Data Security Issues and Mechanisms in Cloud Computing

Pratyusha.T, B.M.G. Prasad

ABSTRACT: Now a day's due to rapid growing of cloud storage many users are outsourcing their data to the cloud but cloud owing security challenges so outsourced data is not secure, the goal this paper is to recommend new mechanism or framework that should overcome all the existing limitations, first to understand security issues in cloud storage this paper reviews various authors work and from that it finds the problem statement and limitations, so in order to overcome the security issues security framework is recommended and it should include secure data auditing, access controls, efficient key management and Secure Multiparty Computation.

KEYWORDS: CSP, data security, ABE, Access controls, Data integrity.

I. INTRODUCTION

IT as a service has grown phenomenally popular current years. The main intention for extension was hope to reduce capital and operating responsibilities also capability to mount and dynamically distribute new services without having to maintain a dedicated computing infrastructure. As a result, cloud computing has quickly started transforming way associations observe their computing sources. So an outline of a particular system contains a unique operating system (OS) and a separate application, companies become turned to a cloud, wherever sources are accessible in plenty and where user possesses a full limit of choices. Cloud is a new concept of IT service provision and largely meets the new IT requirements. It becomes proven a prominent gain to users and groups because significantly diminish accounts provide help survive IT systems outwardly problems. Because of its many advantages, the cloud has repeatedly utilized in various fields such as banking, e-commerce, retail and universities. Besides, cloud computing reduces the investment risk for IT companies. However, cloud is changing established service practices of IT service administration. Presently cloud, information administration services run local customer conditions served remote CSPs. Although section has plenty possible benefits over rigid computer systems, the provision of large data warehouse capacity, high-performance assistance at economical charge, users scared of wasting limitation of their data. In sessions of an essential feature of cloud. In addition, CSPs are plentiful weak to opponents or hackers who can employ them to reap privileges. The cloud is exposed regarding data security, secrecy and confidentiality because sensible user data is collected in a third-party CSP. Data encryption can simply solve privacy and integrity issues, but to embrace the cloud to a large extent, it is required to build a business association between cloud service providers and users.

II. LITERATURE REVIEW

[1] Cloud computing is the long-term vision of computing as a utility, where users can save their data remotely in the cloud to take the position of high-quality on-demand applications and co-operation from a cloud. A shared collection of configurable computing devices. With the outsourcing of data, users can free themselves from the warehouse and the preservation of historical data. Nevertheless, the fact that users no large have physical ownership of the possibly large size of outsourced data makes data integrity assurance in cloud computing a questionable and potentially formidable task, particularly for users with capacity and resources. Restricted computers Therefore, it is essential to allow public auditability for the protection of data accommodation in the cloud, so that users can use an outer part of the state to verify the integrity of outsourced data when needed.

[2] Cloud computing is a developing computing standard in which IT infrastructure resources presented as settings on the Internet. Although promising, this paradigm also introduces many new challenges before data security and access control when users outsource sensitive data to share on cloud servers, which do not belong to the same domain. Data Owners to support the confidentiality of classified user data against untrusted servers, existing clarifications typically enforce cryptographic techniques by divulging the data decryption keys only to authorized users. However, by doing so, these solutions inevitably precede a massive computational overhead in the data owner for key distribution and data management when detailed data access control is desired and therefore do not add scale well.

[3] In the new cloud computing paradigm, data owners are increasingly motivated to outsource their complex data management systems from local sites to the commercial public cloud for greater flexibility and cost savings. For the consideration of user privacy, confidential data must be encrypted before the external contract, which makes the efficient use of data a very difficult task.

Manuscript published on 28 February 2019.
* Correspondence Author (s)

Pratyusha. T, Research scholar, Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan

Dr. B.M.G. Prasad, Professor, Dep of CSE and Dean PG Courses at Holy Mary Institute of Technology and Science Hyderabad, Telangana

The author presents, for the first time that defines and solves the problem of the request for the preservation of privacy on cryptographic data structured in graphic in cloud computing (PPGQ) and establishes a set of strict confidentiality requirements for a secure system for the use of data in the cloud.

[4] In cloud computing, sensitive data must be encrypted before being outsourced to the server, which introduces a computational overhead for crucial derivation and data administration when dynamic control of hierarchical accesses desired. The author presented, he tackle this complex problem by delegating computing activity, such as re-encrypting data, distributing keys, and referencing servers in the cloud. In our construction we use only bilinear couplings and random padding. An exhaustive analysis shows that the proposed scheme simultaneously reaches scalability and dynamics and shows that it is formally secure.

[5] In recent years, the development of cloud computing has increased the demand for services that provide cost-effective information analyzed by huge data from heterogeneous sources of information. In order to reduce user anxiety about storing private and confidential information in the cloud, various Data Privacy Preservation (PPDM) techniques are developed that enable the cloud to extract data from secure data.

[6] Cloud computing is one of the emerging technologies of the computer industry in recent times. This new technology requires the user to entrust the user's precious data to the cloud server, since the latter has the greatest disadvantage on the security and confidentiality of data outsourced to the server. To overcome this disadvantage, different attribute-based encryption (ABE) schemes are reported for encrypting the user data file and also for controlling access to outsourced data in these cloud server; however, the implementation of access control policies in attribute-based cryptography (ABE) is more complex.

[7] To solve the difficulty that the traditional resource allocation scheme does not take into account the behavior of users in the cloud and that has a static authorization process, the author proposes a resource allocation scheme based on access control (RASBAC), which introduces behavioral trust in the authorization process. . The author designs a behavioral confidence calculation algorithm based on a widespread analytical hierarchy process and presents a new dynamic mechanism for authoring regulation.

[8] Access Control (AC), an essential protection element of cloud hierarchical AC, is particularly interesting because, in practice, we authorized to various admittance rights. The author manifests a hierarchical key designation plan based on extended geometry as a flexible hierarchical-AC solution in cloud. In our schema, cryptographic command connected with private vector, public vector, an internal product of the descending class.

[9] Consistent authorization and admittance administration is one of the urgent difficulties that cloud computing utilization face, especially in the circumstances of the dynamic creation of the entity's trust relationship to study the cloud environment open access security. The author proposes a method to generate a strategy of control of interdomain accesses, from the evaluation of the trust to the management of the trust. Based on the trusted method of inter-domain access control method, an access control system based on trust for cloud computing has designed and implemented.

III. ANALYTICAL RESULTS & DISCUSSIONS

Data privacy important portion for the implementation of cloud. In several opinions, researchers, it has emerged that defense now the primary difficulty to be compact in the cloud. He impersonated various security issues related to cloud computing similar to traditional methods of internal computing. This requires the re-evaluation of the risks associated with respective specific areas in the new uncertain situation, where multiple users share resources as indicated. Depending upon cloud example, the user uses multi-location the security level to change. But outwardly any reservations, the public cloud Infrastructure-as-a-Service (IaaS), the highest risk of all. Numerous security superintendence examples proposals have been planned protect the cloud system. This work meditates on distinguishing security fulminations, arguments their countermeasures to enhance confidentiality, honesty availability (CIA) of data collected in the cloud. This work provides a large scale data security solution and protocol to effectively address the protection and retirement risks inherent in complex and complex cloud computing. Focus on privacy and data security outsourcing in the cloud and offer cloud-based storage and computing services to address data privacy issues coud, to protect data from malicious internal and external users. These problems should refer to "The cloud security management problem".

The following security issues for users are not resolved by the existing security solution provided by cloud service providers.

Ensuring and addressing these security issues would increase trust in the cloud computing system and thus attract new customers.

IV. CONCLUSION AND RECOMMENDATIONS

In this paper, reviewed current knowledge regarding privacy concerns in cloud storage, once data outsourced to the remote cloud it can accessible to every user due to this many security issues raised , in order to overcome security issues in literature various authors proposed different methodologies, data auditing is one mechanism to know the data integrity and cryptography techniques implemented for protecting data from unauthorized users and for controlling cloud data access ABE proposed using this the data owner can define set of access policies over cloud data. There is a need to design and develop a cloud data security management system to improve security and privacy of data outsourced to the cloud. The future recommendation to this comprehensive information security framework for IaaS model required. The context presents information protection as a service (ISaaS) to cloud.

REFERENCES

1. Cong Wang; et.al 2010, “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing”, Proceedings IEEE INFOCOM, pp: 1 – 9.
2. Shucheng Yu; et.al 2010, “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing”, Proceedings IEEE INFOCOM, **ISSN:** 0743-166X, pp: 1 – 9.
3. Ning Cao; et.al 2011, “Privacy-Preserving Query over Encrypted Graph-Structured Data in Cloud Computing” 31st International Conference on Distributed Computing Systems, pp: 393 – 402.
4. Ran Yang; et.al 2012, “Enforcing scalable and dynamic hierarchical access control in cloud computing”, IEEE International Conference on Communications (ICC), pp: 923 – 927.
5. Mebae Ushdia; et.al 2013, “A Proposal of Privacy-Preserving Data Aggregation on the CloudComputing”, 16th International Conference on Network-Based Information Systems, Pp: 141 – 148.
6. P. Praveen Chandar; et.al,2014 “Hierarchical attribute based proxy re-encryption access control in cloud computing" , International Conference on Circuits, Power and Computing Technologies [ICCPCT-2014], pp:1565 – 1570
7. Jun-She Wang; et.al 2015, “Research on Resource Allocation Scheme Based on Access Control in Cloud Computing Environment”, International Conference on Computer Science and Applications (CSA), pp: 377 – 380.
8. Shaohua Tang; et.al, 2016, “Achieving Simple, Secure and Efficient Hierarchical Access Control in Cloud Computing”, **ISSN:** 0018-9340, Volume: 65, Issue: 7, Pages: 2325 – 2331.
9. Hui Xia :2017, “Design and implementation of trust based access control system for cloud computing” IEEE 3rd Information Technology and Mechatronics Engineering Conference (ITOEC), pp: 922 – 926.

AUTHOR PROFILE

Pratyusha.T is Research scholar in JJT University and working as assistant professor in CMR Institute of Technology, Medchal, Hyderabad. Currently she has 5 years of experience in teaching and interested areas are cloud computing, Data Mining, Machine Learning, Artificial Intelligence.

Dr. B.M.G. Prasad presently serving as Professor in Computer Science and engineering and Dean PG Courses at Holy Mary Institute of Technology and Science, Hyderabad, Telangana. Prevously, he worked as Principal in Dr K.V.Subha Reddy College Engineering for Women, Kurnool, A.P. He is having 18+ years of teaching experience in various Engineering College. He has done his B.E. at Vijaya Nagar Engineering College, Bellary in July 1997. He completed his M. Tech at J.N.T.U College of Engineering, Anatapur in January 2003. He Completed his Ph.D in Computer Science and engineering from CMJ University, Meghalaya State in February 2013. He has published papers in the I-Manager's International Journal and Indian National Science Congress, Tiruvananthapuram in the Computer Networks area. He has published 15 international Journals and five national Journals and Conferences. He authored two Text books in adhoc networks and Map Reduce. His areas of interest are Software Engineering, Cloud Computing, Wireless Networks, Imag Processing etc.