, 2013.

[4]. MandeepKaur, Manish Mahajan, "Using encryption Algorithms to enhance the Data Security in Cloud Computing," In International Journal of Communication and Computer Technologies, Vol 01, No. 12, 2013.

[5]. Kan Yang and XiaohuaJia, ―Efficient and Revocable Data Access Control for Multi-Authority Cloud Storage ―, in IEEE Trans. Parallel Distributed System, vol 25, No.7, pp 1735- 1744, July 2014.

[6]. S DivyaBharathy et al,International Journal of Computer Science and Mobile Computing, Securing Data Stored in Clouds Using Privacy Preserving Authenticated Access Control Vol.3 Issue.4, April-2014.

[7]. R.Ranjith, S.Murugaanandam Department of IT, SRM University, Privacy Preserving Authenticated Access Control with Decentralized Key Management in Clouds (IJEDR , Volume 2, Issue 1 ,2014

[8]. RachanaChavda, RajanikanthAluvalu, "Encryption Based Access Control Model in Cloud," In Journal of Telematics and Informat- ics, Vol 3, No. 1, pp. 15~21, 2015.

[9]. PriyankaOra, P.R.Pal, "Data Security and Integrity in Cloud Computing Based on RSA Partial Homomorphic and MD5 Cryptography," In IEEE International Conference on Computer, Com- munication and Control, 2015.

[10]. AnirudhaPratap Singh, Syam Kumar Pasupuleti, (2016). Optimized Public Auditing and knowledge Dynamics for knowledge Storage Security in Cloud Computing. 6th International Conference on Advances in Computing & Communications, Procedia Computer Science 93-2016

[11]. MuhamedJasim TK, Mitha Raj,Pinky Mohan,JaneebaSherin(2017) Efficient Security of Data By QR Code Encryption & Steganography IJIRST –International Journal for Innovative Research in Science & Technology| Volume 3 | Issue 12 | May 2017

[12]. Dr. RamalingamSugumar , K.Arul Marie Joycee, "Ensure and Secure Data Confidentiality in Cloud Computing Environment using Data Obfuscation Technique", International Journal of Advanced Studies In Computer Science and Engineering , Volume 6, Issue 12 ,December 31 .2017.

[13]. IhssanAlkadi, Sarah Robert,"Application and Implementation of Secure Hybrid Steganography Algorithm in Private Cloud Platform", journal of computer science applications and information technology, Received: October 12, 2016; Accepted: October 16, 2016; Published: January 20, 2017.

[14]. Dr. R. Sugumar, K. Arul Marie Joycee,"DSCESEA: Data Security in Cloud using Enhanced Symmetric Encryption Algorithm" International Journal of Engineering Research & Technology, Vol. 6 Issu 10, October – 2017.

[15]. A Venkatesh, Marrynal S Eastaff, A Study of Data Storage Security Issues in Cloud Computing International Journal of Scientific Research in Computer Science, Engineering and Information Technology,Volume 3 Issue 1,2018.

Shubham S. Chourasiya" Securing Cloud by Enhancing Privacy Preservation and User Based Access Control Mechanism" International Journal of Engineering Research and Applications (IJERA), Vol. 09, No.02, 2019, pp. 53-58