iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** III **Month of publication:** March 2019

DOI: http://doi.org/10.22214/ijraset.2019.3203

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

Three-Layer Privacy Preserving Cloud Storage Scheme based on Computational Intelligence in Fog Computing

Dr. M. Preetha[1], G. Pravinkumar[2], S. Sabarinathan[3]
[1]*Associate Professor,* [2, 3] *UG Student, S.A. Engineering College*

Abstract: ***Now a days the cloud computing has been widely used in day to day life. Every type of data is stored in the cloud and it can be easily accessed in at any time and any place. But, while coming privacy in the cloud computing is stepping behind due to location awareness. So we are introducing three layer privacy preserving cloud storage scheme using fog computing. Using this scheme we partition the complete data into three part of data. Each of the data is encrypted and stored in the three layer cloud.by this method we can overcome the location awareness and protect the data. To recover the lost data from the cloud we introduce the bucket. Lost data can be recovered and complete data can be obtained.***

Keywords: Cloud Computing, Cloud Memory, Confidentiality, Confidentiality-Preserving, Fog Computing.

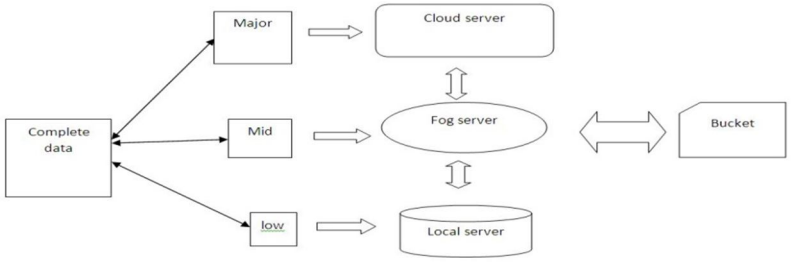
I. INRODUCTION

Confidentiality is a basic for strong confidentiality security in all online computing sides, but confidentiality alone is not satisfies. Companies and customers are ready to use online computing only if they have the belief that their data will stay confidential and safe. Thus to produce a trusted surrounding for customers, we need to create a software, assist and works with confidentiality in mind. The location of physical assets and accessories being allowed in general doesn't known to the particular user. It also affords services for user to form up, use and maintain their data in the applications on the cloud, which maintains and manages the virtualization of assets by itself. Cloud memory is a method of networked online memory in which the data is stored in virtual group of stash that is generally being introduced by the third person. Cloud memory makes data stored remotely to be limitedly cached on mobiles, PC or other Internet connected devices. Confidentiality and cost are the barriers in this field, depending on the dealers. Although the first achievement and identification of the cloud model and the broad availability of producers and tools, a number of trials and prospects are intuitive to this new design of computing. The notion of confidentiality in cloud memory and the confidentiality challenges in cloud memory is presented in Section II. Section III presents the possible solutions for confidentiality problems in cloud memory. This section gives a brief introduction about the traditionally available confidentiality and unity mechanisms and further divisions the existing confidentiality-preserving methods.

II. PROPOSED WORK

A.Three Layer Privacy

Now the cloud server is divided into three different layers for ensuring the security purpose and to avoid the location awareness. The three different privacy preserving layers are Cloud server, Fog server and Local server. A complete data is now partitioned and stored into three different layers. The ratio of the partition of data is major part of the data is stored in the cloud server, neither high nor low range of data is stored in the fog server and finally lower amount of local server. When the data required it can be combined into a single data using pattern matching method.



Three-layer privacy preserving cloud storage architecture

©IJRASET: All Rights are Reserved

B. Encryption

While uploading the data in three layers, first it is encrypted using Hash Solomon algorithm of encryption. The original data is combined with appending bit and it is encrypted. Now the encrypted data is stored in three layers. When the user requires the complete data, it is decrypted first and combined with the other parts and given to the user as a complete original data.

C. Fog Computing

Fog computing is familiar with cloud computing. It consists of low latency and increasing the geographical range of distribution. Fog computing can perform the data processing and limited storage capabilities. Fog computing consist of three-level architecture, the uppermost is a cloud computing layer, it can be used as storing data and computing data. The middle layer is the fog computing layer. Fog computing layer can perform critical data transmission to cloud server. And finally the third layer is wireless sensor network layer. This layer's main job is to collect data and upload it to the fog server. In addition, the rate of transfer between the fog computing layer and other layers is faster than the rate between the cloud layer and the lower layer.

III. LITERATURE SURVEY

A. A Secure Data Privacy Preservation For On-Demand Cloud Service

This paper is focus on privacy and security of data stored in the cloud. They albeit computing is introduced to provide to increasing its efficiency, optimization and effectiveness of the cloud environment. Thus author introduce Privacy Preserving Model to Prevent Digital Data Loss in the Cloud. This proposal helps the Cloud Requester/Users to trust their proprietary information and data stored in the cloud.

B.Privacy-Preserving Security Solution For Cloud Services

This paper is based on the privacy-preserving security solution for cloud. It based on the signature scheme for the nonbilinear group providing the unidentified access to the cloud server and shared storage server. It makes Unidentified Authentication for the registered user.

The user personal information can be displayed without revealing the user detail. However any illegal activity is found, the user rights in the cloud server can be revoked. Author proposed work helps to

Anonymous access, unlinkability and data transmission confidentiality.

C. An Efficient Public Auditing Protocol With Novel Dynamic Structure For Cloud Data

This paper is based on the efficient method of making the structure of the data. Author proposed public auditing scheme in which dynamic operation can be performed. Hashing can be performed in this method. Using Merkle Hash Tree the dynamic data operation can be performed. Ring signature stores the information of the user.

D. On A Relation Between Verifiable Secret Sharing Schemes And A Class Of Error-Correcting Codes

This paper explains about the Verifiable Secret Sharing Schemes. Using the metric author forms a set of codes known as set of error correcting codes. Then they consider the burst error interleaving codes introduces the efficient burst error correcting scheme. By this methods error correcting and secrete sharing of files can be performed.

E.Security And Privacy Of Ensitive Data In Cloud Computing: A Survey Of Recent Developments

This paper represents the Available technologies and a broad collection of

Created and implementation of projects on cloud confidentiality and security. This paper are arranged based on the available works based on the cloud architecture ,Management of resources and cloud work management layers, along with the recollection of the developments that available in privacy preserving confidential data in cloud computing.

F. A Survey On Cloud Security Issues And Techniques

This paper explains about some of the security issues in cloud in various aspects like

Insider attacks, Outsider attacks, Loss of control, data loss, multi tenancy, Network security, elasticity, and availability. It also consists of available security schemes and method for a securing cloud. This paper will deliver the idea about different security issues and tools to the researchers and professionals.

©IJRASET: All Rights are Reserved

G. Security And Privacy Preservation Scheme Of Face Identification And Resolution Framework Using Fog Computing In Internet Of Things

In this paper, used the face recognition in the three layer privacy in cloud computing using fog computing in internet of things. Using the face recognition the data present in the three layers are kept encrypted and secured. Only the authenticated person can open the data in the server. Face recognition is implemented in each layer. It helps to ensure security and privacy in the cloud computing.

H. A Secure Data Privacy Preservation For On-Demand Cloud Service

This paper describes about the portability issues in the cloud environment, the users can have their account information and details including respective cloud providers. Noisy disturbance in the valued data information of cloud, initiate a scheme to abort privacy leakage. Petri net models introduced as a modern tool for to do our own system that tells about concurrency and synchronization. The process is to develop the distributed theories as well as techniques. It is used to analyze the quantitative and logical processes.

I. A Survey On Secure Storage Services In Cloud Computing

This paper proposes a system that has the transparency concept, which is the appropriate disclosure of the aspects of security or government design, practices and policies. Using AES the encryption will be done to secure the data. This involves a policy that might state that, the user data protects the data from unauthorized access to transmit. It includes a POR protocol that encrypts the data and embeds a set of the randomly-valued blocks by randomly called sentinels. By encryption it renders the sentinels as indistinguishable from the other blocks. It has PDP that provides the probabilistic proof for the third party to stores a file. This model allows the server to access the small portions of the file.

J. On Sharing Secrets And Reed-Solomon Codes

This paper explains about the encryption and decryption of data. It helps to secure the data from the third party user to see data. The size and content of the data may varies due addition of padding bits. Only the Authentic user can decrypt the data to its original form using hash Solomon algorithm. By this method the security and privacy of the data can be ensured.

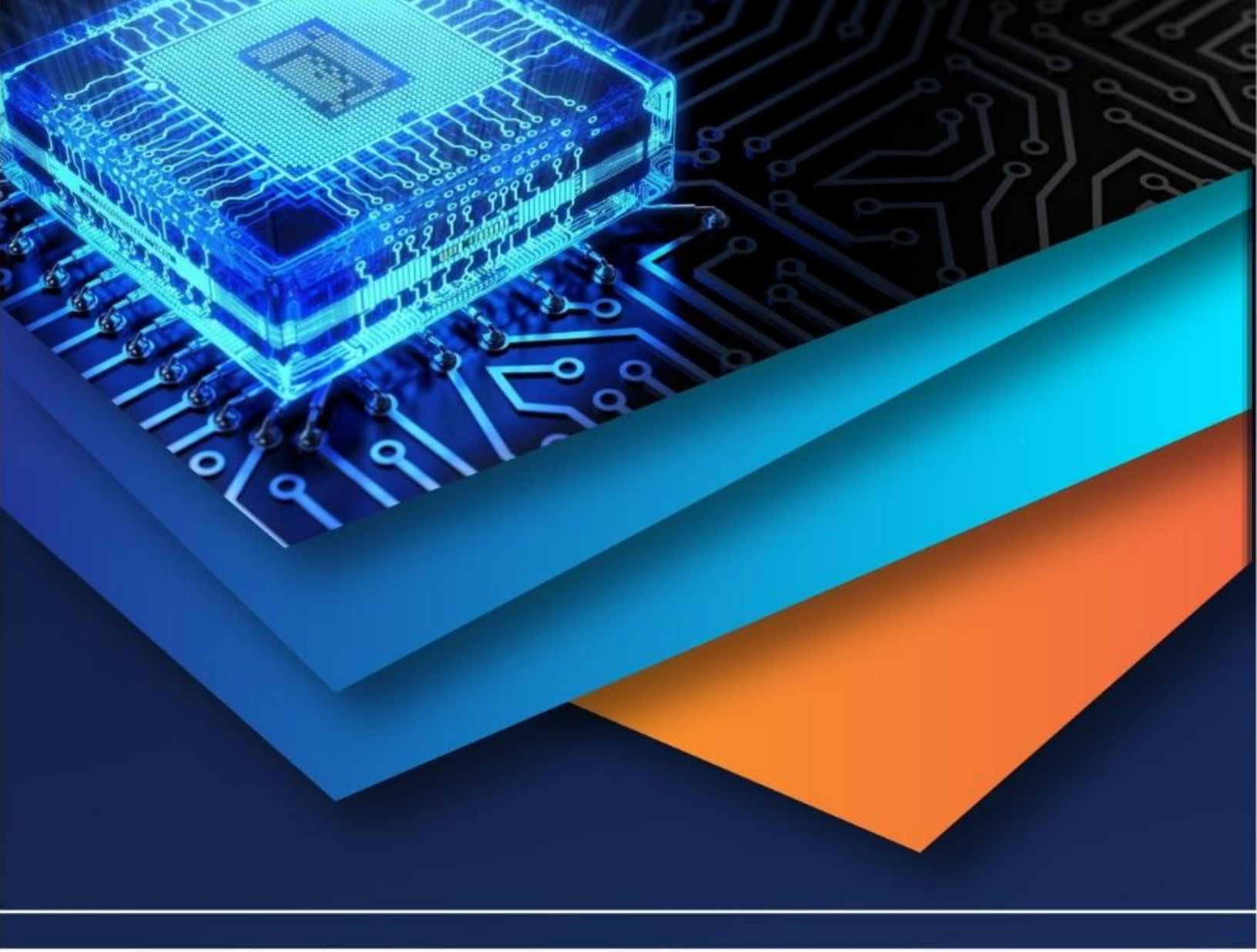
IV. CONCLUSION

Cloud Computing makes the computer world has a wider range of uses and enhances user - friendliness by providing access through any type of internet connection. Even with this increased ease of use also some drawbacks. Confidentiality is to be considered very important and is a key issue for cloud memory. A variety of techniques that can be used in order to ensure confidentiality have been mitigated. This paper has discovered some confidentiality ways for avoiding the problems in confidentiality on unsecured data stores in cloud. There are still some approaches that are not addressed with in this paper. This paper makes difference in the methodologies in the literature is based on encryption methods, based on access control Mechanisms, keyword search schemes, query integrity and Adaptability schemes. The work is making efficient confidentiality-preserving memory

REFERECES

[1] Rajathi, N. Saravanan, A Survey on Secure Storage in Cloud Computing
[2] Ali Gholami, Erwin Laure, SECURITY AND PRIVACY OF SENSITIVE DATA IN CLOUD COMPUTING: A SURVEY OF RECENT DEVELOPMENTS
[3] An Efficient Public Auditing Protocol with Novel Dynamic Structure for Cloud Data and a Class of Error-Correcting Codes
[4] Chandramohan Dhasarathan , Vengattaraman Thirumal, Dhavachelvan Ponnurangam, A secure data privacy preservation for on-demand cloud service
[5] Garima Gupta, P.R.Laxmi, Shubhanjali Sharma, A Survey on Cloud Security Issues and Techniques
[6] L. Malina, J. Hajny, P. Dzurenda, V. Zeman, Privacy-preserving security solution for cloud services
[7] Ms. B.Tejaswi, Dr. L.V.Reddy , Ms. M.Leelavathi, A Survey on Secure Storage Services in Cloud Computing
[8] Pengfei Hu, Student Member, IEEE, Huansheng Ning, Senior Member, IEEE, Tie Qiu, Senior Member, IEEE, Houbing Song, Senior Member, IEEE, Yanna Wang, and Xuanxia Yao
[9] R.J. McEliece, D.V. Sarwat**e,** On Sharing Secrets and Reed-Solomon Codes
[10] Ventzislav Niko, Svetla Nikova, On a Relation Between Verifiable Secret Sharing Schemes

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)