ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 12, July 2017

Secure Sensitive Data Storage on Bigdata Framework

Praneet Mohanbala[1], Manisha Parida[2], Dr.Roopa R[3]

U.G. Student, Department of Information Science &Engg, BMS College of Engineering, Bangalore, India[1]

U.G. Student, Department of Information Science &Engg, BMS College of Engineering, Bangalore, India[2]

Assistant Professor, Department of Information Science &Engg, BMS College of Engineering, Bangalore, India[3]

ABSTRACT: Clients store limitless measures of delicate information on a major information stage. Sharing delicate information will help ventures diminish the cost of furnishing clients with customized benefits and offer some incentive included information administrations. Nonetheless, secure information sharing is dangerous. In this paper, we propose a structure for secure sensitive information sharing on a major information stage, including secure information conveyance, stockpiling and use on a semi-trusted enormous information sharing stage.We display an Encryption calculation in light of heterogeneous figure content change and a client prepares security strategy in view of a virtual machine screen, which offers help for the acknowledgment of framework capacities.The system ensures the security of clients' touchy information viably and offers these information securely.

KEYWORDS: secure, sensitive, structure, encryption, information.

I. INTRODUCTION

With the fast advancement of data digitization, gigantic measures of organized, semi-organized, and unstructured information are created rapidly. By gathering, sorting, investigating, and mining these information, an endeavor can acquire a lot of individual clients' delicate information. These information not just meet the requests of the undertaking itself, additionally give administrations to different organizations if the information are put away on a major information stage. Web uncertainty and the capability of touchy information spillage additionally make security issues for delicate information sharing. Secure delicate information sharing includes four essential wellbeing variables. To begin with, there are security issues when touchy information are transmitted from an information proprietor's nearby server to a major information stage. Second, there can be delicate information figuring and capacity security issues on the huge information stage. Third, there are secure delicate information utilize issues on the cloud stage. Fourth, there are issues including secure information demolition. Some exploration foundations and researchers at home and abroad have made positive commitments to investigation and research gone for taking care of these security issues.

Existing advancements have in part settled information sharing and security insurance issues from different points of view, however they have not considered the whole procedure in the full information security life cycle[5]. In any case, a major information stage is a total framework with multi partner association, and in this manner can't endure any security break bringing about delicate information misfortune.

As indicated by [1], delicate Information which frequently contain sensitive and private data imperative to the client. At that point, Non-touchy information which is not as imperative to the client as the other sort and no mischief in the event that it is distributed handled or put away[2]. In this paper, we dissect security issues including the whole delicate information sharing life cycle and depict a framework demonstrate made to guarantee secure touchy information sharing on a major information stage, to ensure secure capacity on the enormous information stage utilizing Intermediary Re-Encryption (PRE) innovation, and to guarantee secure utilization of delicate information sharing

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 12, July 2017

utilizing a private space prepare in light of a Virtual Machine Screen (VMM). At that point, a security module and an information implosion instrument help to lighten client concern with respect to touchy individual data spillage.

II. DESIGN & ANALYSIS

Model–view–controller (MVC) is a product compositional example for executing UIs on PCs. It partitions a given application into three interconnected parts keeping in mind the end goal to isolate interior portrayals of data from the ways that data is displayed to and acknowledged from the user. The MVC configuration design decouples these significant segments taking into account productive code reuse and parallel improvement.

Generally utilized for desktop graphical UIs (GUIs), this engineering has turned out to be prevalent for outlining web applications and even portable, desktop and other clients. Mainstream programming dialects like Java, C#, Ruby, PHP and others have well known MVC structures[9] that are as of now being utilized as a part of web application improvement straight out of the crate.

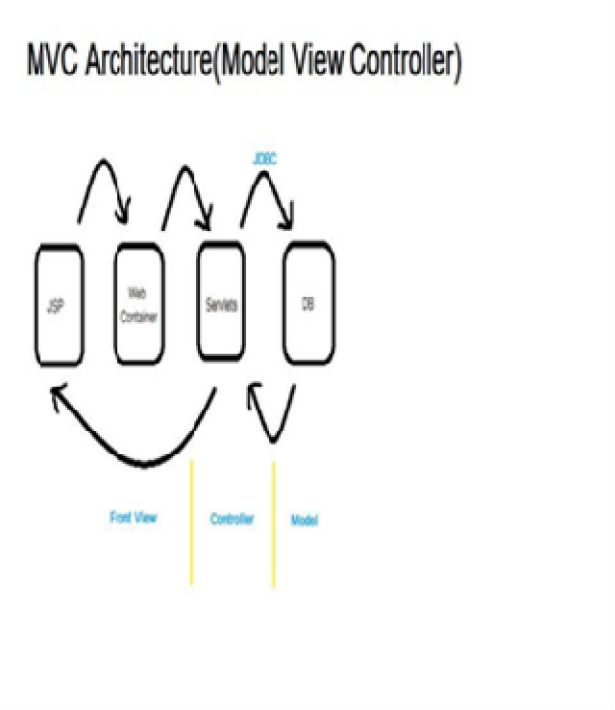


Fig (a):Model View Controller

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 12, July 2017

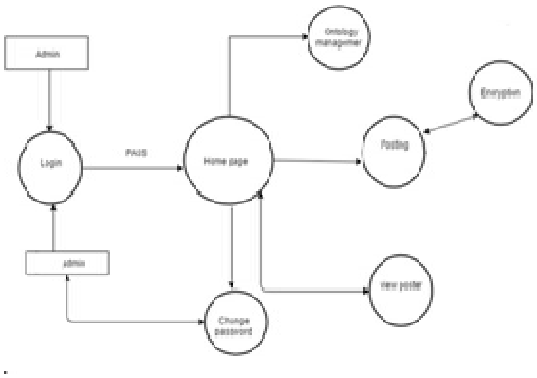


Fig (b):Homepage Design

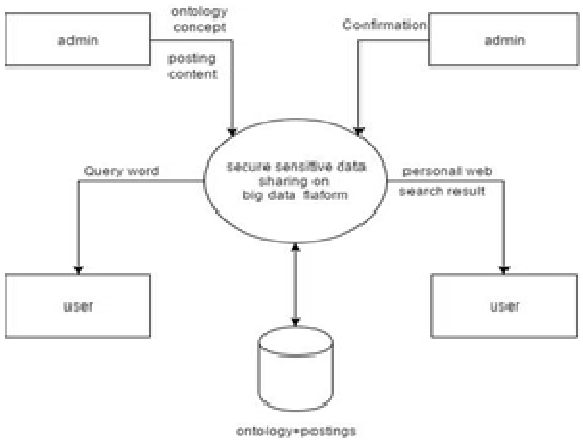


Fig (c): Secure Sensitive Data Sharing

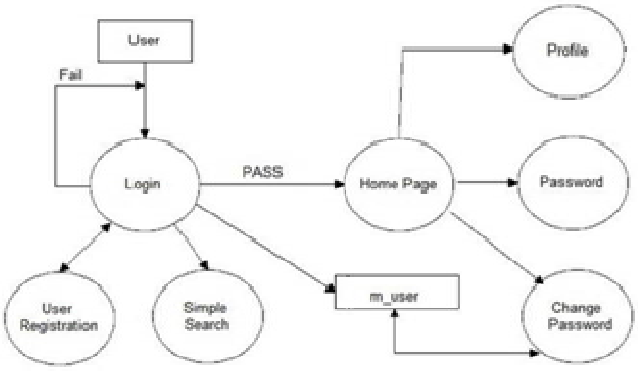


Fig (d)

III. IMPLEMENTATION

SpyNB Algorithm Pseudocode:

Step 1: Get the query keyword from the user Let it be K

Step 2: Compare K with Post Link Content Keywords & Extract the Result Set RS.

Step 3: Re-rank the RS with Location Ontology concept

Step 4: List the Re-ranked RS to User Display.

Step 5: Record the Links which are selected by the users.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 12, July 2017

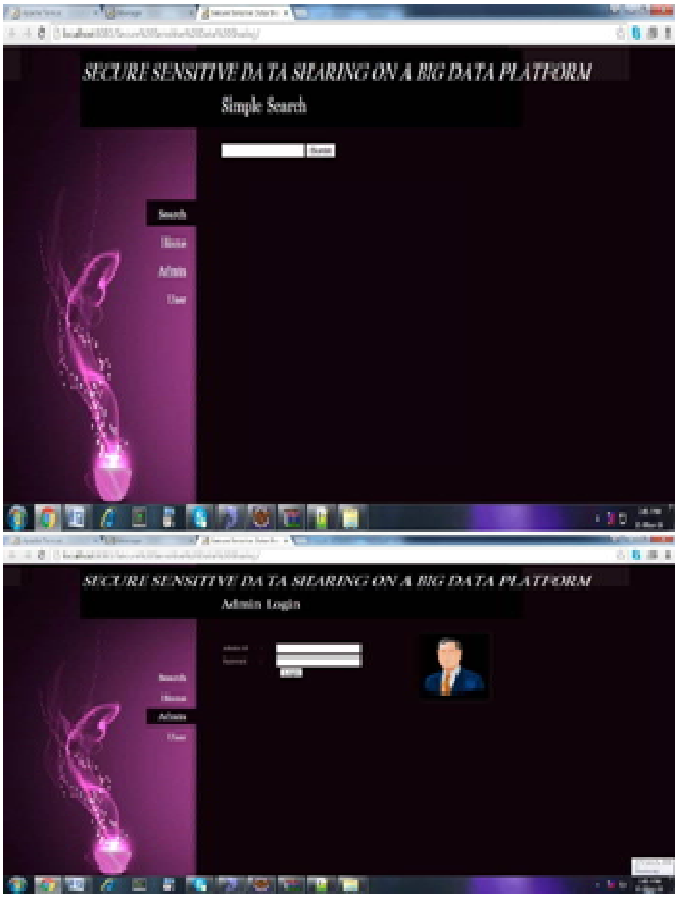
Step 6: Let clicked Result Subset is Positive Set and un-clicked Result sub sets are Negative Set for that search.

Step 7: Record Positive Set and Negative Set in that User Account

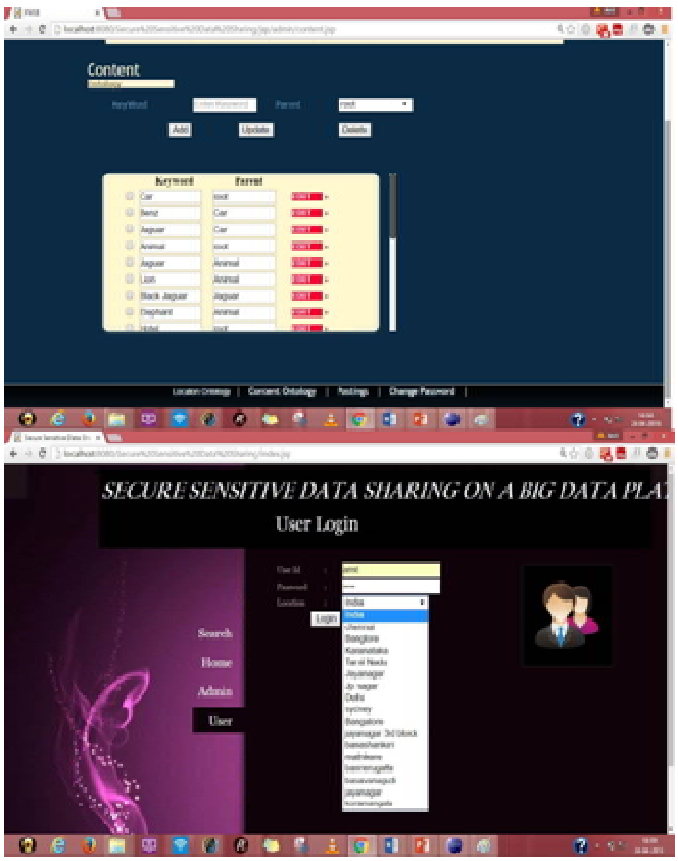
Step 8: Repeat the process for all the search queries.

Step 9: Stop

IV. RESULTS



(a)



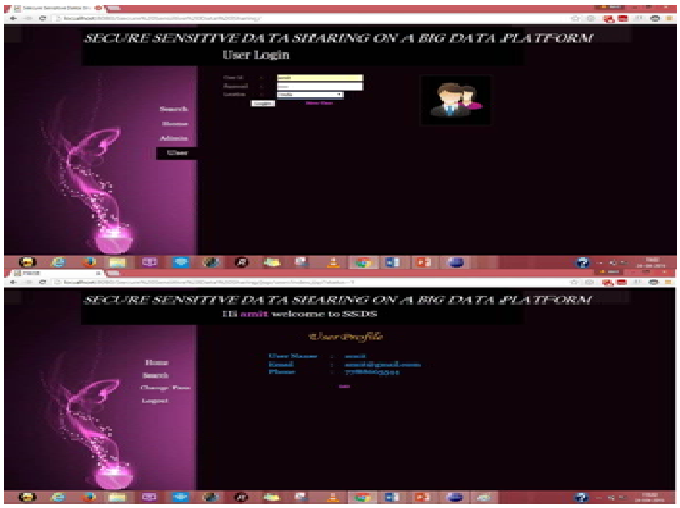
(b)

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

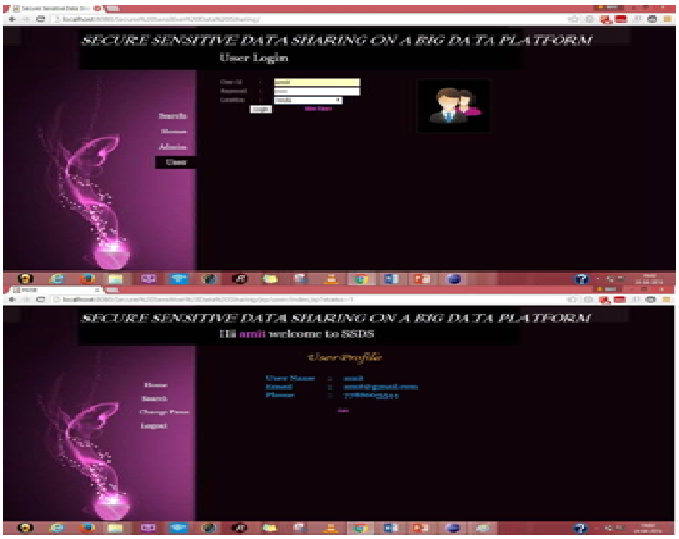
International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

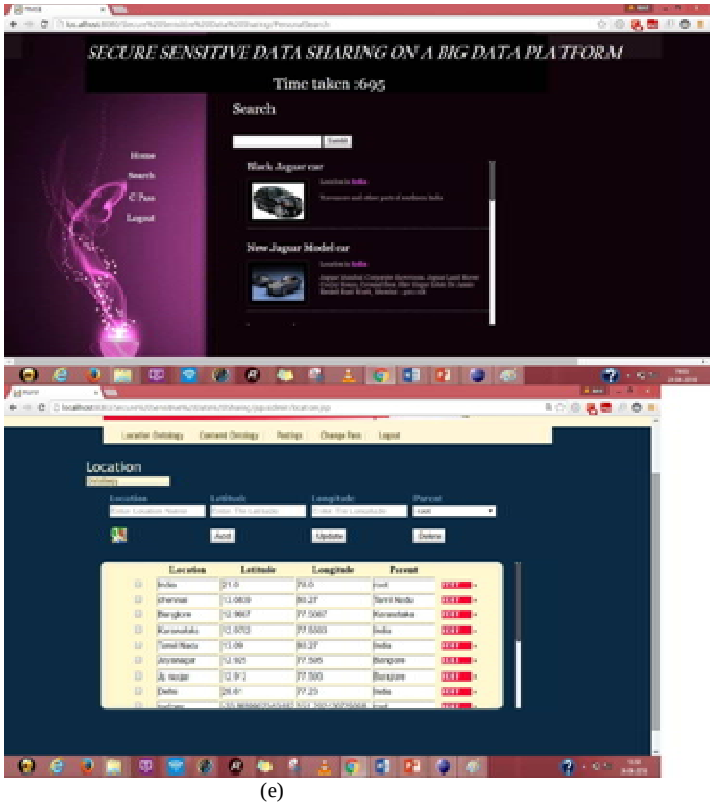
Vol. 6, Special Issue 12, July 2017



(c)



(d)



(e)

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 12, July 2017

V.TESTING

Table 1: Unit testing

Sl # Test Case : -	UTC-1
Name of Test: -	Login as Admin
Items being tested:-	Admin model
Sample Input: -	Correct Username & Password is given as inputs
Expected output: -	Depending on the correct inputs, it must login as Admin
Actual output:-	Login successful
Remarks: -	Pass.

Table 2: Integration Test 1

Sl # Test Case : -	UTC-2
Name of Test: -	Login as User
Items being tested:-	User model
Sample Input: -	Incorrect Username & Password is given as inputs
Expected output: -	Depending on the incorrect inputs, it shouldn't login as user
Actual output:-	Login Failed
Remarks: -	Pass.

Table 3: Integration Test 2

Sl # Test Case : -	ITC-1
Name of Test: -	Change password for Admin
Items being tested:-	Admin & User model
Sample Input: -	Incorrect Old password ,given new password
Expected output: -	Failed to update new password
Actual output:-	Password Update failed
Remarks: -	Pass.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 12, July 2017

VI. CONCLUSION

We proposed a systematic frame work of securely sharing sensitive data on big data platform, this ensures secure submission and storage of valuable data based on the encryption algorithm The proposed personalized web search protects the security off users' valuable private data. At the same time the data owners have all of the control of their data to get personalization on their searched data. The framework protects the security of users' sensitive data effectively and shares these data safely. At the same time, data owners retain complete control of their own data in a sound environment for modern Internet information security.

REFERENCES

[1]L. Dong, Y. Zhuang, Y. Gao, and Y. Bu, Research on real- time trigger system for sensitive data safe destruction, (in Chinese), Journal of Chinese Computer System, vol. 31, no. 7
[2]J. Qin, Q. Deng, and J. Zhang, Design of multi-grade safety data destruction mechanism of HDFS, (in Chinese), Computer Technology and Development, vol. 23, no. 3
[3]F. Zhang, J. Chen, H. Chen, and B. Zang, Lifetime privacy and self-destruction of data in the cloud, (in Chinese), Journal of Computer Research and Development, vol. 48, no. 7
[4]S. Razick, R. Mocnik, L. F. Thomas, E. Ryeng, F. Drabløs, and P. Sætrom, The eGenVar data management system — Cataloguing and sharing sensitive data and metadata for the life sciences, Database, vol. 2014, p. bau027, 2014.
[5]J. Yang and K. G. Shin, Using hypervisor to provide data secrecy for user applications on a per-page basis, in Proc. 4th Int. Conf. on Virtual Execution Environments, Seattle, USA, 2008.
[6]H. Chen, F. Zhang, C. Chen, Z. Yang, R. Chen, B. Zang, W. Mao, H. Chen, F. Zhang, C. Chen, et al., Tamper- resistant execution in an untrusted operating system using a virtual machine monitor, Technical Report, Parallel Processing Institute, Fudan University, FDUPPITR-2007- 0801, 2007.
[7]P. Dewan, D. Durham, H. Khosravi, M. Long, and G. Nagabhushan, A hypervisor-based system for protecting software runtime memory and persistent storage, in Proc. the 2008 Spring Simulation Multiconference, Ottawa, Canada, 2008
[8]G. Wang, F. Yue, and Q. Liu, A secure self-destructing scheme for electronic data, Journal of Computer and System Sciences, vol. 79
[9]D. Feng, Y. Qin, D. Wang, and X. Chu, Research on trusted computing technology, (in Chinese), Journal of Computer Research and Development, vol. 48, no. 8
[10]F. Zhang, J. Chen, H. Chen, and B. Zang, Cloudvisor: Retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization, in Proc. 23rd ACM Symposium on Operating Systems Principles, Cascais, Portugal, 2011
[11]X. Chen, T. Garfinkel, E. C. Lewis, and B. Spasojevic, Overshadow: A virtualization-based approach to retrofitting protection in commodity operating systems, in Proc. 13th Int. Conf. on Architectural Support for Programming Languages and Operating Systems, Seattle, USA, 2008.