How to Cite:
Arunkumar, A. S., Chatterjee, S., Basavaraju, S. K., & Basavaraju, G. C. (2022). Secure search over encrypted data in multi cloud. *International Journal of Health Sciences*, *6*(S9), 3880–3884. Retrieved from https://sciencescholar.us/journal/index.php/ijhs/article/view/13502

Secure search over encrypted data in multi cloud

A S Arunkumar
Resarch scholar, Dept of IS & E, BGI

Sunetra Chatterjee
MCA scholar

Sunil Kunchoorj Basavaraju
Data scientist

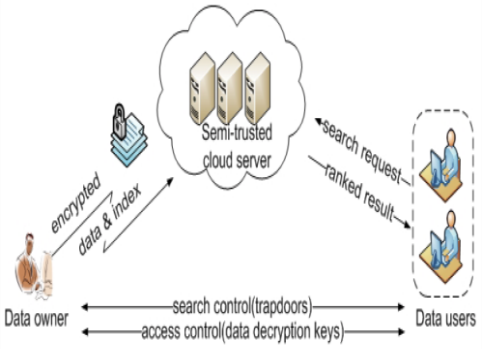
Basavaraju G C
HOD, Dept of Math's

***Abstract*---**A two-thing information protection protection mechanism with element revocability for cloud storage machine. Our gadget permits a sender to send an encrypted message to a receiver thru a cloud storage server. The sender best desires to understand the identification of the receiver however no other information (including its public key or its certificates). The receiver needs to own two things so that it will decrypt the cipher text. The first element is his/her mystery key stored in the pc. The second aspect is a completely unique private safety tool which connects to the computer. It is impossible to decrypt the cipher text without either piece. More importantly, once the safety tool is stolen or lost, this tool is revoked. It cannot be used to decrypt any cipher text. This can be achieved through the cloud server with the intention to right now execute some algorithms to exchange the existing cipher text to be un-decrypt able via this device. This process is absolutely transparent to the sender. Furthermore, the cloud server cannot decrypt any cipher text at any time. The security and performance evaluation display that our gadget is not best steady but also realistic. Cloud storage is a model of networked storage gadget in which facts is stored in swimming pools of storage which are generally hosted by 0.33 events. There are many benefits to apply cloud storage. The maximum exquisite is facts accessibility. Data saved within the cloud may be accessed at any time from any place so long as there may be network get admission to. Storage maintenance obligations, along with buying additional storage potential, may be offloaded to the responsibility of a carrier company. Another gain of cloud garage is information sharing between

customers. If Alice desires to share a bit of information (eg. A video) to Bob, it can be difficult for her to send it with the aid of electronic mail because of the scale of data. Instead, Alice uploads the file to a cloud garage machine in order that Bob can download it at every time. Despite its blessings, outsourcing information storage also will increase the attack surface area on the identical time. For instance, when records is sent, the more places it's far saved the better risk it includes for unauthorized physical access to the facts. By sharing garage and networks with many different customers it's also viable for other unauthorized customers to access your facts.

Keywords---cloud computing, searchable encryption, keyword, security, asymmetric.

Architecture



Introduction

Cloud computing is a fairly new enterprise version inside the computing global. According to the legit National Institute of Standards and Technology (NIST) definition, “Cloud computing is a version for allowing ubiquitous, handy, on demand network get entry to a shared pool of configurable computing assets (e.g., networks, servers, garage, applications, and offerings) that can be swiftly provisioned and released with minimal management effort or provider interplay”.

Existing System

Double Encryption:

- In this technique information encrypted times.
- First, encrypt the facts (plaintext) corresponding to the general public key or identity of the consumer.
- Second, encrypt again similar to the general public key or serial variety of the security device.

Drawback:

- If the user has misplaced his safety device, then his/her corresponding cipher textual content within the cloud can not be decrypted, cannot update device.
- Sender need to understand the serial number/public key of the safety tool.

Proposed System

Data Owner
In this module information proprietor need to upload cypher textual content records in to cloud server.

Data User
In this module information consumer should down load facts form cloud server and decrypt records using mystery key and secret device.

KDC (Key Distribution Center)
In this module KDC should deal with the important thing era and device replace.

Objectives
- Our System is IBE(Identity Based Encryption) mechanism. Sender want to recognise handiest identification of the user to ship encrypted records.
- In order to decrypt the facts stored in the cloud, consumer need to do two matters, wherein he/she must provide secret key which is saved in the computer.
- Second, consumer have to have particular safety tool so as to be connected to laptop.
- It is not possible to decrypt textual content without either of these items (either mystery key or protection device).
- Our device device can be revocable.
- The cloud server can not decrypt any cipher textual content any time.

Cloud Storage Advantages

- Data hosted in the cloud garage server can be accessed at any time from any place.
- Cloud consumer can get any quantity of additional sources any time with a view to be provided via cloud provider provider.
- No chance of Data Maintenance.
- Data sharing between user's may be very clean.

Cloud Storage Disadvantages
- As lengthy as records is stored in third birthday party physical garage device, there's no safety for records saved inside the cloud server.
- Many users are connected to the cloud server each day so that, any entity or consumer can get get right of entry to cloud information saved in the cloud server.
- Malicious cloud customers can get admission to any statistics stored within the cloud server, it's miles tough to predict malicious cloud user because wide variety of users are linked to the cloud every day.

Data Protection in Cloud

- Cloud facts is blanketed through the usage of Asymmetric encryption.
- Asymmetric encryption lets in the encrypt or to apply best the public key or identification of the receiver to generate a cipher text.
- Receiver should use his/her very own secret key to decrypt.

Risk in Protecting Data in Cloud Server

- If the public-key or Identity is saved inside both a personal computer or a depended on server and that server or laptop is protected through a password. This security is enough if the server or laptop is remoted from an opening network.
- But that is what not occurs in the actual world, due to the fact server or pc ought to continually be in hook up with open network.
- The pc or server might also be afflicted by a capability risk, that hacker may additionally compromise the secret-key.

Conclusion

This paper conclude A two-thing information protection protection mechanism with element revocability for cloud storage machine. Our gadget permits a sender to send an encrypted message to a receiver thru a cloud storage server. . Cloud storage is a model of networked storage gadget in which facts is stored in swimming pools of storage which are generally hosted by 0.33 events. There are many benefits to apply cloud storage. The maximum exquisite is facts accessibility. Data saved within the cloud may be accessed at any time from any place so long as there may be network get admission to. Storage maintenance obligations, along with buying additional storage potential, may be offloaded to the responsibility of a carrier company. Another gain of cloud garage is information sharing between customers. If Alice desires to share a bit of information (eg. A video) to Bob, it can be difficult for her to send it with the aid of electronic mail because of the scale of data. Instead, Alice uploads the file to a cloud garage machine in order that Bob can download it at every time. Despite its blessings, outsourcing information storage also will increase the attack surface area on the identical time. For instance, when records is sent, the more places it's far saved the better risk it includes for unauthorized physical access to the facts. By sharing garage and networks with many different customers it's also viable for other unauthorized customers to access your facts.

References

[1] T. Mather, S. Kumaraswamy, and S. Latif, Cloud security and privacy: an enterprise perspective on risks and compliance: O'Reilly, 2009.
[2] S. Pearson and A. Benameur, "Privacy, security and trust issues arising from cloud computing," in Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on, 2010, pp. 693-702.
[3] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. 34, pp. 1-11, 2011.

[4] H. Takabi, J. B. Joshi, and G.-J. Ahn, "Security and privacy challenges in cloud computing environments," Security & Privacy, IEEE, vol. 8, pp. 24-31, 2010.
[5] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and privacy in cloud computing: A survey," in Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on, 2010, pp. 105-112. [6] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vol. 28, pp. 583-592, 2012.