International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 3 Issue 6, October 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

A Data Sharing Protocol to Minimize Security and Privacy Risks in Cloud Storage

S. Nandhini Devi[1], Mr. S. Rajarajan[2]

[1]M.E (CSE) Student, [2]M.E., (Ph.D), Assistant Professor,
[1,2]Department of CSE, Kings College of Engineering, Thanjavur, Tamil Nadu, India

ABSTRACT

Data contribution in the cloud is a procedure so as to allow users to expediently right of entry information in excess of the cloud. The information holder outsources their data in the cloud due to cost lessening and the huge amenities provided by cloud services. Information holder is not able to manage over their information, since cloud examination contributor is a third party contributor. The main disaster with data partaking in the cloud is the seclusion and safety measures issues. Different techniques are obtainable to sustain user seclusion and protected data sharing. This paper focal point on different schemes to contract by means of protected data partaking such as information contribution with forward security, protected information partaking for energetic groups, quality based information partaking, encrypted data sharing and mutual influence Based Privacy-Preserving verification set of rules for right to use manage of outsourced information.

KEYWORDS: *conveniently access data, secure data sharing, forward security, Privacy-Preserving Authentication Protocol*

How to cite this paper: S. Nandhini Devi | Mr. S. Rajarajan "A Data Sharing Protocol to Minimize Security and Privacy Risks in Cloud Storage" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-6, October 2019, pp.1142-1145, URL: https://www.ijtsrd.com/papers/ijtsrd29345.pdf

IJTSRD29345

INTRODUCTION

Emerging technologies about big data such as Cloud Computing , Business Intelligence , Data Mining, Industrial Information Integration Engineering(IIIE) and Internet-of-Things have opened a new era for future Enterprise Systems(ES) . Cloud computing is a new computing model, in which all resource on Internet form a cloud resource pool and can be allocated to different applications and services dynamically. Compared with traditional distribute system, a considerable amount of investment saved and it brings exceptional elasticity, scalability and efficiency for task execution. By utilizing Cloud Computing services, the numerous enterprise investments in building and maintaining a supercomputing or grid computing environment for smart applications can be effectively reduced. Despite these advantages, security requirements dramatically rise when storing personal identifiable on cloud environment. This raise regulatory compliance issues since migrate the sensitive data from federate domain to distribute domain. To take the benefit enabled by big data technologies, security and privacy issues must be addressed firstly. Building security mechanism for cloud storage is not an easy task. Because shared data on the cloud is outside the control domain of legitimate participants, making the shared data usable upon the demand of the legitimate users should be solved. Additionally, increasing number of parties, devices and applications involved in the cloud leads to the explosive growth of numbers of access points, which makes it more difficult to take proper access control. Lastly, shared data on the cloud are vulnerable to lost or incorrectly modified by the cloud provider or network attackers. Protecting shared data from unauthorized deletion, modification and fabrication is a difficult task.

LITERATURE SURVEY

1. **"Efficient and secure identity-based encryption scheme with equality test in cloud computing,"**

Xinyi Huang et.al [1] (2015) introduced a Identity-based (ID-based) ring signature, which eliminates the process of certificate verification. By providing forward secure ID-based ring signature method security level of ring signature is increased. In this method, if the secret key of any user has been compromised, previous generated signatures of all is included and the user still remains valid. If a secret key of single user has been compromised it is impossible to ask all data owners to reauthenticate their data. It is especially important to any large scale data sharing system and it is very efficient and does not require any pairing operations. The user secret key is one integer, while the key update process requires an exponentiation. This scheme is useful; especially to those require authentication and user privacy.

2. **"A scalable attributed-set-based access control with both sharing and full-fledged delegation of access privileges in cloud computing,"**

Huang Qinlong et.al [2] (2015) suggested an attribute-based secure data sharing scheme with Efficient revocation (EABDS) in cloud computing. To guarantee the data confidentiality and to achieve fine-grained access control this proposed scheme encrypts data with Data encryption key (DEK) using symmetric encryption method and then encrypts DEK based on Ciphertext policy attribute-based encryption (CP-ABE). The homomorphic encryption technique is used to solve key escrow problem in order to generate attribute secret keys of users by attribute authority in support with key server. This homomorphic encryption technique is used to prevent the attribute authority from accessing the data by generating the attribute secret keys alone. EABDS scheme achieves immediate attribute revocation which guarantees forward and backward security, and less computation cost on users. Advantages of this method are more secure and efficient.

3. **"Securing outsourced data in the multi-authority cloud with fine-grained access control and efficient attribute revocation,"**

Hong Liu et.al [3] (2015) proposed a shared authority based privacy preserving authentication protocol (SAPA) to address the privacy issues for a cloud storage. Their protocol is attractive for multi-user collaborative cloud applications. The existing security solutions mainly focus on authentication. In SAPA, the shared access authority is achieved by anonymous access request matching mechanism, provides Ciphertext-policy attribute based access control to enable users to reliably access its own data fields and proxy re-encryption is applied to provide data sharing among multiple users. Universal Compos ability (UC) model is established to prove the SAPA has design correctness. When a user challenges the cloud server to request other users for data sharing, this access request itself may reveal user's privacy. This scheme addresses user's sensitive access related privacy during data sharing in cloud environment and achieves data access control, access authority sharing and privacy preservation. Through the SAPA protocol, authentication and authorization is preserved without compromising user's private information.

4. **"Privacy-preserving public auditing for secure cloud storage,"**

Xin dong et.al [4] (2014), proposed an effective, scalable and flexible privacy-preserving data policy with semantic security. They used two techniques Ciphertext policy attribute-based encryption (CP-ABE) and Identity based Encryption (IBE) that provided a dependable and secure cloud data sharing service that allows dynamic data access to users. Their scheme ensures robust data sharing preserves privacy of cloud users and supports efficient and secure dynamic operations which include file creation, user revocation and modification of user attributes. This scheme also enforces fine-grained access control, full collusion resistance and backward secrecy. Although cloud computing is economically attractive to customers and enterprises, it does not guarantee users privacy and data security. The proposed scheme provides semantic security for data sharing in cloud computing through the generic bilinear group model and also imposes backward secrecy and access privilege confidentiality. The performance analysis of this scheme incurs a small overhead compared to existing schemes.

5. **"Secure Multi-Authority Data Access Control Scheme in Cloud Storage System Based on Attribute-based Sign encryption"**

Qiang Tang et.al [5] (2014) suggested a searchable encryption namely multi-party searchable encryption (MPSE). It enables users to selectively permit each other to search in their encrypted data. For worst-case and average-case collusion due to the user status dynamics a security model is considered. He proposed a new scheme with provable security. A security model for MPSE provides stronger security guarantee than that from. In the formulation of MPSE, authorization is approved on index level, for each of her indexes example Alice can make a decision whether Bob can search or not i.e. if all keywords try by authorized Bob then Alice supports authorize Bob to look for a subset of keywords in her indexes as well as the cloud server colluded with Bob can recover the keyword in all Alice's search queries. In this MPSE formulation, expected to be that Alice can find out a problem of single trapdoor search for all indexes that have been authorized by her. Disadvantages of this formulation are If Alice have many key pairs in the index and use them with various peers then it leaks some unnecessary information. In contrast, inverted index structure may not face this kinds of problem.

IMPLEMENTATION

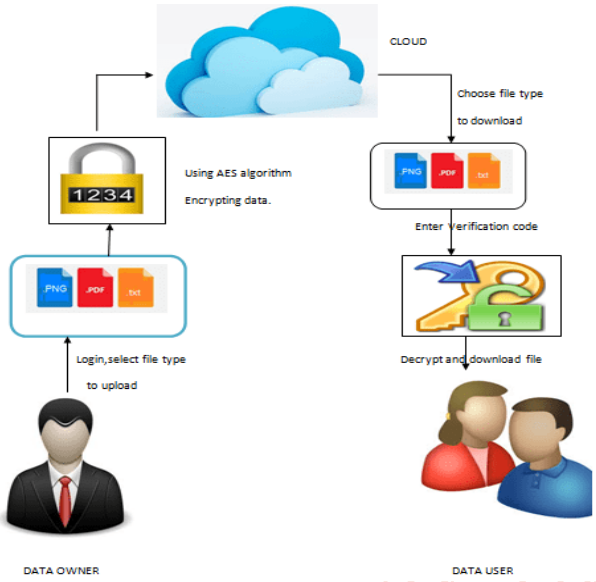
Existing System

Cloud systems can be used to enable data sharing capabilities and this can provide several benefits to the user and organization when the data shared in cloud. Since many users from various organisations contribute their data to the Cloud, the time and cost will be less compared to manually exchange of data. Google Docs provides data sharing capabilities as groups of students or teams working on a project can share documents and can team up with each other successfully. This allows higher productivity compared to previous methods of frequently sending updated versions of a document to members of the group via email attachments. People are expecting data sharing capability on their computers, phones and laptop etc. People love to share their information with others such as family, colleagues, friends or the world. Students also get benefit when working on group projects, as they are able to team up with members and get work done efficiently.

Proposed System

In this proposed system common temp key is shared to reduce the information leakage from cloud storage in big data. To minimize security and privacy risks some limits were provided which are time limit, size limit, and credit point limit. Information was encrypted to provide more security (AES, DES algorithm). The temp key can be used by person who requests to retrieve information for once. If other than the request person tries to use temp key then that key is removed and alert notification will be send to data owner. Temp key provider sends the key to request person by mail using SMTP protocol. (Gmail -high secure) The main advantage of proposed system is to separate

storage space into module and each module is secured with temp password. This makes more efficient constructions. This key can be used only once. We propose a new secret sharing scheme that is computationally secure and can reduce the number of shares Temp key helps information retrieval more secured with low cost. Only request person can use temp key. Encryption standards make information difficult to theft. Limitations of temp key provide high security.



CONCLUSION

Common temp key is shared to reduce the information leakage from cloud storage in big data. To minimize security and privacy risks some limits were provided which are time limit, size limit, and credit point limit. Information was encrypted to provide more security (AES, DES algorithm). The temp key can be used by person who requests to retrieve information for once. If other than the request person tries to use temp key then that key is removed and alert notification will be send to data owner. Temp key provider sends the key to request person by mail using SMTP protocol. (Gmail -high secure) The main advantage of proposed system is to separate storage space into module and each module is secured with temp password. This makes more efficient constructions. This key can be used only once. We propose a new secret sharing scheme that is computationally secure and can reduce the number of shares Temp key helps information retrieval more secured with low cost. Only request person can use temp key. Encryption standards make information difficult to theft. Limitations of temp key provides high security

FUTURE ENHANCEMENT

The new applications are generating vast amount of data in structured and unstructured form. Big data is able to process and store that data and probably in more amounts in near future. Hopefully, Hadoop will get better. New technologies and tools that have ability to record, monitor measure and combine all kinds of data around us, are going to be introduced soon. We will need new technologies and tools for anonymzing data, analysis, tracking and auditing information, sharing and managing, our own personal data in future. So many aspects of life health, education, telecommunication, marketing, sports and business etc that manages big data world need to be polished in future.

References

[1] Sen, J. (2011a). A Robust Mechanism for Defending Distributed Denial of Service Attacks on Web Servers. International Journal of Network Security and its Applications, Vol 3, No 2, pp. 162-179, March 2011.

[2] Sen, J. (2011b). A Novel Mechanism for Detection of Distributed Denial of Service Attacks. In Proceedings of the 1st International Conference on Computer Science and Information Technology (CCSIT'11), pp. 247-257, Springer CICS Vol 133, Part III, January 2011, Bangalore, India.

[3] Sen, J. (2010a). An Agent-Based Intrusion Detection System for Local Area Networks. International Journal of Communication Networks and Information Security (IJCNIS), Vol 2, No 2, pp. 128-140, August 2010.

[4] Sen, J. (2010b). Intrusion Detection Architecture for Clustered Wireless Ad Hoc Networks. In Proceedings of the 2nd IEEE International Conference on Intelligence in Communication Systems and Networks (CICSyN'10), pp. 202-207, July, 2010, Liverpool, UK.

[5] Sen, J. (2010c). A Robust and Fault-Tolerant Distributed Intrusion Detection System. In Proceedings of the 1st International Conference on Parallel, Distributed and Grid Computing (PDGC'10), pp. 123-128, October 2010, Waknaghat, India.

[6] Sen, J. (2010d). A Distributed Trust Management Framework for Detecting Malicious Packet Dropping Nodes in a Mobile Ad Hoc Network. International Journal of Network Security and its Applications (IJNSA), Vol 2, N0 4, pp. 92-104, October 2010.

[7] Sen, J. (2010e). A Distributed Trust and Reputation Framework for Mobile Ad Hoc Networks. In Proceedings of the 1st International Workshop on Trust Management in Peer-to-Peer Systems (IWTMP2PS), pp. 538-547, July 2010, Chennai, India, Springer CCIS Vol 89.

[8] Sen, J. (2010f). A Trust-Based Robust and Efficient Searching Scheme for Peer-to-Peer Networks. In Proceedings of the 12th International Conference on Information and Communication Security (ICICS), pp. 77-91, December 2010, Barcelona, Spain, Springer LNCS Vol 6476.

[9] Sen, J. (2010g). Reputation- and Trust-Based Systems for Wireless Self-Organizing Networks. Book Chapter in Security of Self-Organizing Networks: MANET, WSN, WMN, VANET, pp. 91-122, Al-Shakib Khan Pathan et al. (eds.), Aurbach Publications, CRC Press, USA, December 2010.

[10] Sen, J. (2011c). A Secure and Efficient Searching for Trusted Nodes in Peer-to-Peer Network. In Proceedings of the 4th International Conference on Computational Intelligence in Security for Information Systems (CISIS'11), pp. 101-109, Springer LNCS Vol 6694, June 2011.

[11] Sen, J. & Sengupta, I. (2005). Autonomous Agent-Based Distributed Fault-Tolerant Intrusion Detection System. In Proceedings of the 2nd International Conference on Distributed Computing and Internet Technology (ICDCIT'05), pp. 125-131, December, 2005, Bhubaneswar, India. Springer LNCS Vol 3186.

[12] Sen, J., Sengupta, I., & Chowdhury, P. R. (2006a). A Mechanism for Detection and Prevention of Distributed Denial of Service Attacks. In Proceedings of the 8th International Conference on Distributed Computing and Networking (ICDCN'06), pp. 139-144, Springer LNCS Vol 4308, December 2006, Guwahati, India.

[13] Sen, J., Sengupta, I., & Chowdhury, P.R. (2006b). An Architecture of a Distributed Intrusion Detection System Using Cooperating Agents. In Proceedings of the International Conference on Computing and Informatics (ICOCI'06), pp. 1-6, June, 2006, Kuala Lumpur, Malaysia.