IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DESIGN AND ANALYSIS OF CLOUD DATA SECURITY FOR MASSES

NAKARABOYINA SANKAR [#1], L. SOWJANYA [#2]

[#1] MCA Student, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

[#2] Assistant Professor, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

ABSTRACT

In present days cloud has gained a lot of importance in storing and accessing the information through remote locations with the help of internet .The primary advantage of adopting this cloud computing domain for business and firms is mainly because the service can be accessed from anywhere, time independent and remote access with the help of secure internet connection. Since this was mostly adopted by several clients for storing and accessing their valuable information still it is having a problem like data theft to misuse the sensitive data by modifying the content illegally. Here we try to design DSaaS (Data Security as a Service) by integrating two main techniques called Data Encryption and Verification using TPA (Third Party Auditor) in order to protect the data from un-authorized users. This DSaaS service offered by a cloud platform enforces data security and privacy to data owners, even if there are any compromised applications or users present within the cloud storage .

1. INTRODUCTION

CLOUD computing is a paradigm that provides massive computation capacity and huge memory space at a low cost [1]. It enables users to get intended services irrespective of time and location across multiple platforms (e.g., mobile devices, personal computers), and thus brings great convenience to cloud users. Among numerous services provided by cloud computing, cloud storage service, such as Apple's iCloud [2], Microsoft's Azure [3] and Amazon's S3 [4], can offer a more flexible and easy way to share data over the

Internet, which provides various benefits for our society [5], [6]. However, it also suffers from several security threats, which are the primary concerns of cloud users [7].

Firstly, outsourcing data to cloud server implies that data is out control of users. This may cause users' hesitation since the outsourced data usually contain valuable and sensitive information. Secondly, data sharing is often implemented in an open and hostile environment, and cloud server would become a target of attacks. Even worse, cloud server itself may reveal users' data for illegal profit. Thirdly, data sharing is not static. That is, when a user's authorization gets expired, he/she should no longer possess the privilege of accessing the previously and subsequently shared data. Therefore, while outsourcing data to cloud server, users also want to control access to these data such that only those currently authorized users can share the outsourced data. A natural solution to conquer the aforementioned prob-lem is to use cryptographically enforced access control such as identity-based encryption (IBE).

The specific problem addressed in this paper is how to construct a fundamental identity-based cryptographical tool to achieve the above security goals. We also note that there exist other security issues that are equally important for a practical system of data sharing, such as the authenticity and availability of the shared data [8], [9], [10], [11], [12]. But the research on these issues is beyond the scope of this paper.

PROJECT SCOPE

In the current cloud servers ,there was no concept like encryption of cloud data and also there was no facility like TPA to identify the integrity of data. The current cloud storage is almost centralized and all the data which is stored along with details of data owners and data users is clearly visible by the cloud server department, which is almost a big problem in the current cloud service providers.

PROJECT OVERVIEW

The proposed system we try to design DSaaS Model by integrating Data Encryption and Verification using TPA (Third Party Auditor) in order to protect the data from un-authorized users. Initially the data owners try to upload the data into the cloud server, the application will generate keys by owner username and file name and based on these pair combination randomized keys will be generated for data encryption. By using this random key the input file will be encrypted and stored into the cloud server. If any un-authorized user try to access the data illegally the data cannot be decrypted and even if the cloud service provider try to modify the data content, the verification technique will identify that data modification and inform the same to data owner and data users .

OBJECTIVE

The main objective of choosing this current application is to provide data security by integrating TPA concept in general cloud server which can able to give utmost security for the data which is stored in the cloud server.

2. LITERATURE SURVEY

Literature survey is the most important step in software development process. Before developing the tool, it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, ten next steps are to determine which operating system and language used for developing the tool. Once the programmers start building the tool, the programmers need lot of external support. This support obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into for developing the proposed system.

1) A new general framework for secure public key encryption with keyword search

AUTHORS: R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang

Public Key Encryption with Keyword Search (PEKS), introduced by Boneh et al. in Eurocrypt'04, allows users to search encrypted documents on an untrusted server without revealing any information. This notion is very useful in many applications and has attracted a lot of attention by the cryptographic research community. However, one limitation of all the existing PEKS schemes is that they cannot resist the Keyword Guessing Attack (KGA) launched by a malicious server. In this paper, we propose a new PEKS framework named Dual-Server Public Key Encryption with Keyword Search (DS-PEKS). This new framework can withstand all the attacks, including the KGA from the two untrusted servers, as long as they do not collude. We then present a generic construction of DS-PEKS using a new variant of the Smooth Projective Hash Functions (SPHFs), which is of independent interest.

2) Searchable symmetric encryption: Improved definitions and efficient constructions

AUTHORS: R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky,

Searchable symmetric encryption (SSE) allows a party to outsource the storage of his data to another party in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research and several security definitions and constructions have been proposed. In this paper we begin by reviewing existing notions of security and propose new and stronger security definitions. We then present two constructions that we show secure under our new definitions. Interestingly, in addition to satisfying stronger security guarantees, our constructions are more efficient than all previous constructions.

Further, prior work on SSE only considered the setting where only the owner of the data is capable of submitting search queries. We consider the natural extension where an arbitrary group of parties other than the owner can submit search queries. We formally define SSE in this multi-user setting, and present an efficient construction.

3) Public Key Encryption with Keyword Search based on K-Resilient IBE

AUTHORS: D. Khader

Abstract. An encrypted email is sent from Bob to Alice. A gateway wants to check whether a certain keyword exists in an email or not for some reason (e.g. routing). Nevertheless Alice does not want the email to be decrypted by anyone except her including the gateway itself. This is a scenario where public key encryption with keyword search (PEKS) is needed. In this paper we construct a new scheme (KR-PEKS) the KResilient Public Key Encryption with Keyword Search. The new scheme is secure under a chosen keyword attack without the random oracle. The ability of constructing a Public Key Encryption with Keyword Search from an Identity Based Encryption was used in the construction of the KR-PEKS. The security of the new scheme was proved by showing that the used IBE has a notion of key privacy. The scheme was then modified in two different ways in order to fulfill each of the following: the first modification was done to enable multiple keyword search and the other was done to remove the need of secure channels.

4) Generic constructions of secure-channel free searchable encryption with adaptive security

AUTHORS: K. Emura, A. Miyaji, M. S. Rahman, and K. Omote,

For searching keywords against encrypted data, public key encryption scheme with keyword search (PEKS), and its extension secure-channel free PEKS (SCF-PEKS), has been proposed. In this paper, we extend the security of SCF-PEKS, calling it adaptive SCF-PEKS, wherein an adversary (modeled as a "malicious-but-legitimate" receiver) is allowed to issue test queries adaptively. We show that adaptive SCF-PEKS can be generically constructed by anonymous identity-based encryption only. That is, SCF-PEKS can be constructed without any additional cryptographic primitive when compared with the Abdalla et al. PEKS construction (J. Cryptology 2008), even though adaptive SCF-PEKS requires additional functionalities. We also propose other adaptive SCF-PEKS construction, which is not fully generic but is efficient compared with the first one. Finally, we instantiate an adaptive SCF-PEKS scheme (via our second construction) that achieves a similar level of efficiency for the costs of the test procedure and encryption, compared with the (non-adaptive secure) SCF-PEKS scheme by Fang et al. (CANS2009). Copyright © 2014 John Wiley & Sons, Ltd. 5) Cooperative provable data possession for integrity verification in multicloud storage

3. EXISTING SYSTEM

In the existing cloud servers, there was no concept like encryption of cloud data and also there was no facility like TPA to identify the integrity of data. The current cloud storage is almost centralized and all the data which is stored along with details of data owners and data users is clearly visible by the cloud server department, which is almost a big problem in the current cloud service providers.

LIMITATION OF EXISTING SYSTEM

The following are the main limitations of the existing system. They are as follows:

1. All the current cloud servers has search in a normal manner under plain text model, but they don't have any facility to search in a ENRYPTED manner
2. The existing cloud servers are almost operated in a centralized manner, where all the access can be viewed and monitored by the cloud service providers.
3. There is no concept like TPA for verifying the data which is uploaded into the cloud server.

4. PROPOSED SYSTEM

The proposed system we try to design DSaaS Model by integrating Data Encryption and Verification using TPA (Third Party Auditor) in order to protect the data from un-authorized users. Initially the data owners try to upload the data into the cloud server, the application will generate keys by owner username and file name and based on these pair combination randomized keys will be generated for data encryption. By using this random key the input file will be encrypted and stored into the cloud server. If any un-authorized user try to access the data illegally the data cannot be decrypted and even if the cloud service provider try to modify the data content, the verification technique will identify that data modification and inform the same to data owner and data users

ADVANTAGES OF THE PROPOSED SYSTEM

The following are the advantages of our proposed system. They are as follows:

1. Here the data will be stored in the form of encrypted manner rather than in a plain text manner.
2. We achieved high level of accuracy and efficiency of our proposed scheme.
3. This is providing security for the data if any user try to edit the data illegally from the cloud server.

5. SOFTWARE PROJECT MODULES

Implementation is a stage where theoretical design is converted into programmatically manner. The implementation will be divided into number of modules like 5 modules

1. Data Owner
2. Data User
3. Cloud Server
4. Third Party Auditor (TPA)
5. Attacker

5.1 Data Owner Module

The **Data Owner** is the one who try to register with their details and then login into their account. Once the data owner login into their account they can upload the sensitive information into the cloud server and the owner will try to encrypt the data by using well known cryptography algorithm AES Algorithm and then try to generate verification key by using SHA1 algorithm.

5.2 Data User Module:

The **data user** is one who try to register with their details and then login into their account. Once the data user login into their account they can operations like search for the sensitive documents by entering filename. Once if the file is found, the cloud server will show the details of that file and ask user to get the decryption key from the data owner. Here the files will be stored in untrusted cloud server in encrypted manner and those key details and verification objects are maintained by the TPA.

5.3 Cloud Server Module:

The cloud server is one which is mainly used to store all the data into its storage medium.In general the data will be stored in plain text manner hence no security for the data.But in this current application the data owner will try to encrypt the data and those who want to access the file need to substitute the decryption key and verify that key from TPA and then only cloud server can able to provide download option for the end users.

5.4 hird Party Auditor (TPA) Module:

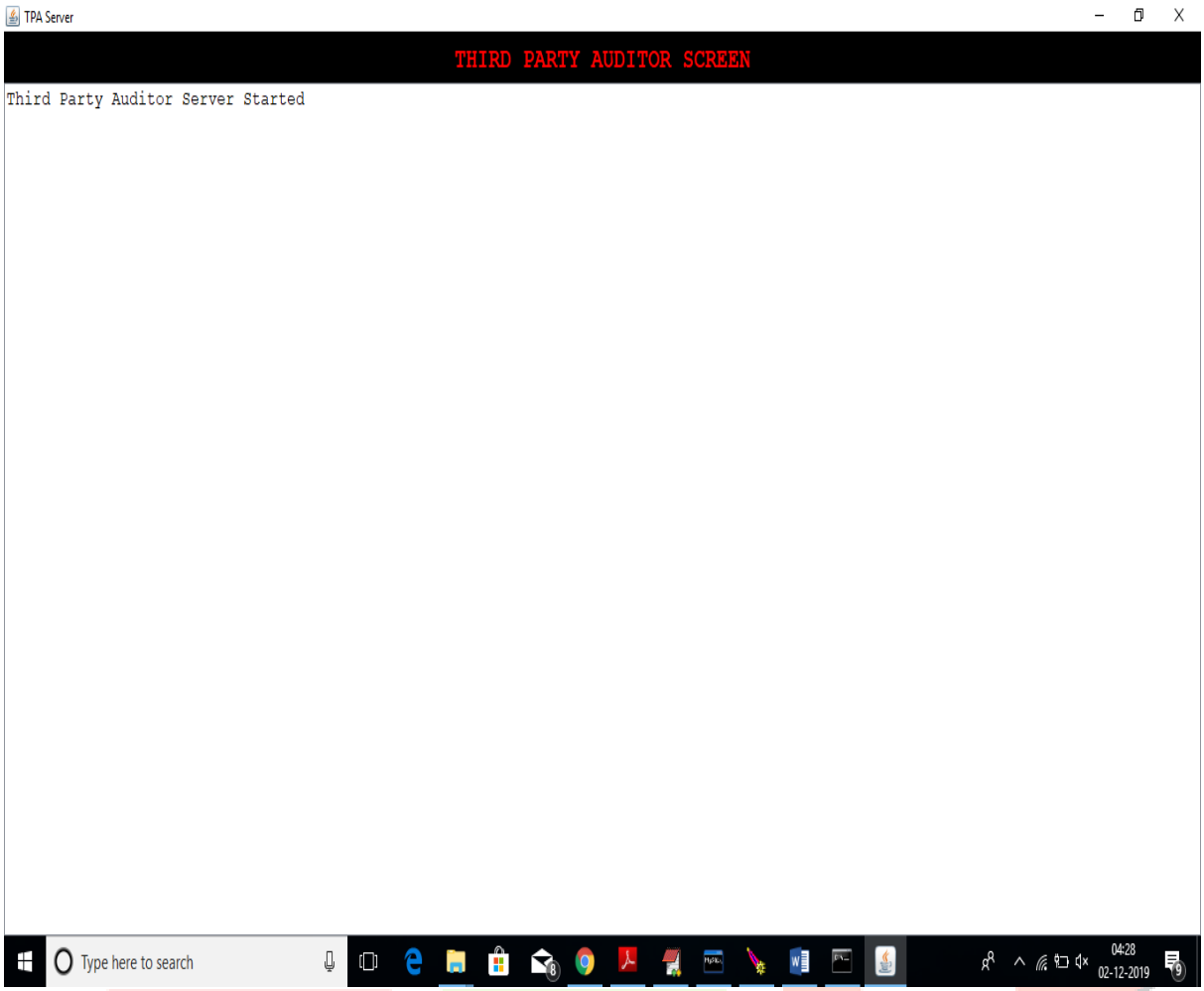
He is the one who login into the account and try to see all the activities which are performed by owner and user.If any owner want to upload the data in encrypted manner he will be giving permission for him.If any data user want to download the data in plain text manner, he will be granting the decryption key.

5.5 Attacker Module:

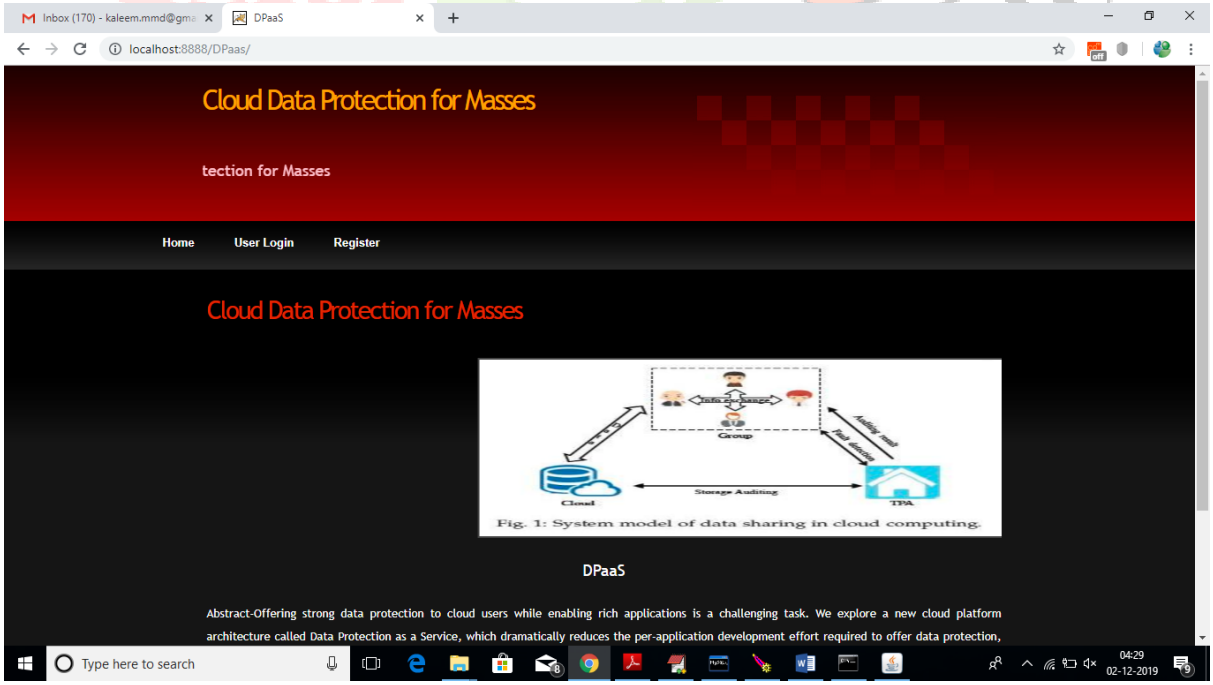
The **attacker** is one who try to create attack internally by disturbing the content which is present on the cloud server and he try to edit or modify the sensitive data which is present inside the cloud memory.

6. RESULTS (OUTPUT SCREENS)

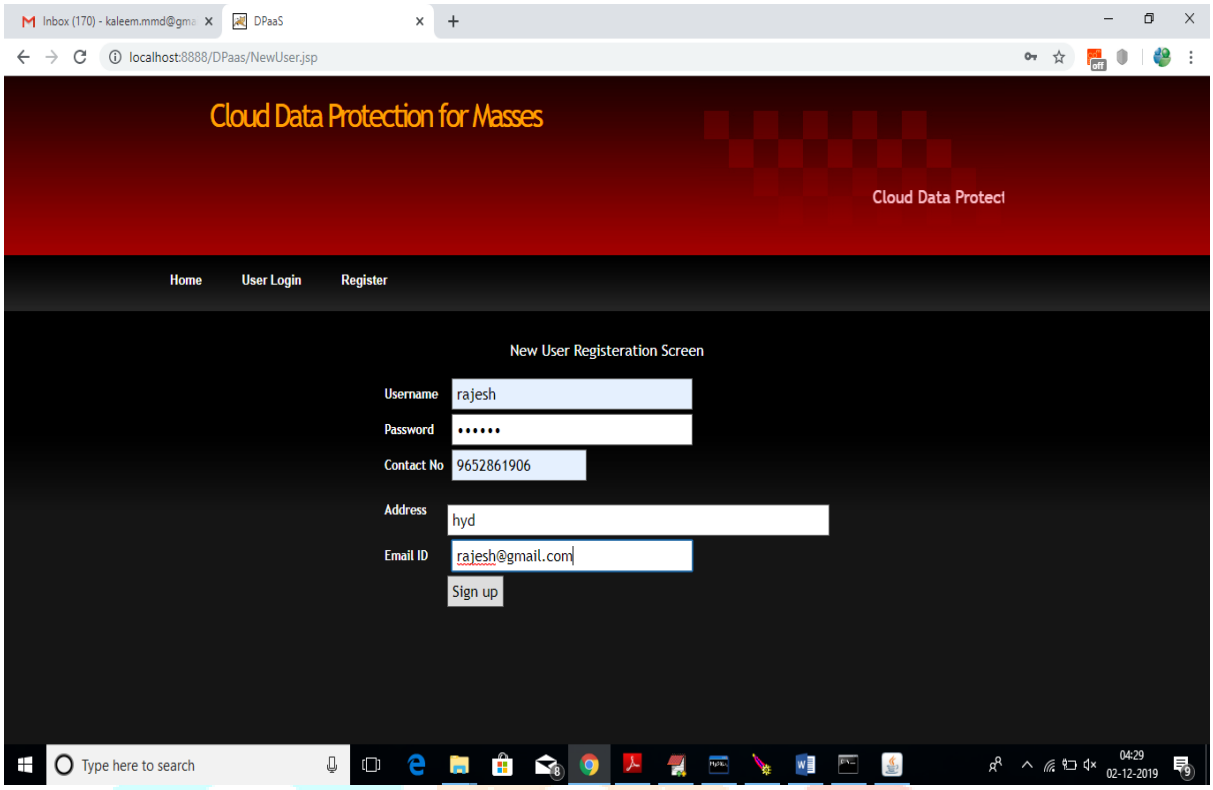
To run this projects first create database in MYSQL by copying content from ‘DB.txt’ file and paste in MYSQL. Double click on ‘run.bat’ file from TPA folder to start TPA application and to get below screen.



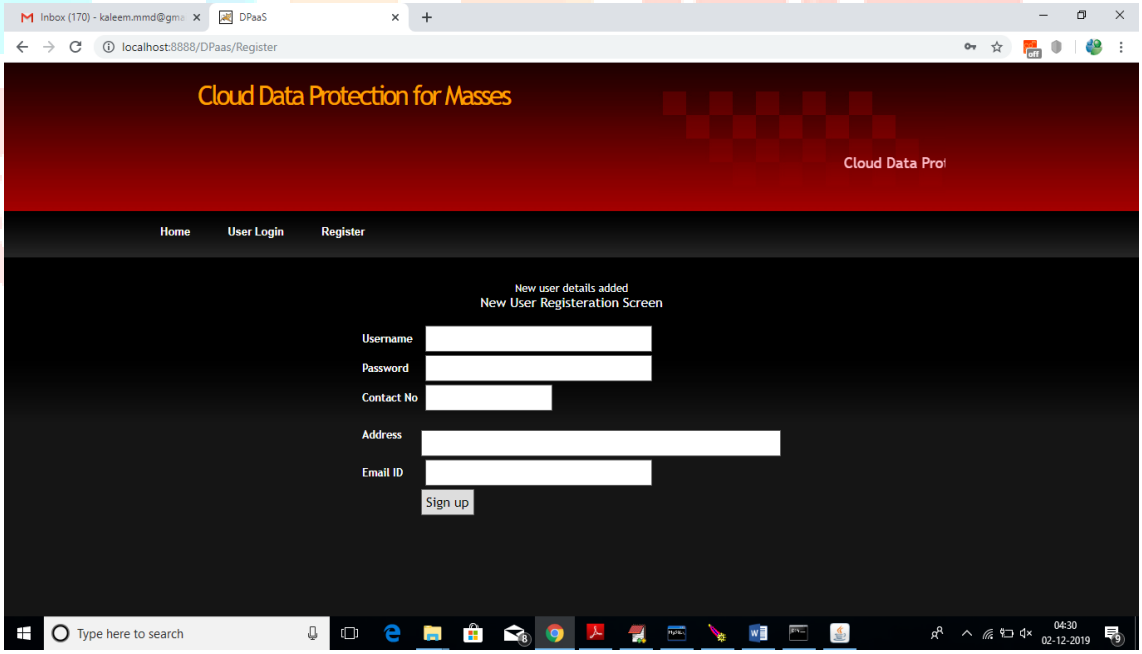
Then deploy DPaaS folder on tomcat and then start tomcat server and run in browser to get below screen



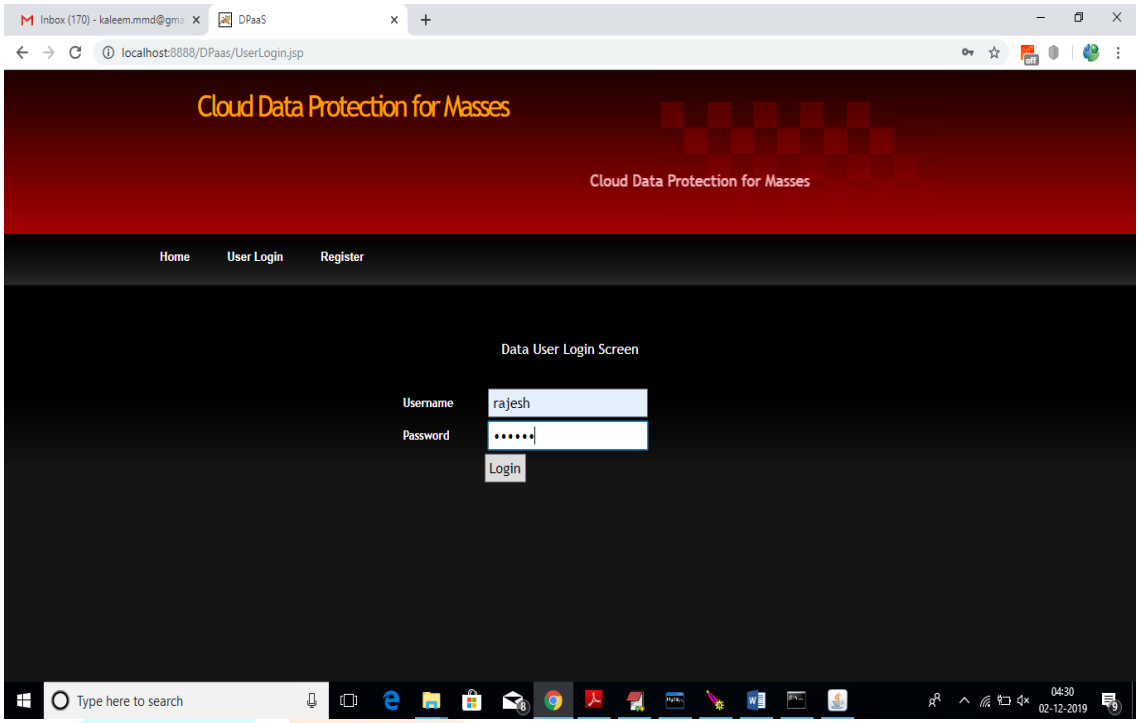
In above screen click on ‘Register’ link to add new user



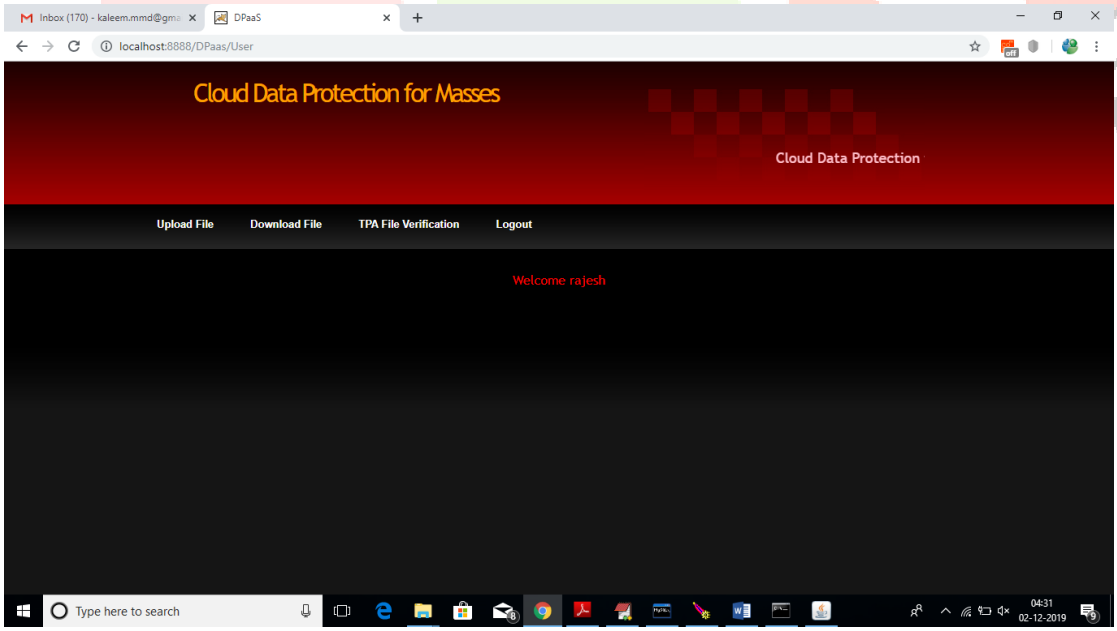
In above screen enter new user details and click on 'Sign Up' button to add new user



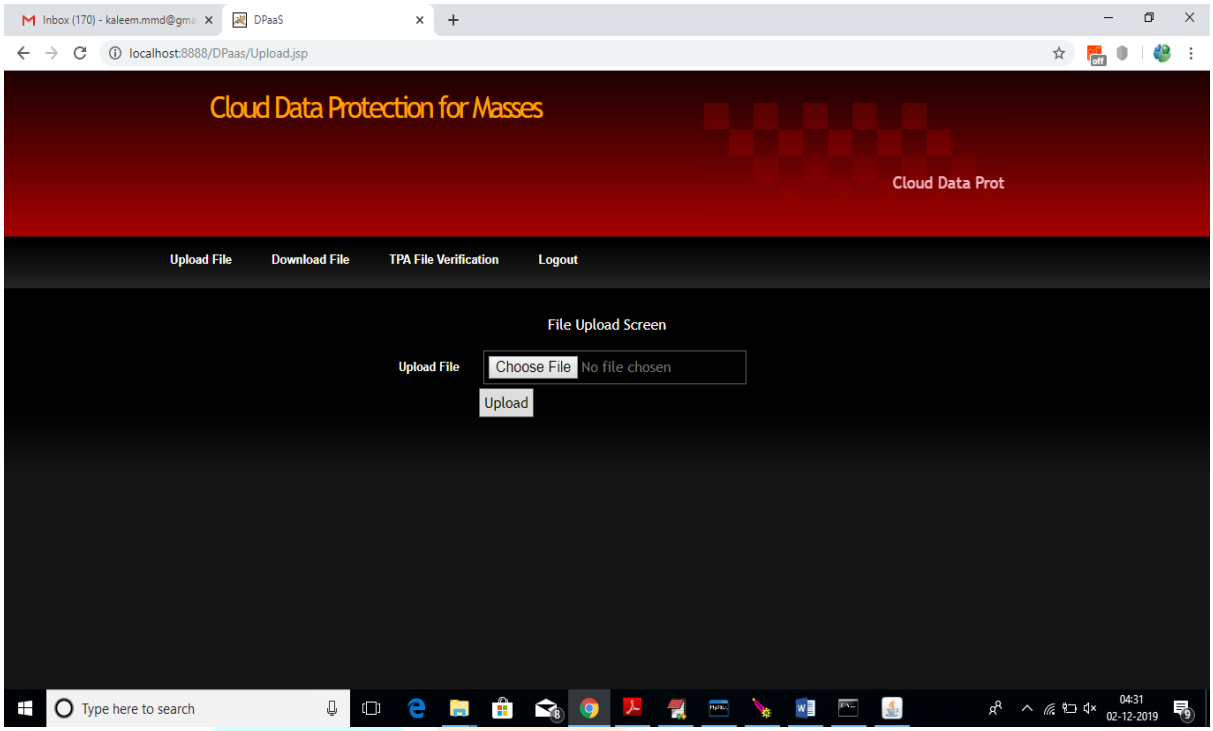
After adding new user click on 'User Login' link to login to application



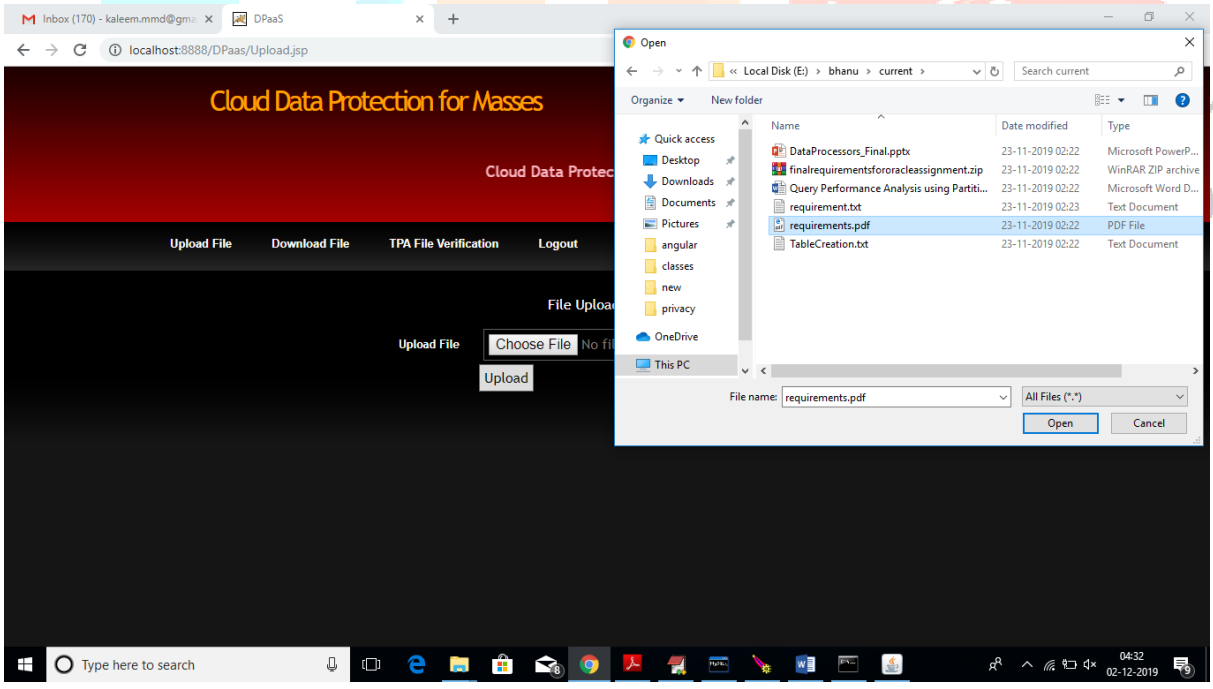
After login will get below screen



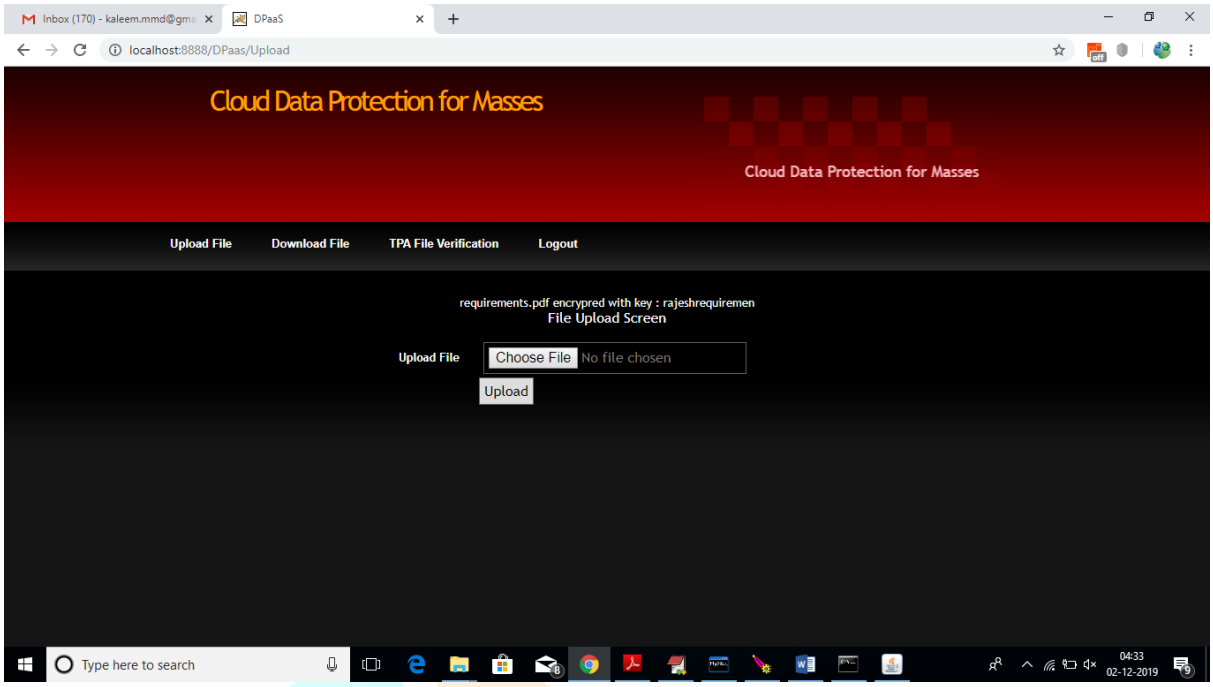
In above screen click 'Upload File' link to upload files



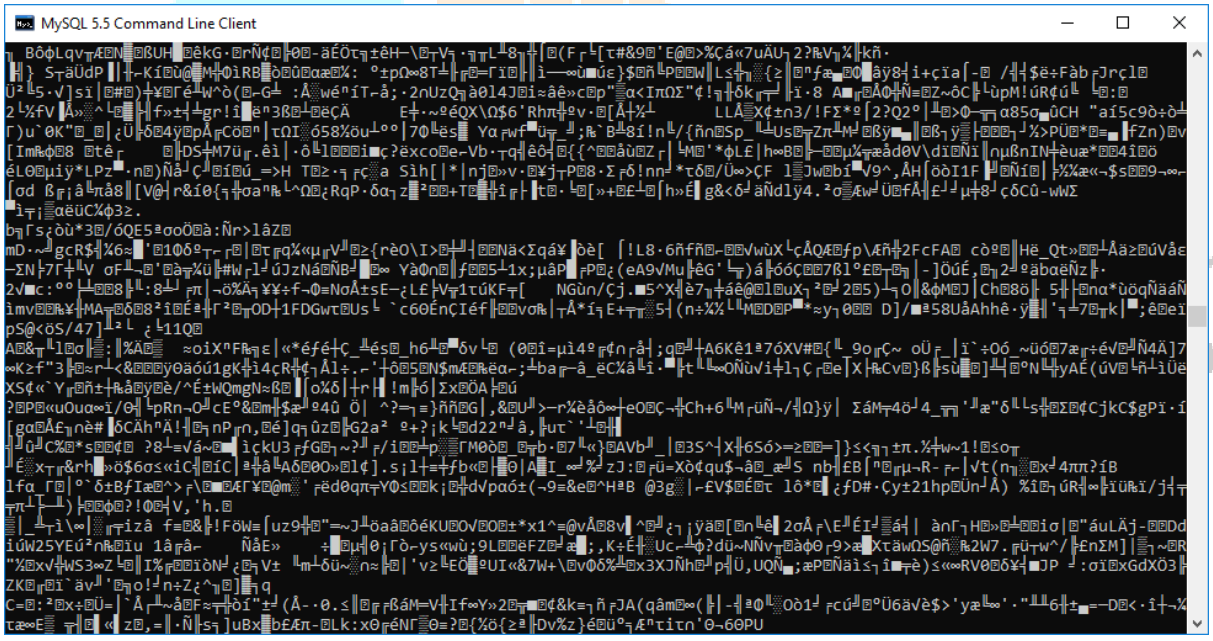
In above screen click on 'Choose File' button to upload any type of files



In above screen I am uploading one pdf file, after upload will get below screen

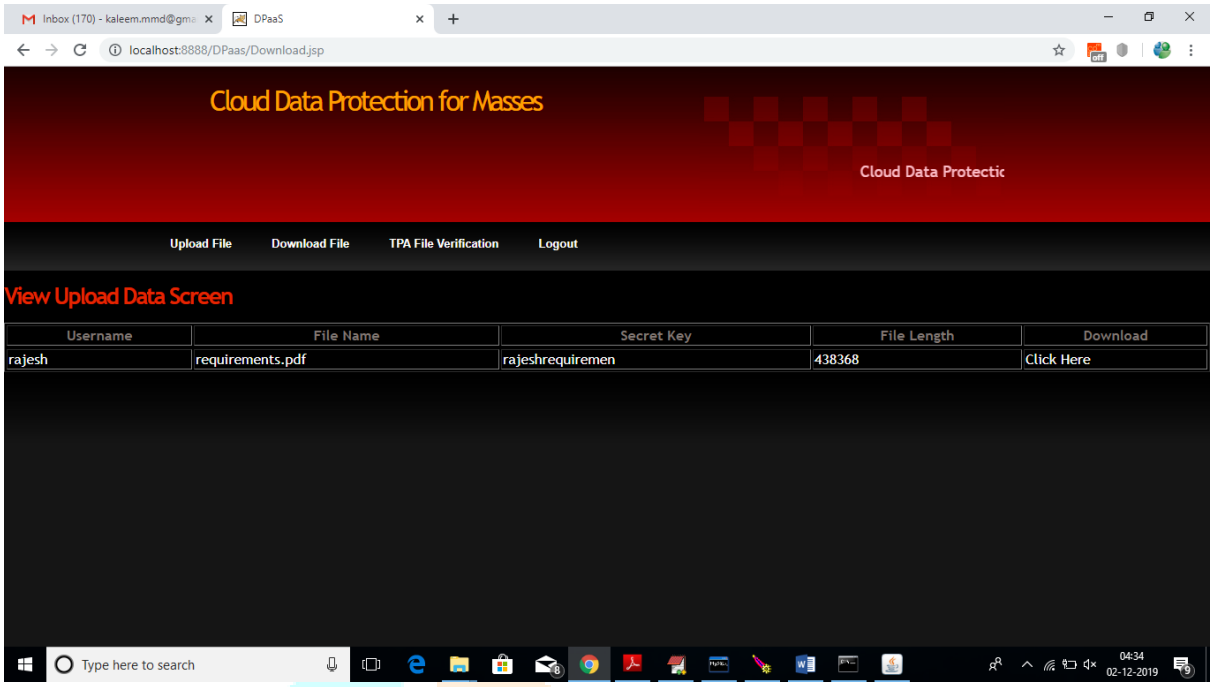


After file upload we can see encrypted file content in mysql



In above screen we can see all file data is encrypted and store in mysql.

Now click on 'Download' link to download that



In above screen all files from the same user will be displayed in table, to download any file just click on 'Click Here' link to download file.

7. CONCLUSION

In this project we introduced two techniques called Data Encryption and verification using TPA (Third Party Auditor). When users upload data then this application will generate keys by using username and file name and these keys will be randomized to generate encryption key. Using this key files will be encrypted and then store at cloud database. If anybody theft data then data is in encrypted format and attacker cannot understand the data. Sometime clouds may also works in malicious manner and to tackle this issue we are

using secure TPA which will generate keys and then encrypt data and then store file at cloud database. Before storing file data TPA will extract length of the file and store it in database for future verification.

8. REFERENCES

[1] C. Dwork, "The Differential Privacy Frontier Extended Abstract," Proc. 6th Theory of Cryptography Conf. (TCC 09), LNCS 5444, Springer, 2009, pp. 496-502.

[2] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, 34(1), 2011, pp 1-11.

[3] H. Takabi, J.B.D. Joshi and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security & Privacy, 8(6), 2010, pp. 24-31.

[4] (NIST), http://www.nist.gov/itl/cloud/.

[5] S. Kamara and K. Lauter, "Cryptographic cloud storage", FC'10: Proc. 14thIntl.Conf. on Financial cryptography and data security, 2010, pp. 136-149.

[6] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud Computing", Journal of Network and Computer Applications, 34(1), 2011, pp 1-11.

[7] Brunette, G. and R. Mogull (ed), 2009, Security Guidance for Critical Areas of Focus in Cloud Computing.