Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Environment in Cloud Computing: Privacy Preservation and Security Solutions

J.Sumitha[1], V.Padmaja[2], R.Vaishnidi[3]
[1](Assistant Professor, Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore, India
Email: sumithaj@skasc.ac.in)
[2,3] (PG Students, Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore, India
Email: padmajav16mss029@skasc.ac.in, vaishnidir16mss052@skasc.ac.in)

****

Abstract:

The security problem for cloud computing including memory security, information security, arranges security and secure representation. Specifically we talk about the blueprint for outsider of record in a cloud. The utilization of making sure about co-processor for cloud computing is examined. The structure confided in application from untrusted part will be the significant parts of made sure about cloud computing is acknowledged. So the research work is focused on analysing the qualities of cloud computing condition. The main role of cloud computing architecture is to preserve the privacy of the data ensuring that it cannot be misused. So the cloud security is designed to address the client protection issue in a cloud.

Keywords **—** Cloud Computing, Security Issues, Privacy Preserving, Cloud Techniques.

****

I. INTRODUCTION

The development of cloud and putting away information in it has gigantic advantages. It encourages the verified and approved cloud clients to get to gigantic assets that are redistributed and partaken in the cloud. At whatever point required, the user can ask for and gain the entrance in a simple manner and easily, regardless of the user area. Additionally, cloud computing removes the cost spent on introducing all equipment and programming, by permitting user to lease the assets dependent on their requirements. Regardless of every one of these advantages, cloud computing despite everything faces numerous difficulties which preclude the effective execution of the cloud. These incorporate both the customary just as cloud security challenges. Explicit to cloud computing, the issues are many, of which some are: character the board of cloud clients, multi-occupancy support, making sure about the security of uses, protecting security of the user, achieving authority over the existence pattern of redistributed information, and so forth.

II. CLOUD COMPUTING USES

The cloud uses better utilization and security aspects which alludes to applications and administrations that sudden spike in demand for a conveyed organizer and utilizing the virtualized assets to go by regular internet conventions and systems administration gauges. T is distinguished by the notion that resources are virtual and limitless and whichever details of the physical systems the software runs are abstracted from the user. Cloud computing is fundamentally separated into three fragments: “application”, “storage” and “connectivity”.

Each portion fills a different need and offers various items for organizations around the world. In cloud computing, resources are given as a utility over the internet to customers who use them as when required premise. The same number of associations re-appropriating their information to the cloud, they need it to be guarantee and private. What’s more, instead of re-appropriating our information to the cloud server, we have to give security to it. Hence, security is a greatest worry of user when utilizing cloud computing. Security objectives of information incorporates Authentication, Authorization, Auditing, Confidentiality, Integrity, Availability and Nonrepudiation.

A. Privacy Preserving Methods

1) Anonymity based approach

To achieve and preserve privacy in cloud Jiang Wang et al. make use of Anonymity based method. Before releasing the data in cloud, the anonymity algorithm involves in processing the data and anonyms entire data or few information. To mine the specified knowledge cloud service provider utilize its background information and associate the specifics with the anonymous data. For preserving users privacy this methodology differentiate from the classic form of cryptography technique, The anonymity algorithm get rid of key managing process because of this reason it showcase as simple and versatile. The anonym sing is quiet simple because, anonymous varies according to the attributes and it is based on cloud service provider. Only finite number of services helped for this approach .This approach would be better if it is based on automating the automization.

2) Architecture of Privacy Preserving

The anonymity algorithm involves in processing the data and anonymized whole data or few information. To mine the specified knowledge cloud service provider utilizes its background information and associate the specifics with the anonymous data. For preserving users privacy this methodology differentiate from the classic form of cryptography technique, The anonymity algorithm get rid of key managing process because of this reason it showcase as simple and flexible. The anonymizing is quiet simple because, anonymous varies according to the attributes and it is based on cloud service provider. Only finite number of services supported for this approach. This approach would be better if it is formed on automating the automization.

3) Access control for privacy preserving

Certain type of attributes linked with every cloud user that determines their access rights. Two tier encryption model is introduced in this paper where the root phase and surface phase builds up the two tiers of the model. In the first phase local attribute-based encryption takes place on the outsourced data by the info owner. Contrastingly, surface phase process involves where operation done by cloud servers, afterwards the initialization completed by the data owner. Server re-encryption mechanism (SRM) performs by the surface phase. The encrypted data within the cloud is dynamically re-encrypted by the SRM during the info owner request. Either a different user has to be created or an existing cloud user has to be repealed when the request for SRM given. The access policies remains hidden to the cloud server so the security of user data is not agreed because however the re-encryption going to take place in cloud server. In this manner privacy of data is preserved by giving complete access manage to the data owner and by not allowing the cloud provider to learn information about the stored data.

4) Authorization system for privacy preserving task

David W. Chadwick et al. introduced a policy for the intention of privacy preserving of users data that is based on authorization infrastructure for the cloud .Access policies can be define by user itself and users data also be attached with it. Byaccomplishing this process assuring the controlled access of data in cloud. For making and enforcing authorization decision, Policy Decision Points (PDPs) and Policy Enforcement Points (PEPs) are used. Commenced master PDP is used to figure out and solves the issues among different decision of PDPs. Obligation service act as a piece of authorization substructure, because of this process the info owner is indicated regarding the access of authorized and unauthorized data access. Cloud provider is trusted by the authorization substructure and deal with the problems that enter by means of outsider. If the encryption of deployed data has not done properly even after trusting the cloud provider.

5) *Dynamic Metadata reconstruction*

In cloud overall chance of metadata exploitation is focused by AdeelaWaqar et al. There are chances of exposing users' privacy by attacker by means of retrieving knowledge of the metadata. To preserve data privacy a framework is proposed. For this reason, the initiative is that the metadata in cloud has got to be separated then the separated data are grouped into a nonpublic form. Based on the sensitivity of data, Groups are divided into partially private and non-private form. The next phase is table splitting, in which the database table has two splitting namely horizontal and vertical splitting. Database normalization is ensured by the splitting of the table database. The next phase is ephemeral referential consonance where metadata reconstruction can be take place when required by the cloud. This phase ensures that no data leakage occurs before and after splitting of database table. Thus this method proves to be efficient.

6) *Public auditing for protected data storage*

In cloud overall possibility of metadata exploitation is focused by AdeelaWaqar et al. There is chances to compromise user's privacy by attacker by means of retrieving knowledge of the metadata. To preserve data privacy a framework is proposed. For this reason first step is the metadata in cloud has got to be separated then the separated data are grouped into a private form. Based on the sensitivity of data, Groups are divided into partially private and non-private form.

The next phase is table splitting, in which the database table has two splitting namely horizontal and vertical splitting. Database normalization is ensured by the splitting of the table database. The next phase is called ephemeral referential consonance where metadata renovation can be take place when required by the cloud. This phase assures that no data leakage occurs before and after splitting of database table. Thus this method proves to be efficient. By improving the security strength of data storage.

III. SECUTITY ISSUES AND SOLUTION

A. *Trust*

Trust among customer and service organizations is the principle issue looked by cloud computing now days. Customer is never certain whether the Service is dependable or not, and whether his information is secure from the gatecrashers or not. The Customer and Service supplier are limited by Service Level Agreement (SLA) record. This is a kind of an understanding between the Customer and the specialist co-op; it contains the obligations of specialist co-op and his likely arrangements. However, tragically there are no models for SLA.

B. *Confidentiality*

Confidentiality intends to forestall the exposure of private and significant data. Since all the data is put away on topographically scattered areas, secrecy turns into a major issue. Numerous techniques are utilized to safeguard secrecy from which, encryption is the broadly utilized strategy. In any case, it is moderately a costly strategy.

C. *Authenticity*

Integrity is a primary issue looked by cloud computing. It alludes to the inappropriate alteration of data. As the information dwells in better places in a cloud so the entrance control instrument ought to be secure and every client must be checked as a credible user. Authentication problem can be settled by utilizing the advanced marks however considerably subsequent to approaching computerized marks a user can't get to and confirm the subsets of information.

D. Encryption

Encryption is the most broadly utilized information making sure about strategy in cloud computing. It has numerous disadvantages. It needs high computational force. The encoded information should be decoded each time when a question is run so it lessens the general database execution. Numerous strategies are introduced to guarantee better encryption regarding better security or the activities. A technique proposed by recommends that by utilizing a few cryptographic strategies rather than just one can build the general throughput. Information is encoded utilizing these strategies in every cell of a table in cloud. At whatever point a user needs to make an inquiry, the question parameters are assessed against the information put away. The inquiry results are likewise decoded by the client not simply the cloud so it builds the general execution.

E. Key Management

While doing encryption, we need encryption/decryption keys and dealing with these keys itself is a major security issue in cloud condition. Putting away these encryption keys on cloud is a terrible alternative. It is anything but difficult to store single encryption key however for the ongoing frameworks it become an intricate errand to store these keys. This may require a different little database to store the keys locally in a secured database. Yet, again that is not a smart thought on the grounds that the reason for which we are moving our information to mists will get useless.

F. Data Splitting

Data Splitting might be the better option in contrast to encryption. It is without a doubt quick when contrasted with encryption itself. The primary thought behind it is to part the information over different hosts that are non-communicable. At whatever point a user needs its information back, he should approach both of the specialist co-ops to recall his unique information. Almost certainly it is exceptionally quick strategy however it has its own security issues.

IV. CLOUD COMPUTING SECURITY ISSUES

In past few years, cloud computing has developed to one of the quickest developing sections of IT industry. However, this development need cloud security to be unblemished. Beneath referenced are hardly any most significant issues of cloud computing.

A. Privacy

The Cloud computing uses a virtual registering innovation. Right now, information is kept on different virtual server farms which may cross universal limits. This is the place information security assurance may confront discussion of different legitimate frameworks.

B. Security

Where is your information increasingly secure, on your nearby hard driver or on high security servers in the cloud? Some contend that customer information is increasingly secure when overseen inside, while others contend that cloud suppliers have a solid motivating force to keep up trust and as such utilize a more significant level of security. In any case, in the cloud, your information will be conveyed over these individual PCs paying little heed to where your base storehouse of information is eventually put away Reliability: Server in the cloud have indistinguishable issues from your own occupant servers. The cloud servers likewise experience personal times and lulls, what the thing that matters is that clients have a higher reliant on cloud specialist organization (CSP) in the model of distributed computing. There is a major contrast in the CSP's administration model, when you select a specific CSP, you might be secured, consequently bring a potential business secure hazard.

C. Open Standard

In cloud computing, open guidelines are basic to develop. Numerous CSP gives very much reported

APIs which are novel to their execution and along these lines hard to interoperable. Towards the advancement, there are many open gauges are a work in progress; OGF's Open Cloud Computing Interface is one of them.

D. Long Term Viability

It should be the information you put into the cloud will never become invalid even your cloud computing supplier go belly up or get obtained and gobbled up by a bigger organization. "Ask potential suppliers how you would recover your information and on the off chance that it would be in an arrangement that you could bring into a substitution application.

E. Compliance

Numerous guidelines relate to the capacity and utilization of information require customary detailing and review trails, cloud suppliers must empower their clients to consent fittingly with these guidelines. Overseeing Compliance and Security for Cloud Computing, gives understanding on how a top-down perspective on all IT assets inside a cloud-based area can convey a more grounded administration and authorization of consistence strategies.

V. CONCLUSION

Cloud computing is an innovation which has been utilized efficiently by purchasers to store and offer information the place security and protection is the principal concern. It diminishes client troubles and guarantees the information integrity. Additionally this strategy used to settle the security strings. Different approach to comprehend the issue is that are forestalling the protection conservation or likewise examinations. In future, this proposed model could be utilized to get the ensured distributed computing condition which would be an incredible improvement in the privacy preservation.

REFERENCES

1. Kundu, C. D. Banerjee, P. Saha, “Introducing New Services in Cloud Computing Environment”, International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143- 152, 2010.
2. Lizhe Wang, Jie Tao,Kunze M., Castellanos A.C., Kramer D., Karl W., “Scientific Cloud Computing: Early Definition and Experience,” 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825- 830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.
3. R. L Grossman, “The Case for Cloud Computing,” IT Professional, vol. 11.
4. http://www.interoute.com/cloud-article/what-hybrid-cloud
5. Messmer, Ellen (March 31, 2009). "Cloud Security Alliance formed to promote best practices". Computer world. Retrieved May 02, 2014
6. "Security Guidance for Critical Areas of Focus in Cloud Computing". Cloud Security Alliance. Retrieved May 02, 2014
7. https://vdocuments.mx/public-auditing-and-user-revocation-in-dynamic-cloud-environment.html
8. https://www.irjet.net/archives/V7/i2/IRJET-V7I2348.pdf
9. http://www.jetir.org/papers/JETIR1906824.pdf
10. https://www.ijser.org/onlineResearchPaperViewer.aspx?Privacy-Preservation-of-Cloud-Storage-Data-using-Classification.pdf