



SECUREDATA GROUP SHARINGAND CONDITIONAL DISSEMINATION WITH MULTI-OWNERIN CLOUD COMPUTING

Dr.C.Parthasarathy, Mr. Md. Ateeq Ur Rahman , Mr. BOKAM RAO , Mr. Mohd Hussain

Department of Computer Science and Engineering,Shadan College of Engineering and Technology HYD,T.S,INDIA"

ABSTRACT With the rapid development of cloud services, huge volume of data is shared via cloud computing. Although cryptographic techniques have been utilized to provide data confidentiality in cloud computing, current mechanisms cannot enforce privacy concerns over cipher text associated with multiple owners, which makes co-owners unable to appropriately control whether data disseminators can actually disseminate their data. In this paper, we propose a secure data group sharing and conditional dissemination scheme with multi-owner in cloud computing, in which data owner can share private data with a group of users via the cloud in a secure way, and data disseminator can disseminate the data to a new group of users if the attributes satisfy the access policies in the cipher text. We further present a multiparty access control mechanism over the disseminated cipher text, in which the data co-owners can append new access policies to the cipher text due to their privacy preferences.

Moreover, three policy aggregation strategies, including full permit, owner priority and majority permit, are provided to solve the privacy conflicts problem caused by different access policies. The security analysis and experimental results show our scheme is practical and efficient for secure data sharing with multi-owner in cloud computing.

1. INTRODUCTION

The popularity of cloud computing is obtained from the benefits of rich storage resources and instant access. It aggregates the resources of computing infrastructure, and then provides on-demand services over the Internet. Many famous companies are now providing public cloud services, such as Amazon, Google, Alibaba. These services allow individual users and enterprise users to upload data (e.g. photos, videos and documents) to cloud service provider (CSP), for the purpose of accessing the data at any time anywhere and sharing the data with others. In order to protect the privacy of users, most cloud services achieve access control by maintaining access control list (ACL). In this way, users can choose to either publish their data to anyone or grant access rights merely to their approved people. However, the security risks have raised concerns in people, due to the data is stored in plaintext form by the CSP. Once the data is posted to the CSP, it is out of the data owner's control. Unfortunately, the CSP is usually a semi-trusted server which honestly follows the designated protocol, but might collect the users' data and even use them for benefits without users' consents. On the other hand, the data has tremendous usages by various data consumers to learn the behavior of users. These security issues motivate the effective solutions to protect data confidentiality. It is essential to adopt access control mechanisms to achieve secure data sharing in cloud computing. Currently, cryptographic mechanisms such as attribute-based encryption (ABE), identity-based broadcast encryption (IBBE), and remote attestation have been exploited to settle these security and privacy problems. ABE is one of the new cryptographic mechanisms used in cloud computing to reach secure and finegrained data sharing. It features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among decryption keys and cipher texts. As long as the attribute set satisfies the access policy that the cipher text can be decrypted. IBBE is another prevalent technique employed in cloud computing, in which users could share their encrypted data with multiple receivers at one time and the public key of the receiver can be regarded as any valid strings, such as unique identity and email. In fact, IBBE can be seen as a special case of ABE for policies consisting of an OR gate. Compared to ABE in which the secret key and cipher text are both correspond to a set of attributes, IBBE incurs low-cost key management and small constant policy sizes, which is more suitable for securely broadcasting data to specific receivers in cloud computing. Hence, by using identities, data owner can share data with a group of users in a secure and efficient manner, which motivates more users to share their private data via cloud.

2. OVERVIEW

We further present a multiparty access control mechanism over the disseminated ciphertext, in which the data co-owners can append new access policies to the ciphertext due to their privacy preferences. Moreover, three policy

Research Paper

Available online at: www.ijsrset.com

UGC Approved Journal No: 45483

aggregation strategies, including full permit, owner priority and majority permit, are provided to solve the privacy conflicts problem caused by different access policies. The security analysis and experimental results show our scheme is practical and efficient for secure data sharing with multi-owner in cloud computing.

➤ In this paper, we aim at presenting a novel data protection scheme by combining fragmentation, encryption, and dispersion with high performance and enhanced level of protection.

➤ Fragmentation methods are introduced for data storage in a cost-effective manner using a public Cloud for the less confidential data fragments.

➤ Our method can provide both, data storage cost effectiveness and prevention of any information leak from the storage in a public Cloud.

3. REQUIREMENTS

3.1 HARDWARE REQUIREMENT:

- PROCESSOR : PENTIUM IV 2.6 GHz, Intel Core 2 Duo.
- RAM : 512 MB DD RAM
- MONITOR : 15" COLOR
- HARD DISK : 40 GB

3.2 SOFTWARE REQUIREMENT

- Front End : J2EE (JSP, SERVLET)
- Back End : MY SQL 5.5
- Operating System : Windows 7
- IDE : Eclipse

3.3 FUNCTIONAL REQUIREMENTS

A functional requirement defines a function of a software-system or its component. A function is described as a set of inputs, the behaviour, and outputs. The outsourced computation is data is more secured. In this paper, we propose a secure data group sharing and conditional dissemination scheme with multi-owner in cloud computing, in which data owner can share private data with a group of users via the cloud in a secure way, and data disseminator can disseminate the data to a new group of users if the attributes satisfy the access policies in the ciphertext. We further present a multiparty access control mechanism over the disseminated ciphertext, in which the data co-owners can append new access policies to the ciphertext due to their privacy preferences.

➤ Proxy Agents: ▪ Proxy Agent Console ▪ Customer's Requirements ▪ Customers Request ➤ Customers: ▪ User Console ▪ Send Requirements.

3.4 NON-FUNCTIONAL REQUIREMENTS

:The major non-functional Requirements of the system are as follows ➤ Usability

The system is designed with completely automated process hence there is no or less user intervention. ➤ Reliability

The system is more reliable because of the qualities that are inherited from the chosen platform java. The code built by using java is more reliable. ➤ Performance

This system is developing in the high level languages and using the advanced front-end and back-end technologies it will give response to the end user on client system with in very less time. ➤ Supportability

The system is designed to be the cross platform supportable. The system is supported on a wide range of hardware and any software platform, which is having JVM, built into the system. ➤ Implementation

The system is implemented in web environment using struts framework. The apache tomcat is used as the web server and windows xp professional is used as the platform. Interface the user interface is based on Struts provides HTML Tag

4. BRIEF NOTE ON DESIGN ENGINEERING

Design Engineering deals with the various UML [Unified Modelling language] diagrams for the implementation of project. Design is a meaningful engineering representation of a thing that is to be built. Software design is a process through which the requirements are translated into representation of the software. Design is the place where quality is rendered in software engineering. Design is the means to accurately translate customer requirements into finished product.

- 4.1 GENERAL
- 4.2 USECASE DIAGRAM
- 4.3 CLASSDIAGRAM
- 4.4 OBJECTDIAGRAM

- 4.5 STATEDIAGRAM
- 4.6 SEQUENCED DIAGRAM
- 4.7 ACTIVITY DIAGRAM
- 4.8 COMPONENTDIAGRAM
- 4.9 DATAFLOW DIAGRAM
- 4.10 E-RDIAGRAM
- 4.11 DEPLOYMENTDIAGRAM
- 4.12 SYSTEM ARCHITECTURE

5. APPLICATIONS AND FUTURE ENHANCEMENTS

5.1 APPLICATION

The data owner can choose a policy aggregation strategy and define an access policy to enforce dissemination conditions. Then he encrypts data for a set of receivers, and outsources the ciphertext to CSP for sharing and dissemination. The data co-owners tagged by data owner can append access policies to the encrypted data with CSP and generate the renewed ciphertext. The data disseminator can access the data and also generate the reencryption key to disseminate data owner's data to others if he satisfies enough access policies in the ciphertext. The data accessory can decrypt the initial, renewed and re-encrypted ciphertext with her or his private key.

5.2 FUTURE ENHANCEMENT

We further present a multiparty access control mechanism over the ciphertext, which allows the data coowners to append their access policies to the ciphertext. Besides, we provide three policy aggregation strategies including full permit, owner priority and majority permit to solve the problem of privacy conflicts. In the future, we will enhance our scheme by supporting keyword search over the ciphertext.

6. CONCLUSION & REFERENCE

6.1 CONCLUSION

The data security and privacy is a concern for users in cloud computing. In particular, how to enforce privacy concerns of multiple owners and protect the data confidentiality becomes a challenge. In this paper, we present a secure data group sharing and conditional dissemination scheme with multi-owner in cloud computing. In our scheme, the data owner could encrypt her or his private data and share it with a group of data accessors at one time in a convenient way based on IBBE technique. Meanwhile, the data owner can specify fine-grained access policy to the ciphertext based on attribute-based CPRE, thus the ciphertext can only be re-encrypted by data disseminator whose attributes satisfy the access policy in the ciphertext.

REFERENCE:

1. Z. Yan, X. Li, M. Wang, and A. V. Vasilakos, "Flexible data access control based on trust and reputation in cloud computing," *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 485-498, 2017.
2. B. Lang, J. Wang, and Y. Liu, "Achieving flexible and self-contained data protection in cloud computing," *IEEE Access*, vol. 5, pp. 1510-1523, 2017.
3. Q. Zhang, L. T. Yang, and Z. Chen, "Privacy preserving deep computation model on cloud for big data feature learning," *IEEE Transactions on Computers*, vol. 65, no. 5, pp. 1351-1362, 2016.
4. H. Cui, X. Yi, and S. Nepal, "Achieving scalable access control over encrypted data for edge computing networks," *IEEE Access*, vol. 6, pp. 30049-30059, 2018.
5. K. Xue, W. Chen, W. Li, J. Hong, and P. Hong, "Combining data owner-side and cloud-side access control for encrypted cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2062-2074, 2018.
6. C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys," *Proc. International Conf. on the Theory and Application of Cryptology and Information Security (ASIACRYPT'2007)*, pp. 200-215, 2007.
7. N. Paladi, C. Gehrman, and A. Michalas, "Providing user security guarantees in public infrastructure clouds," *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 405-419, 2017.
8. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," *Proc. IEEE Symposium on Security and Privacy (SP'07)*, pp. 321-334, 2007.
9. L. Liu, Y. Zhang, and X. Li, "KeyD: secure key-deduplication with identity-based broadcast encryption," *IEEE Transactions on Cloud Computing*, 2018, <https://ieeexplore.ieee.org/document/8458136>.
10. Q. Huang, Y. Yang, and J. Fu, "Secure data group sharing and dissemination with attribute and time conditions in Public Clouds," *IEEE Transactions on Services Computing*, 2018, <https://ieeexplore.ieee.org/document/8395392>.
11. Box, "Understanding collaborator permission levels", <https://community.box.com/t5/Collaborate-By-Inviting-Others/Understanding-Collaborator-Permission-Levels/ta-p/144>.

12. Microsoft OneDrive, "Document collaboration and co-authoring", <https://support.office.com/en-us/article/document-collaboration-and-co-authoring-ee1509b4-1f6e-401e-b04a-782d26f564a4>.
13. H.He,R.Li,X.Dong,andZ.Zhang,"Secure,efficientandfinegraineddataaccesscontrolmechanismforP2Pstoragecloud,"IEEE Transactionson Cloud Computing, vol.2, no.4, pp. 471-484, 2014.
14. Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, "A survey of proxy reencryption for secure data sharing in cloudcomputing,"IEEETransactionsonServicesComputing,2018,<https://ieeexplore.ieee.org/document/7448446>.
15. J. Son, D. Kim, R. Hussain, and H. Oh, "Conditional proxy reencryption for secure big data group sharing in cloudenvironment,"Proc.of2014IEEEConferenceonComputerCommunicationsWorkshops(INFOCOMWKSHPs),pp.541-546, 2014.
16. L.Jiang,andD.Guo"Dynamicencrypteddatasharingschemebasedonconditionalproxybroadcastre-encryptionforcloudstorage,"IEEE Access, vol.5, pp. 13336-13345, 2017.
17. K.Liang,M.H.Au,J.K.Liu,W.Susilo,D.S.Wong,G.Yang,Y.Yu,andA.Yang,"Asecureandefficientciphertext-policy attribute-based proxy re-encryption for cloud data sharing," Future Generation Computer Systems, vol. 52, pp. 95-108, 2015.
18. X.Li,Y.Zhang,B.Wang,andJ.Yan,"Mona:securemulti-ownerdatasharingfordynamicgroupsinthecloud,"IEEETransactionson Paralleland Distributed Systems,vol.24,no. 6, pp. 1182-1191,2013.
19. K. Xu, Y. Guo, L. Guo, Y. Fang, and X. Li, "My privacy my decision: control of photo sharing on online socialnetworks," IEEE Trans. OnDependableand Secure Computing,vol. 14, no.2, pp.199-210, 2017.
20. K. Thomas, C. Grier, and D. M. Nicol, "UnFriendly: multi-party privacy risks in social networks," Proc. InternationalSymposium on PrivacyEnhancing Technologies Symp.(PETS'2010), pp. 236-252, 2010.
21. L.Fang,L.Yin,Y.Guo,Z.Wang,andFenzhuaLi,"Resolvingaccessconflicts:anauction-basedincentiveapproach,"Proc.IEEE MilitaryCommunications Conference (MILCOM),pp. 1-6, 2018.
22. L. Xu, C. Jiang, N. He, Z. Han, and A. Benslimane, "Trust-based collaborative privacy management in online socialnetworks,"IEEE Transactions onInformation Forensics andSecurity, vol. 14, no.1, pp. 48-60, 2019.
23. C.GentryandB.Waters,"Adaptivesecurityinbroadcastcryptosystems(withshortciphertexts),"Proc.28thAnn.International Conf. on Advances in Cryptology: the Theory and Applications of Cryptographic (EUROCRYPT '09), pp.171-188, 2009.
24. Q.Huang,W.Yue,Y.He,andY.Yang,"Secureidentity-baseddatasharingandprofilematchingformobilehealthcaresocial networksincoudcomputing," IEEE Access, vol.6, pp.36584-36594,2018.
25. S. Patranabis, Y. Shrivastava, and D. Mukhopadhyay, "Provably secure key-aggregate cryptosystems with broadcastaggregatekeys foronlinedatasharingonthecloud,"IEEETransactionsonComputers,vol.66,no.5,pp.891-904,2017.
26. A. Sahai and B. Waters, "Fuzzy identity-based encryption," Proc. 24th Ann. International Conf. on Theory andApplicationsofCryptographicTechniques (EUROCRYPT'05), pp. 457-473,2005.
27. V.Goyal,O.Pandey,A.Sahai,andB.Waters,"Attribute-basedencryptionforfine-grainedaccesscontrolofencrypteddata,"Proc. 13th ACMConf. on Computerand Communications Security(CCS'06), pp.89-98,2006.
28. S. Wang, K. Liang, J. K. Liu, J. Chen, J. Yu, and W. Xie, "Attribute based data sharing scheme revisited in cloudcomputing,"IEEE Transactionson InformationForensicsandSecurity, vol.11, no.8, pp.1661-1673, 2016.
29. L.Guo,C.Zhang,H.Yue,andY.Fang,"Aprivacy-preservingsocialassistedmobilecontentdisseminationschemeinDTNs,"Proc.32ndIEEEInternationalConf.onComputer Communications(INFOCOM'2013),pp.2301-2309,2013.
30. W. Teng, G. Yang, Y. Xiang, T. Zhang, and D. Wang, "Attribute based access control with constant-size ciphertext incloudcomputing,"IEEE Transactions on CloudComputing, vol. 5, no.4,pp.617-627, 2017.
31. Y. Zhang, D. Zheng, and R. H. Deng, "Security and privacy in smart health: efficient policy-hiding attribute-basedaccess control," IEEE Internetof ThingsJournal,vol.5, no. 3, pp. 2130-2145,2018.
32. K. Seol, Y. Kim, E. Lee, Y. Seo, and D. Baik, "Privacy-preserving attribute- based access control model for XML-basedelectronic healthrecord system,"IEEE Access,vol. 6, pp. 9114-9128, 2018.
33. M.GreenandG.Ateniese,"Identity-basedproxyre-encryption,"Proc.5thInternationalConf.onAppliedryptographyandNetworkSecurity(ACNS '07),pp.288-306,2007.
34. Y. Zhou, H. Deng, Q. Wu, B. Qin, J. Liu, and Y. Ding, "Identity-based proxy re-encryption version 2: Making mobileaccess easyin cloud,"Future Generation ComputerSystems,vol.62, pp.128-139,2016.
35. J.Weng,R.H.Deng,X.Ding,C.K.Chu,andJ.Lai,"Conditionalproxyre-encryptionsecureagainstchosen-ciphertextattack,"inProc.of4thInternationalSymposiumonInformation,Computer,andCommunicationsSecurity(ASIACCS'09),pp. 322-332, 2009.
36. P. Xu, T. Jiao, Q. Wu, W. Wang, and H. Jin, "Conditional identity based broadcast proxy re-encryption and itsapplicationtocloudemail,"IEEE Trans.on Computers, vol. 65, no.1,pp. 66-79, 2016.
37. Y. Yang, H. Lu, J. Weng, Y. Zhang, and K. Sakurai, "Fine-grained conditional proxy re-encryption and application,"Proc.InternationalConf. on ProvableSecurity(ProvSec '2014),pp.206-222,2014.
38. K. Wang, J. Yu, X. Liu and S. Guo, "A pre-authentication approach to proxy re-encryption in big data context," IEEETransactionson Big Data,2018,<https://ieeexplore.ieee.org/document/7921569>.

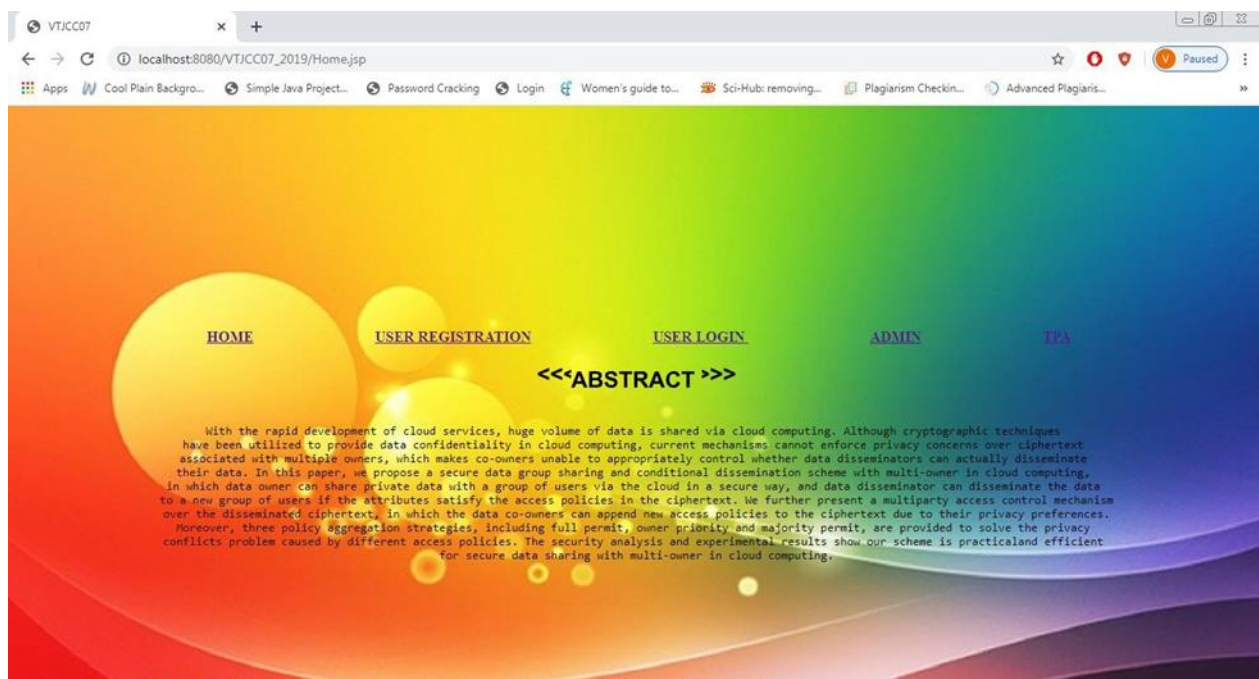
Research Paper

Available online at: www.ijsrset.com

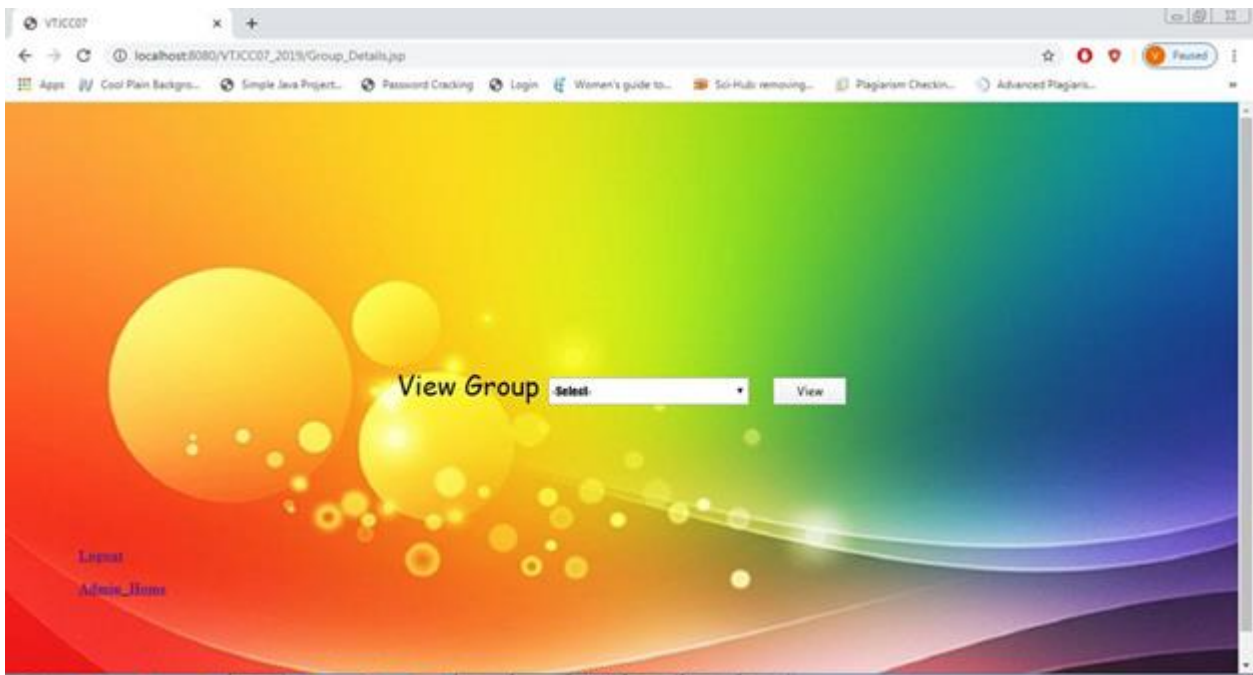
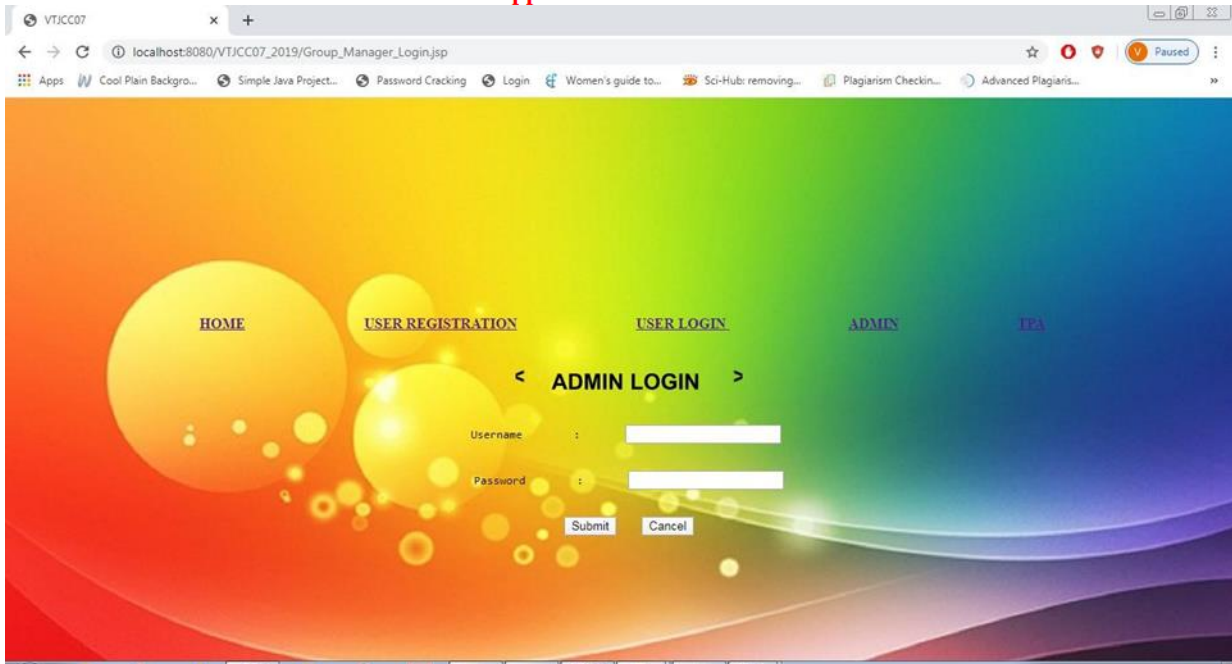
UGC Approved Journal No: 45483

39. H. Hu, G. J. Ahn, and J. Jorgensen, "Detecting and resolving privacy conflicts for collaborative data sharing in onlinesocial networks,"Proc.27th Ann.Computer SecurityApplications Conf.(ACSAC'11),pp. 103-112,2011.
40. J. M. Such and N. Criado, "Resolving multi-party privacy conflicts in social media," IEEE Trans. on Knowledge andData Engine, vol. 28, no. 7, pp. 1851-1863, 2016. Transactions on Information Forensics and Security, vol. 14, no. 1, pp.48-60, 2019.
41. H. Hu, G. Ahn, and J. Jorgensen, "Multiparty access control for online social networks: Model and mechanisms,"IEEETrans. on Knowledgeand Data Engine, vol.25,no. 7, pp. 1614-1627, 2013.
42. Q.Huang,Y.Yang,andM.Shen,"Secureandefficientdatacollaborationwithhierarchicalattribute-basedencryptionincloud computing,"Future Generation Computer Systems, vol.72,pp. 239-249,2017.
43. J.Hur,"Improvingsecurityandefficiencyinattribute-baseddatasharing,"IEEETrans.onKnowledgeandDataEng.,vol. 25,no. 10,pp. 2271-2282, 2013.
44. K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," IEEETransactionson Paralleland Distributed Systems,vol.25, no. 7, pp.1735-1744, 2014.
45. S. Jiang, T. Jiang, and L. Wang, "Secure and efficient cloud data deduplication with ownership management," IEEETransactionsonServicesComputing, <https://ieeexplore.ieee.org/document/8100969>
46. B.Lynn.Thepairing-basedcryptographylibrary.[Online].Available:<http://crypto.stanford.edu/pcb/>,accessedMarch1, 2018.
47. A.Michalas,"Thelordoffheshares:combiningattribute-basedencryptionandsearchableencryptionforflexibledatasharing,"Proc.34thACM/SIGAPPSymposium On Applied Computing(SAC), pp.146-155, 2019.
48. P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with fuzzy keyword search: a provably secure schemeunderkeyword guessing attack," IEEE TransactionsonComputers, vol. 62,no. 11, pp.2266-2277, 2013

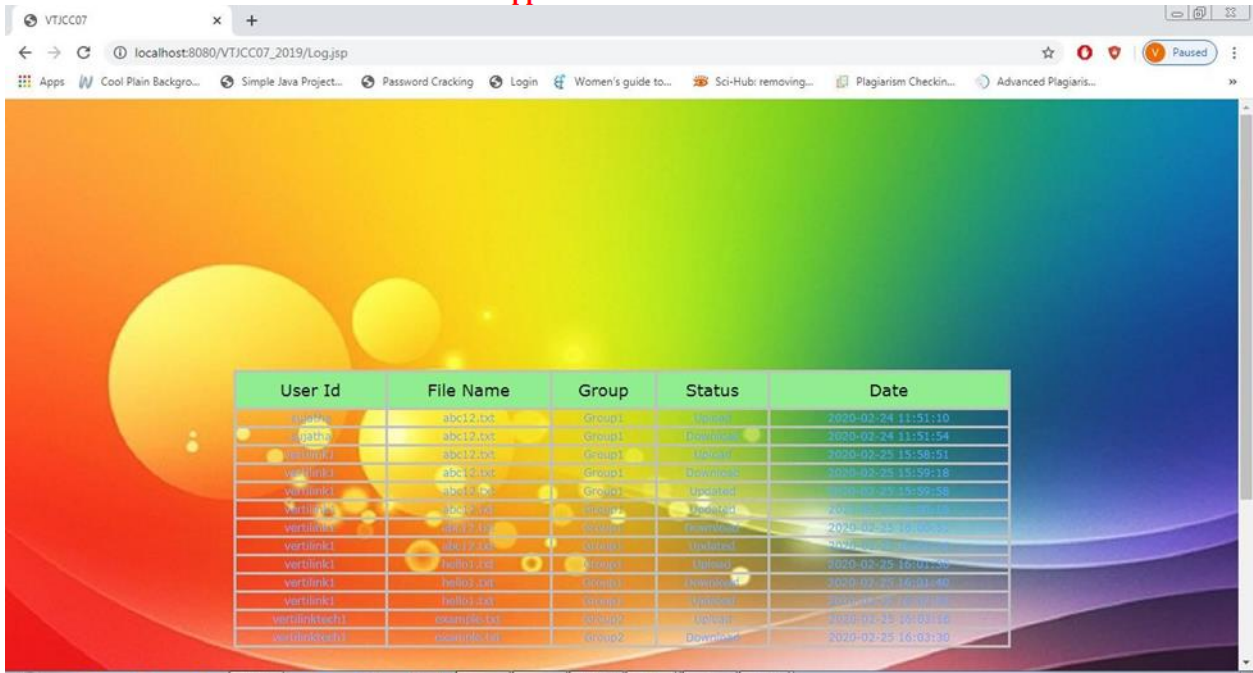
APPLICATION SNAPSHOTS:



Research Paper
Available online at: www.ijrrset.com
UGC Approved Journal No: 45483



Research Paper
Available online at: www.jrset.com
UGC Approved Journal No: 45483



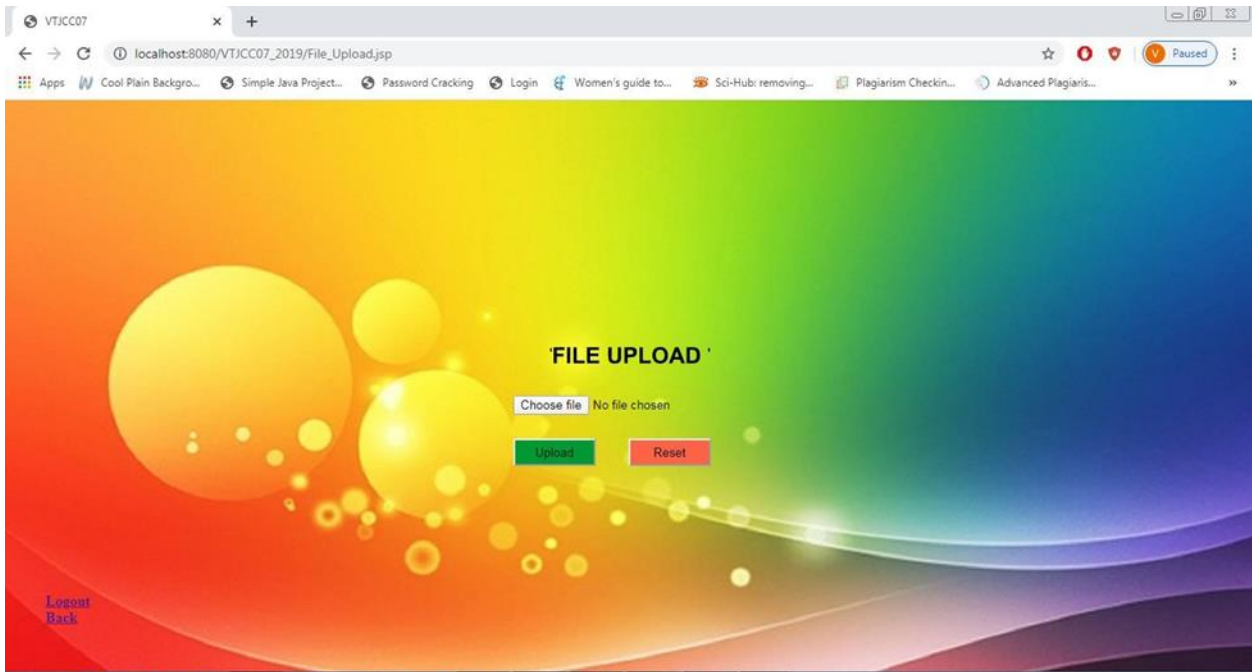
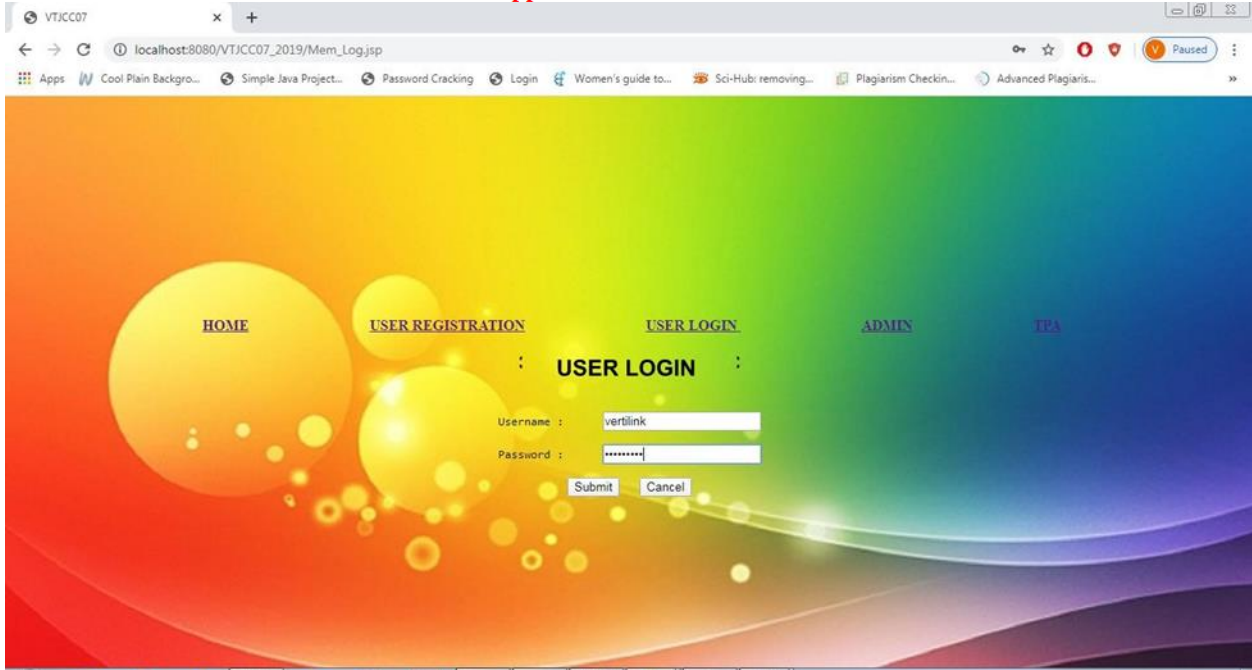
User Id	File Name	Group	Status	Date
vertlink	abc12.txt	Group1	Upload	2020-02-24 11:51:10
gpath	abc12.txt	Group1	Download	2020-02-24 11:51:54
vertlink	abc12.txt	Group1	Upload	2020-02-25 15:58:51
vertlink	abc12.txt	Group1	Download	2020-02-25 15:59:16
vertlink	abc12.txt	Group1	Updated	2020-02-25 15:59:58
vertlink	abc12.txt	Group1	Deleted	2020-02-25 16:01:14
vertlink	abc12.txt	Group1	Deleted	2020-02-25 16:01:22
vertlink	abc12.txt	Group1	Deleted	2020-02-25 16:01:30
vertlink	abc12.txt	Group1	Upload	2020-02-25 16:01:38
vertlink	abc12.txt	Group1	Download	2020-02-25 16:01:46
vertlink	abc12.txt	Group1	Download	2020-02-25 16:01:54
vertlinktech	example.txt	Group2	Upload	2020-02-25 16:03:16
vertlinktech	example.txt	Group2	Download	2020-02-25 16:03:30



[HOME](#) [USER REGISTRATION](#) [USER LOGIN](#) [ADMINS](#) [DB](#)

<USER REGISTRATION >

User name :
 Password :
 Group :
 E-mail :
 Contact No. :
 Place :





Research Paper

Available online at: www.jrrset.com

UGC Approved Journal No: 45483

