iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4238

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

Server Aided Data Authentication

T.Chandrababu[1], C.Anand[2], K.Harish[3], S.Dhanabal[4],Mr.A.Ganesan[5]
[1, 2, 3, 4] *Final MCA,* [5]*Associate Professor, PG and Research Department of Computer Applications,Hindusthan College of Arts and Science, Coimbatore, India*

Abstract: ***The data from investigate organizations, safety firms and government organizations demonstrate that the numbers of data leak instances have developed rapidly. Among different data leak cases, major causes of data loss are one of the human being mistakes. Present live solutions detect unintentional responsive data leaks caused by human being mistakes and to provide alerts intended for organization. In this system, there a privacy preserving data leak detection solution where a particular set of receptive data digests is used in discovery. Privacy-preserving data-leak detection representation intended for preventing inadvertent data leak in scheme traffic. Such a demonstration yields a powerful and delegable data-leak detection framework. The cloud computing surroundings the cloud source can perform data leak detection as add on service to its customers. The assessment results show that the detection method can supports accurate detection through very miniature number of false alarms under various data leak scenarios. The benefit of this method is that it enables the data owner to safely hand over the detection operation without enlightening the sensitive data to the source. The user can two or three time login incorrectly the account has been locked this method used for secure. Then the user can request for admin. Admin will accepted user account automatically unlocked.***

Keywords: ***Data Leak Detection (DLD), Watermarking.***

I. INTRODUCTION

Objective is to identify when the distributor's responsive information have been leaked by agents, and if likely to identify the agent that leaked the information. Traditionally, leakage discovery is handled by watermarking, e.g., a unique code is entrenched in each dispersed copy.

Water-marks can be very useful in some cases, but again, involve some alteration of the unique data. Refer the next situation: following giving a set of objects to agents, the dispenser discovers some of those same objects in an illegal place. (For example, the information may be found on a website, or may be obtained through an authorized detection procedure.) At this point, the distributor can assess the likelihood that the leaked information came from one or more agents, as opposite to having been separately gathered by other means. In this system, develop a model for assessing the guilt of agents. Also new algorithms for distributing objects to agents, in a way that improve chances of identify a leaker. The unauthorized users can access the account that can be predicted in this method.

If the unauthorized person tries to access the user account that can be predict and monitored on this method. And also identify the details about the user, IP address and details of the user. Thus the details are transferred to the authorized Person. The message can be transferred from source to the destination that time using the cryptography method. The source is encrypt the message using the public key of the receiver and then sends to the destination. The receiver can be decrypting the message using the private key. That time unauthorized Persian performs the illegal activities that can be predicted. The private key is not matched to the decryption process then identifies the user details, IP address. Thus the details are transferred to the sender side. The Privacy preserving data-leak detection (DLD) solution to solve the issue where a special set of sensitive data digests is used in detection. The advantage of our method is that it enables the data owner to safely delegate the detection operation to a semi honest provider without revealing the sensitive data to the provider.

A. Problem Definition

Refer the next situation: following giving a set of objects to agents, the dispenser discovers some of those same objects in an illegal place. (For example, the information may be found on a website, or may be obtained through an authorized detection procedure.) At this point, the distributor can assess the likelihood that the leaked information came from one or more agents, as opposite to having been separately gathered by other means. In this system, develop a model for assessing the guilt of agents. Also new algorithms for distributing objects to agents, in a way that improve chances of identify a leaker.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

II. PROPOSED SYSTEM

The system model in this project involves three parties: the cloud server, a group of users and a public verifier. There are two types of users in a group: the original user and a number of group users. The original user initially creates shared data in the cloud, and shares it with group users. Both the original user and group users are members of the group. The data owner share the data into the cloud users, and the users should be access the data securely. The data should be transmitted from the data owner on securely through network.

A. Proposed System Provides With Following Solutions

1) The users should be access the data securely
2) Reduced For Data Leakage
3) The data should be transmitted from the data owner on securely through network.

III. MODULE DESIGN

A. Modules

1) Data Allocation Module
2) Optimization Module
3) Data Distributor
4) Secure transaction
5) user side

B. Data Allocation Module

The main focus of our project is the data allocation problem as how can the distributor "intelligently" give data to agents in order to improve the chances of detecting a guilty agent.

C. Optimization Module

The Optimization Module is the distributor's data allocation to agents has one constraint and one objective. The distributor's constraint is to satisfy agents' requests, by providing them with the number of objects they request or with all available objects that satisfy their conditions. His objective is to be able to detect an agent who leaks any portion of his data.

D. Data Distributor

A data distributor has given sensitive data to a set of supposedly trusted agents (third parties). Some of the data is leaked and found in an unauthorized place (e.g., on the web or somebody's laptop). The distributor must assess the likelihood that the leaked data came from one or more agents, as opposed to having been independently gathered by other means.

E. Secure Transaction

Each user is assigned to data owner from the Provider. Each user can freely get the cipher texts from the server. To decrypt a cipher text, each user may submit their secret keys issued by data owner together with its secret key to the server and ask it to generate decryption token for some cipher text. Upon receiving the decryption token, the user can decrypt the cipher text by using its secret key. The users those who are having matching keys as in the access policy defined in the cipher text can retrieve the entire data content. It aims to allow the users with eligible attributes to decrypt the entire data and access the data. However it cannot limit the users from accessing the data's which are not accessible to them. That is it cannot limit the data access control to the authorized users.

F. User Side

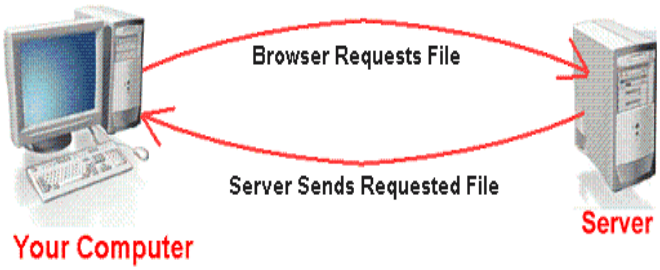
The user access the data from the service provider, decrypt and got the original data. The unauthorized person access the secure data from the service provider on the person account and miss use the account. If the account hack into the unauthorized person or another person enters into the account, the server side read the current details about the user and ip address of the system .If the authorized user receives the unsecured message and then change the account user name and password.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

IV. DEPLOYMENT DETAILS

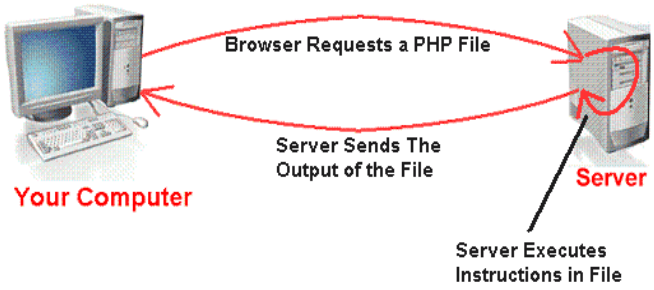
Hypertext refers to files linked together using hyperlinks, such as HTML (Hyper-Text Mark-up Language) files. Pre-processing is executing instructions that modify the output. Below is a demonstration of the difference between HTML and PHP files.

A. Accessing an HTML Page



1) Your browser sends a request to that web page's server (computer) for the file (HTML or image) you wish to view.
2) The web server (computer) sends the file requested back to your computer.
3) Your browser displays the file appropriately.
4) If you request a PHP file (ends with ".php"), the server handles it differently.

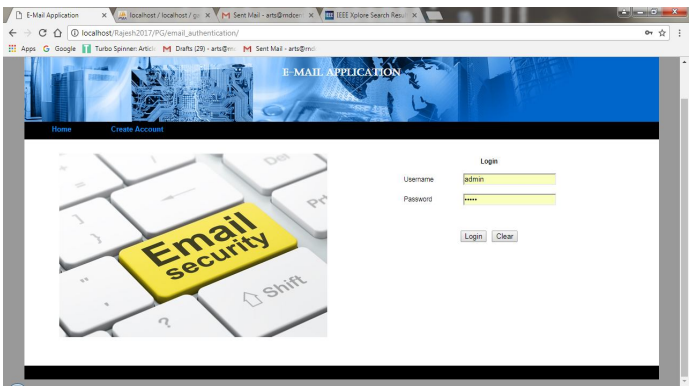
B. Accessing a PHP Page



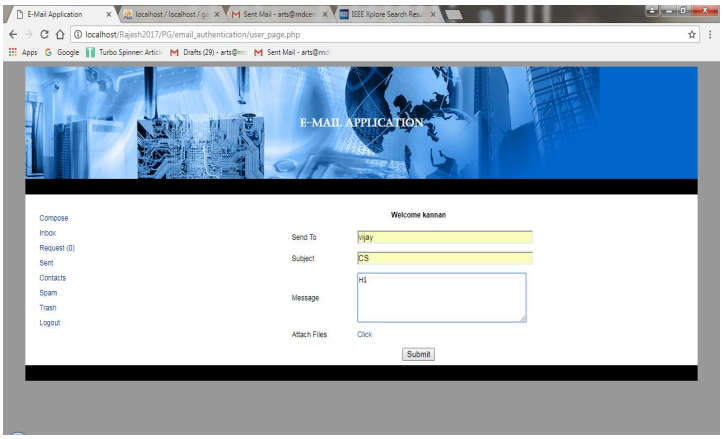
1) Your browser sends a request to that web page's server for the PHP file you wish to view.
2) The web server calls PHP to interpret and perform the operations called for in the PHP script.
3) The web server sends the output of the PHP program back to your computer.
4) Your browser displays the output appropriately.

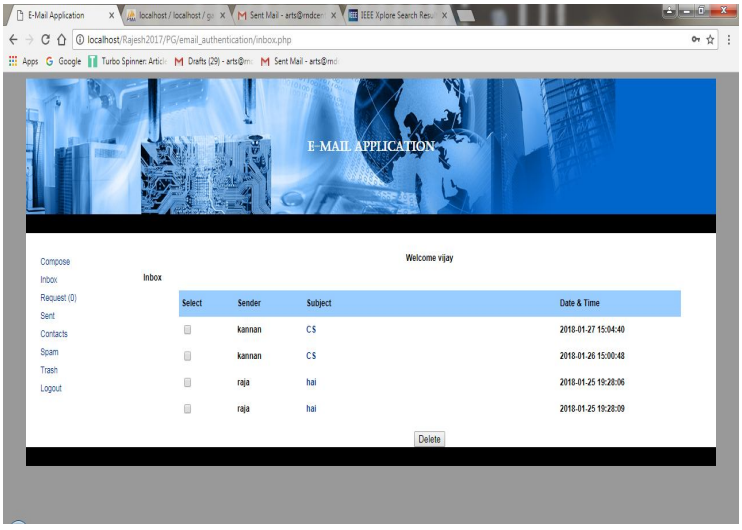
V. EXPERIMENTAL RESULTS

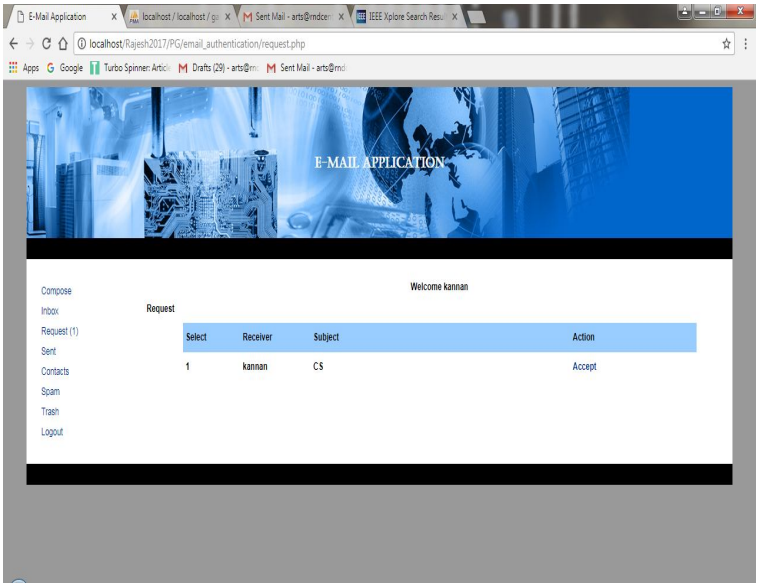
A. Main Page

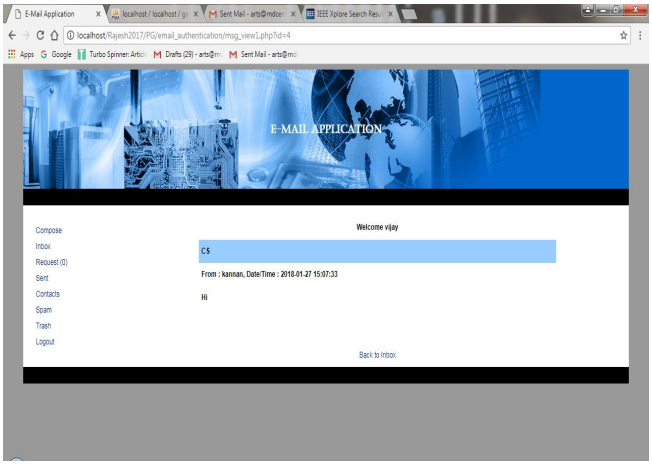


B. Mail Application









VI. CONCLUSION

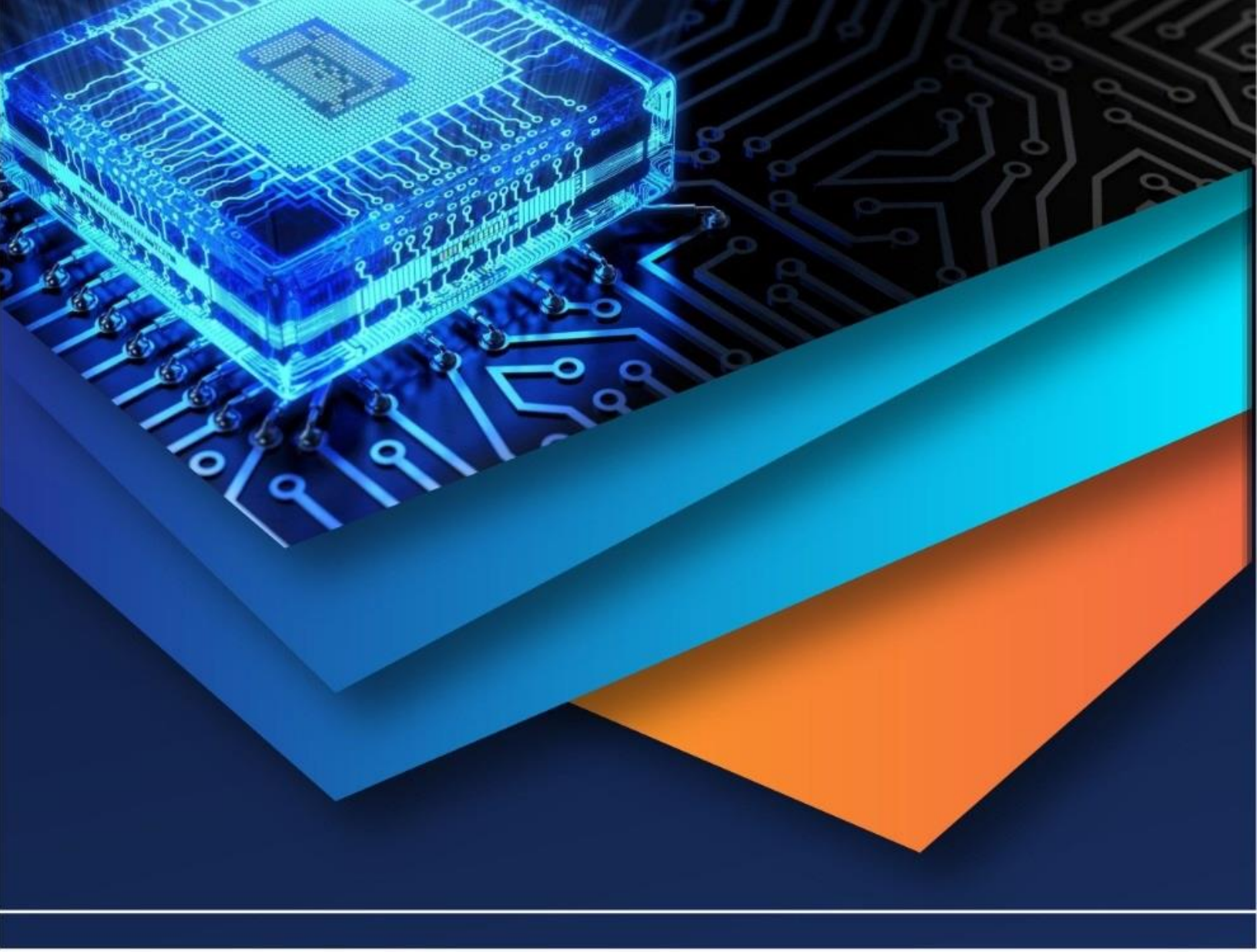
Such a demonstration yields a powerful and delegable data-leak detection framework. The cloud computing surroundings the cloud source can perform data leak detection as add on service to its customers. The assessment results show that the detection method can supports accurate detection through very miniature number of false alarms under various data leak scenarios. The benefit of this method is that it enables the data owner to safely hand over the detection operation without enlightening the sensitive data to the source.

A. Scope For Future Enhancement

The original user initially creates shared data in the cloud, and shares it with group users. Both the original user and group users are members of the group. The data owner share the data into the cloud users, and the users should be access the data securely. The data should be transmitted from the data owner on securely through network.

REFRENCES

[1] D. X. Song, D. Wagner, A. Perrig, "Practical techniques for searches on encrypted data", *Proc. IEEE Symp. Secur. Privacy*, pp. 44-55, May. 2000.
[2] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions", *Proc. ACM CCS*, pp. 79-88, 2006.
[3] D. Boneh, G. Di Crescenzo, R. Ostrovsky, G. Persiano, "Public key encryption with keyword search", *Proc. EUROCRYPT*, pp. 506-522, 2004.
[4] X. Yi, E. Bertino, J. Vaidya, C. Xing, "Private searching on streaming data based on keyword frequency", *IEEE Trans. Dependable Secure Comput.*, vol. 11, no. 2, pp. 155-167, Mar./Apr. 2014.
[5] P. Xu, H. Jin, Q. Wu, W. Wang, "Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack", *IEEE Trans. Comput.*, vol. 62, no. 11, pp. 2266-2277, Nov. 2013.
[6] R. Chen, Y. Mu, G. Yang, F. Guo, X. Wang, "A new general framework for secure public key encryption with keyword search", *Proc. ACISP*, pp. 59-76, 2015.
[7] R. Chen, Y. Mu, G. Yang, F. Guo, X. Wang, "Dual-server public-key encryption with keyword search for secure cloud storage", *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 4, pp. 789-798, Apr. 2016.
[8] M. Abdalla et al., "Searchable encryption revisited: Consistency properties relation to anonymous ibe and extensions", *Proc. CRYPTO*, pp. 205-222, 2005.
[9] D. Khader, "Public key encryption with keyword search based on K-resilient IBE", *Proc. Int. Conf. Comput. Sci. Appl. (ICCSA)*, pp. 298-308, 2006.
[10] P. Xu, Q. Wu, W. Wang, W. Susilo, J. Domingo-Ferrer, H. Jin, "Generating searchable public-key ciphertexts with hidden structures for fast keyword search", *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1993-2006, Sep. 2015.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY