Ilkogretim Online - Elementary Education Online, 2020; Vol 19 (Issue 2): pp. 1908-1913
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2020.02.696775

Enhancing Data Security For Sensitive Data Using Encryption And Geo-Fencing Technique In Cloud Environment

[1]Suganya M , [2]Dr. SU. Suganthi , [3]L. Kannagi , [4] J. Mathiyazhagan

[1,,3]Assistant Professor, Department of Computer and Communication Engineering, Sri Sairam Institute of Technology

[2,]Assistant Professor, Department of Computer and Communication Engineering, Sri Sairam Institute of Technology

[4]Technical team lead, Maitri Technology solutions

Abstract: Security has consistently been a significant issue in cloud environment. Sensitive information need to be secured from intruders or attackers. Nowadays, data is intentionally or unintentionally access without authorization. In large medical organizations, end users trust cloud providers and store their medical records in the cloud. Data stored in public cloud are more vulnerable than private cloud. In this paper, COVID 19 real time dataset is stored securely using encryption and geo-fencing technique is used to alert the data owner in the cloud environment when data users try accessing sensitive data away from the defined location. Experimental results were shown to identify the hackers entering into the unauthorized location.

Keywords: Public Cloud, Encryption, Geo Fencing, Security, Service Providers, Consumers.

I. INTRODUCTION

As organizations continue to grow and expand, it is necessary to store their data in the secured manner from vulnerabilities. Cloud security plays a vital role for both professional and personal users in terms of data. The location- based cloud data security can be used alongside many organizations so that their cloud data cannotbe accessed away from their organization without the owner's permission as well as individual end user sensitive data can be safe guarded once stored on to cloud environment.

CLOUD SECURITY

Cloud security, also known as cloud computing security is an assortment of safety efforts intended to ensure cloud-based framework, applications, and information. Cloud information security turnsout to be progressively significant as we move ourgadgets, server farms, business cycles, and more to the cloud. Guaranteeing quality cloud information security is accomplished through complete security arrangements, an authoritative culture of safety, and cloud security arrangements. Cloud security is a bunch of control-based shields and innovation insuranceintended to shield assets put away online from spillage, robbery, or cloud information misfortune. Cloud security is a duty that is divided among the cloud supplier and the client. There arefundamentally three classifications of obligations in the Shared Responsibility Model: duties that are consistently the provider's, duties that are consistently the customer's, and obligations that fluctuate contingent upon the service model. Choosing the correct cloud security answer for your business is basic on the off chance that you need to get the best from the cloud and guarantee your association is shielded from unapproved access, information breaks and different dangers. The cloud security should include encryption to scramble the data and identity and access management to identify who is trying to access the data and giving accessibility if necessary.

II. ARCHITECTURE

The architecture diagram shows the data access between the data owner, provider and consumer.

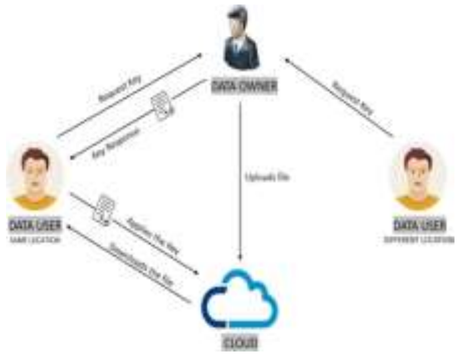


Fig. 1.Data Storage in cloud Architecture

III. METHODOLOGY

The data owner upload the datainformation in the cloud. The data owner upload the data along with the location details in which these data can be accessed. While uploading, advanced encryption standard algorithm encrypts the file , the encrypted format is stored in the cloud. The cloud service admin maintains the storage process details in the cloud. An index for the data is generated in the cloud. The data user who needs the data, sends request to the data owner, who owns the data.The request sent by the data user is visible to the data owner.If the data user is in accessible location, then the data user gets the secret key to download the file.If the data user is in different location, thenthe data user cannot able to download the file.

A. Existing System

Many organizations store there data in the cloud environment. Even though cloud provides security to the data, cloud data is accessible on anytime- anywhere. In this case, confidential data of the organization can be accessed from anywhere without data owner's permission. Security challenges is not addressed efficiently and many data breaches are occurring in cloud environment.

B. Proposed System

In this Proposed system, security of data stored in cloud environment is implemented efficiently. In this methodology, the data owner uploads the COVID 19 medical data in the cloud along with the location details. If the Data user are under same location, then the data can be downloaded by applying the secret key. If the Data users are in different location, then file cannot be downloaded. To overcome the security challenges, a fencing technology is used to provide more security for organization's data

IV. WORKING

A. Data owner uploading data (with location):

In this phase, data owner uploads file into the cloud using key for encryptingthe sensitive text document. The data owner uploads and downloads the file with location. Any employee, contractor or third-party provider who is authorized by the Data Owner can access information assets.

B. Key generation and encryption:

Data owner outsourcing the data to the cloud while uploading the data owner need to mention the location from where data is been uploaded. During the data upload, a secret keyvisible to the data owner. This key is used to download the required file.

C. Cloud admin generating index:

The cloud admin maintains everything in the cloud, indexing is generated for data which is available in the cloud. Semantic Search Engine for Logical searchingusing Word Embedding and Transportation is used to finally produce the result with RLP Algorithm from the Indexed dataset in the cloud.

D. Data user downloading data using key:

In this phase, In order to download the file a key is requested from the data owner and applied, if key matches, the file is downloaded, if key does not matches, file cannot be downloaded.

E. Data owner and user access dataset:

This phase describes the usage of symmetric key. the user and data owner can access the files from the cloud.A Data Owner has administrative control and hasbeen officially designated as accountable for a specific information asset dataset.

FLOWCHART

This flowchart of our Proposal will clearly explain the whole process of our system. Data usersearch for data in the cloud using a keyword.If the data is found at the same location in which data owner uploaded, data user can download the data by applying the secret key.If the location is not matched, data user cantable to download the file

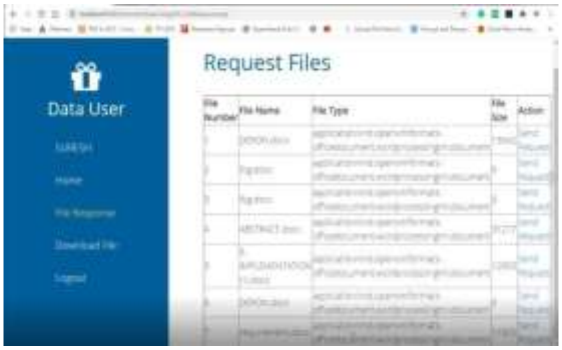
.

Fig. 2. Flowchart

VI. SCREENSHOTS

Fig. 3.1. Data Owner Login

Fig. 3.2. Data Owner Uploading data



Request Files

File Number	File Name	File Type	File Size	Action
1	DEMON.docx	application/vnd.openxmlformats-officedocument.wordprocessingml.document	[illegible]	Send Request
2	fig.docx	application/vnd.openxmlformats-officedocument.wordprocessingml.document	0	Send Request
3	fig.docx	application/vnd.openxmlformats-officedocument.wordprocessingml.document	0	Send Request
4	ABSTRACT.docx	application/vnd.openxmlformats-officedocument.wordprocessingml.document	[illegible]	Send Request
5	[illegible] IMPLEMENTATION.docx	application/vnd.openxmlformats-officedocument.wordprocessingml.document	[illegible]	Send Request
6	DEMON.docx	application/vnd.openxmlformats-officedocument.wordprocessingml.document	0	Send Request
7	[illegible]	application/vnd.openxmlformats-officedocument.wordprocessingml.document	[illegible]	Send Request

Fig. 3.3. Data User requesting file

Fig. 3.4. Data Owner checks the requested files

VII. CONCLUSION AND FUTURE WORK

The proposed system is very much useful in organizations where sensitive date is stored in the cloud environment. The system helps by identifying the data user who needs to access their data in particular locations. The proposed system provides access to the data user of same location to download the data, whereas for the data user who requesting key from different location, access is denied. The future work can be implemented with the novel techniquein which owner can decide whether to provideaccess to the data user from different location or deny access.

REFERENCES

[1] L. Badger, D. Berstein, R. Bohn, F. de Valux, M. Hogan, J. Mao, J. Messina, K. Mills, A. Sokol, J. Tong, F. Whiteside, and D. Leaf, US government cloud computing technology roadmap volume 1: High- priority requirements to further USG agency cloud computing adoption (NIST SP 500-293, Vol. 1), National Institute of Standards and Technology, U.S. Department of Commerce (2011).

[2] W. Jansen and T. Grance, Guidelines on security and privacy in public cloud computing (NIST SP 800-144). National Institute of Standards and Technology, U.S. Department of Commerce (2011).

[3] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, NIST Cloud Computing Reference Architecture (NIST SP 500-292), National Institute of Standards and Technology, U.S. Department of Commerce (2011).

[4] R. Choubey, R. Dubey, and J. Bhattacharjee, "A survey on cloud computing security, challenges and threats," Int. J. Comput. Sci. Eng., vol. 3, no. 3, pp. 1227–1231, 2011.

[5] A. Hussain, C. Xu, and M. Ali, "Security of Cloud Storage System using Various Cryptographic Techniques," International Journal of Mathematics Trends and Technology (IJMTT), vol. 60, no. 1, pp. 45–51, 2018.

[6] D. Panth, D. Mehta, R. Shelgaonkar "A Survey on Security Mechanisms of Leading Cloud Service Providers," Int. J. Comput. Appl. , vol. 98, no. 1, pp. 24–34, 2014.