iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VI **Month of publication:** June 2017

DOI:

www.ijraset.com

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

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Secure and Attribute-Based Keyword Search with Fine-Grained Owner-Authorization in the Cloud with Time Server

Pratiksha S. Gadekar[1], Prof. G.S.Deokate[2]
[1]M.E. Computer Engineering Pune University, Sharadchandra Pawar College of Engineering, Otur,Pune, India.
[2]M.E. Computer Engineering Pune University, Sharadchandra Pawar College of Engineering, Otur,Pune, India.

Abstract: ***Search over scrambled information is a basically critical empowering system in distributed computing, where encryption-before outsourcing is a principal answer for securing client information protection in the untrusted cloud server environment. Many secure hunt plans have been concentrating on the single-donor situation, where the outsourced dataset or the protected searchable file of the dataset are encoded and overseen by a solitary proprietor, regularly in view of symmetric cryptography. In this paper, we concentrate on an alternate yet additionally difficult situation where the outsourced dataset can be contributed from different proprietors and are searchable by numerous clients, i.e. multi-client multi-supporter case. Propelled by trait based encryption (ABE), we show the main characteristic based watchword look conspire with proficient client disavowal (ABKS-UR) that empowers versatile fine-grained (i.e. document level) look approval. Our plan permits different proprietors to encode and outsource their information to the cloud server freely. Clients can create their own particular pursuit abilities without depending on a constantly online trusted power. Fine-grained seek approval is additionally actualized by the proprietor implemented get to strategy on the list of every record. Promote, by fusing intermediary re-encryption and lethargic re-encryption procedures, we can appoint overwhelming framework redesign workload amid client disavowal to the creative semi-trusted cloud server. We formalize the security definition and demonstrate the proposed ABKS-UR plot specifically secure against picked catchphrase assault. To assemble certainty of information client in the proposed secure inquiry framework, we additionally outline a query item check conspire. At long last, execution assessment demonstrates that the productivity of our plan. In ABKS-UR, the get to approach is connected to the figure message in plaintext shape, which may likewise release some private data about end-clients. Existing techniques just halfway shroud the characteristic values in the get to approaches, while the trait names are still unprotected, these issues are change in our plan to give more security. While transferring a record time server is connected with document to give access to record to restricted time simply after that time document is inaccessible for shoppers additionally property blossom channel create characteristics of record while transferring and this traits are store with document. Quality power in our plan relegate open key to client while transferring documents on cloud furthermore records mystery key and private key to information customer while transferring. Subsequent to entering watchword client buyer will get best rank outcome relies on characteristic and time and can download that document if customer having key of that record and can decode record.***

Keywords: Cloud Computing, Attribute-based Keyword Search, Fine-grained Owner-enforced Search Authorization, Multi-user Search, Verifiable Search, Time Server

I. INTRODUCTION

CLOUD computing has risen as another undertaking IT architecture. Many organizations are moving their applications and databases into the cloud and begin to appreciate numerous unparalleled points of interest brought by distributed computing, for example, on-request figuring asset design, universal and adaptable get to, extensive capital use reserve funds, and so on. In any case, protection concern has remained an essential boundary keeping the appropriation of distributed computing by a more extensive scope of clients/applications. At the point when touchy information are outsourced to the cloud, information proprietors normally get to be distinctly worried with the protection of their information in the cloud and past. Encryption-before-outsourcing has been viewed as an essential method for ensuring client information security against the cloud server [2], [3], [4]. Be that as it may, how the encoded information can be successfully used then turns into another new test. Huge consideration has been given and much exertion has been made to address this issue, from secure inquiry over scrambled information [5], secure capacity assessment [6], to

completely homeomorphic encryption frameworks [7] that give nonspecific answer for the issue in principle yet are still too a long way from being reasonable because of the greatly high many-sided quality. This paper concentrates on the issue of inquiry over encoded information, which is an essential empowering method for the encryption-before-outsourcing security insurance worldview in distributed computing, or as a rule in any arranged data framework where servers are not completely trusted. Much work has been done, with lion's share concentrating on the single-benefactor situation, i.e. the dataset to be looked is scrambled and overseen by a solitary element, which we call proprietor or benefactor in this paper. Under this setting, to empower look over encoded information, the proprietor needs to either impart the mystery key to approved clients [5], [8], [9], or remain online to create the inquiry trapdoors, i.e. the "encoded" type of catchphrases to be sought, for the clients upon demand [10], [11]. The same symmetric key will be utilized to encode the dataset (or the searchable list of the dataset) what's more, to produce the trapdoors. These plans truly constrain the clients' hunt adaptability.

Consider a document sharing framework that has countless, contributed from various proprietors and to be shared among different clients (e.g. 4shared.com, mymedwall. com). This is an all the more difficult multi-proprietor multiuser situation. How to empower various proprietors to encode and add their information to the framework and make it searchable by different clients? Also, information proprietors may want fine-grained seek approval that lone permits their approved clients to look their contributed information. By fine-grained, we mean the pursuit approval is controlled at the granularity of per record level. Symmetric cryptography based plans [5], [8], [9] are unmistakably not reasonable for this setting because of the high multifaceted nature of mystery key administration. Albeit approved catchphrase hunt can be acknowledged in single-proprietor setting by unequivocally characterizing a server-implemented client list that assumes the liability to control genuine clients' pursuit capacities [12], [13], i.e. inquiry must be done by the server with the help of genuine clients' corresponding keys on the client list, these plans did not understand fine-grained proprietor upheld seek approval and along these lines can't give separated get to benefits to various clients inside a dataset. Deviated cryptography is more qualified to this dynamic setting by scrambling singular commitment with various open keys. For instance, Hwang et al. [14] verifiably characterized a client list for every document by scrambling the record of the record with all the general population keys of the proposed clients. Be that as it may, stretching out such client list way to deal with the multi-proprietor setting and on a for each document premise is not paltry as it would force noteworthy adaptability issue considering a potential substantial number of clients and records bolstered by the framework. Extra difficulties incorporate how to handle the redesigns of the client records on account of client enlistment, repudiation, and so on., under the dynamic cloud environment.

In this paper, we address these open issues and present an approved watchword look conspire over scrambled cloud information with effective client disavowal in the multi-client multi-information giver situation. We understand fine-grained proprietor upheld look approval by misusing cipher text strategy quality based encryption (CPABE) system. In particular, the information proprietor scrambles the record of every document with a get to strategy made by him, which characterizes what sort of clients can look this list. The information client creates the trapdoor autonomously without depending on a constantly online trusted power (TA). The cloud server (CS) can look over the encoded records with the trapdoor for a client's sake, and after that profits coordinating outcome if and just if the client's characteristics connected with the trapdoor fulfill the get to arrangements inserted in the scrambled files. We separate traits and watchwords in our plan. Catchphrases are genuine substance of the records while credits allude to the properties of clients. The framework just keeps up a predetermined number of properties for hunt approval reason. Information proprietors make the file comprising of all catchphrases in the document however scramble the list with a get to structure just in light of the qualities of approved clients, which makes the proposed plot more versatile and appropriate for the huge scale record sharing framework. So as to further discharge the information proprietor from the oppressive client enrollment administration, we utilize intermediary re-encryption [15] and lethargic re-encryption [16] strategies to move the workload however much as could be expected to the CS, by which our proposed plot appreciates proficient client denial. Formal security examination demonstrates that the proposed plan is provably secure and meets different pursuit protection necessities.

We present a period server in our plan to allocate specific time with every record which is transferring on cloud. So while client transfers record on cloud specific time is connected with it. So this document is open to information buyer just for that particular day and age then after that time records are not accessible for client to get to.

II. LITERATURE SURVEY

A. *Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing*

Authors: Shucheng Yu , Cong Wang , Kui Ren , Wenjing Lou

In this paper addresses this testing open issue by, on one hand, characterizing and upholding access approaches in light of information properties, and, then again, permitting the information proprietor to designate the majority of the calculation undertakings required in fine grained information get to control to untrusted cloud servers without uncovering the basic information substance. We accomplish this objective by abusing and remarkably consolidating methods of quality based encryption (ABE), intermediary re-encryption, and lethargic re-encryption. Our proposed conspire likewise has remarkable properties of client get to benefit classification and client mystery key responsibility. Broad examination demonstrates that our proposed plan is very productive and provably secure under existing security models.

1) *Advantages:* It is exceedingly effective and provably secure under existing security models. Accomplishes fine-grained ness, versatility and information privacy for information get to control in distributed computing
2) *Disadvantages:* It is most mind boggling framework information record creation/cancellation and new client allow operations simply influence current document/client without including framework wide information document overhaul or re-keying.

B. Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption

Authors: Ming Li, Shucheng Yu, Yao Zheng, Wenjing Lou

In this paper, we propose a novel patient-driven system and a suite of instruments for information get to control to PHRs put away in semi trusted servers. To accomplish fine-grained and adaptable information get to control for PHRs, we influence trait based encryption (ABE) procedures to scramble every patient's PHR document. Not the same as past works in secure information outsourcing, we concentrate on the various information proprietor situation, and partition the clients in the PHR framework into numerous security spaces that significantly diminishes the key administration many-sided quality for proprietors and clients. A high level of patient security is ensured all the while by misusing multi power ABE. Our plan additionally empowers dynamic adjustment of get to approaches or record properties, bolsters effective on-request client/characteristic renouncement and break-glass access under crisis situations. Broad expository and exploratory outcomes are displayed which demonstrate the security, adaptability, and productivity of our proposed conspire.

1) *Advantages:* In this framework plot likewise empowers dynamic change of get to strategies or document qualities, underpins proficient on-request client/trait disavowal and break-glass access under crisis situations
2) *Disadvantages:* It bolster just characteristic based encryption not in the least.

C. Multi-User Private Keyword Search for Cloud Computing.

Authors: Yanjiang Yang , Haibing Lu , Jian Weng

In this paper Searchable encryption is a cryptographic primitive taking into consideration private watchword based inquiry over the scrambled database. The above setting of big business outsourcing database to the cloud requires multi-client searchable encryption, while practically the greater part of the current plans consider the single-client setting. To extension this crevice, we are spurred to propose a down to earth multi-client searchable encryption plot, which has various points of interest over the known methodologies. The related model and security necessities are likewise figured. We additionally talk about to expand our plan in severalways in order to accomplish diverse inquiry capacities.

1) *Advantages:* In this Paper Multi - client searchable encryption plot.
2) *Disadvantages:* Paper Data encryption would extraordinarily limit the cloud's capacity in taking care of client get to ask.

D. Authorized Private Keyword Search over Encrypted Data in Cloud Computing

Authors: Ming Li, Shucheng Yu, Ning Cao, Wenjing Lou

In this paper, utilizing on the web Personal Health Record (PHR) as a contextual investigation, we first demonstrate the need of inquiry capacity approval that decreases the security presentation coming about because of the indexed lists, and set up an adaptable structure for Authorized Private Keyword Search (APKS) over encoded cloud information. We then propose two novel answers for APKS in view of a late cryptographic primitive, Hierarchical Predicate Encryption (HPE). Our answers empower effective multi-dimensional watchword looks with range inquiry, permit assignment and denial of pursuit capacities. In addition, we upgrade the question security which conceals clients' inquiry catchphrases against the server. We actualize our plan on a cutting edge workstation, and trial comes about show its appropriateness for functional utilization.

1) *Advantages:* In this paper It upgrade the question security which shrouds clients' inquiry catchphrases against the server
2) *Disadvantages:* Share data put away in the cloud, free of their areas ex. Facebook.

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

E. Securing Cloud Server & Data Access with Multi-Authorities

Authors: Tejaswini R M, Roopa C K, Ayesha Taranum

In this engineering comprises of operators: Cloud Service Provider Agent (CSPA), Control Agent (CA), third gathering Auditor (TPA) and Attribute Authority Agent (AAA). The TPA gives a graphical interface to the cloud client that encourages the entrance to the administrations offered by the Cloud Service Provider (CSPA).

1) *Advantages:* In this paper third gathering examiner (TPA) which goes about as an intermediary server to defend the cloud server.
2) *Disadvantages:* Correspondence cost and calculation cost is more.

III. PROPOSED APPROACH FRAMEWORK AND DESIGN

A. Architecture

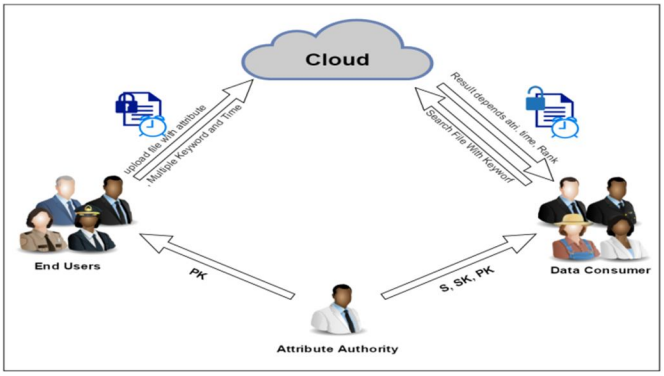


Figure 1. Architecture

In our improved Cipher text policy attribute base encryption scheme, as our scheme is an efficient encryption scheme and also file is upload on cloud with its attribute access policy and encrypted file upload on cloud. Our scheme also hide whole attribute of file and upload encrypted attributed on cloud so safety of file store on cloud are ensure. Attribute authority in our scheme generate public key while uploading file on cloud and also provides secret key of file for downloading file from cloud.

Our scheme also provide multikeyword rank search, in this scheme while uploading file on cloud user enter multiple keyword while uploading file so that when consumer want search file then result is exact matching to consumers keyword. Also while uploading file time server in our scheme assign time duration with file so that file is accessible to user only for that particular time period after time expire files are not display to user or not accessible.

Data consumer of cloud enter keyword and attribute of file to search require file on cloud and consumer get to rank file and after entering secret key of file user can download that file and decrypt file

In scheme overview, we get the proper system for storing and accessing. Data owner of cloud store their files in cloud and generate access policy of files according to attribute and then upload file on cloud after receiving keys from Attribute authority. User want to download file from cloud then attribute bloom filter first match attributes of users with files attribute and also check user according to access policy. Data file on cloud are uploaded with access policy and time specified with that file for proper search and access also for providing an efficient results to user.

B. Propose Work

In this paper the proposed work is at data owner upload data on cloud that time assign a file on cloud these file is access to Data User as with attributes and time server. If time is over then these file is not access to data user.

C. Mathematical Model:

Let S be the Whole system S= {I, P, O}

I-input

P-procedure

O-output

Input I- F = {f1, f2… fn}

Where,

F- Files
Procedure (P) = {uploadf , attrigen,keyr,time,searchf}
Input (I1): Upload file (uploadf):
Procedure (P1):
In this step first user select file to upload on cloud so input to this step is plaintext file is select for uploading procedure and converted to encrypted format and upload on cloud.
F=F (encr)->EF
Where,
encr=encryption.
EF=Encrypted File.
Output (O1): Output of this process is file in encrypted format.
Input (I2): Generate Attribute (attrigen):
Procedure (P2)
Input to this process is an encrypted file and procedure to generate attribute for that file is applied an output of step is generated attribute of file which provides access policy.
attrgn =EF-(attrigen)-> EF(attrigen)
Where,
EF (attrigen) =attribute generated for file.
Input (I3): Keyword generate(keyr):
Procedure (P3):
Input to this process is an encrypted file with generated attribute and procedure to generate keyword for that file is applied an output of step is generated keyword of file which provides search efficiency.
keyr= EF(attrigen)keyr -> EF(attrigen)keyr
Where,
EF (attrigen)keyr=file with keyword.
EF (attrigen)=attribute generated for file.
Keyr=keyword
Input (I4): Assign time (t):
Procedure (P4):
In this step time is assign to file and output is time file.
EF (attrigen)keyr(t)=t+ EF(attrigen)keyr
Where,
t= time.
Output (O4): Time is assign to file.
Input (I5):Search File on cloud(sf):
Procedure (P5):
In this step user search file on cloud for accessing of file and generate trapdoor of attribute ,keyword and time and get exact matching file from cloud.
sf= t(attri+t+keyr)
Where,
t= trapdoor
Output (O5): Exact match result is search base on trapdoor.
Output (O) - Finally, the security and experimental analysis show that, compared with its relevant schemes our scheme is also secure and efficient.

IV. PRACTICAL RESULT AND ENVIRONMENT

A. Hardware and Software Configuration

1) Hardware Requirements

Processor: Pentium IV 2.6 GHz
Ram: 512 MB DD RAM

Monitor: 15" color
Hard disk: 20 GB
Keyboard: Standard 102 keys
Mouse: 3 buttons

2) Software Requirements
Front End: Java
Back End: MYSQL
Tools Used: Eclipse
Operating System: Windows XP/7.

B. Result of Practical Work

Table I: Performance of File Size with Time

	encrypt	Decrypt	search
20KB	1.2	1.3	1.2
40KB	2.1	2.6	2.4
80KB	4.3	3.7	3.5
160KB	6.6	5.4	6.2

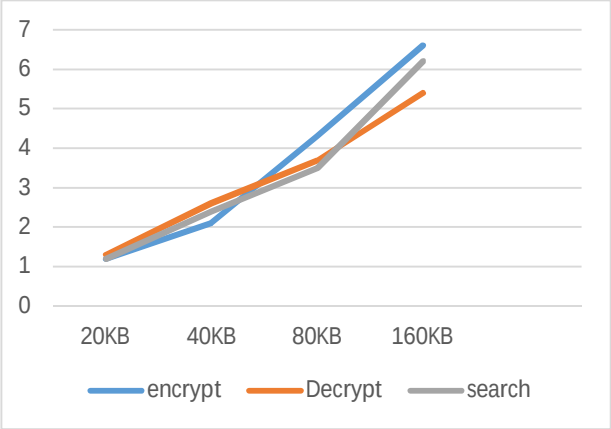


Fig 2 : Graph of File Size with Time

On this graph showing the time graph between various methods like encryption, decryption, Searching time in ms

V. CONCLUSION

In this paper, we design the first verifiable attribute structured keyword search scheme in the cloud environment, which permits scalable and fine-grained owner-enforced encrypted data search supporting multiple data owners and data users. Compared to existing public key certified keyword search scheme, our scheme could achieve system scalability and fine-grained ness at the same time. Different from search system with predicate encryption, our scheme permits a versatile authorized keyword search over arbitrarily-structured data. In addition, by using proxy re-encryption and lazy re-encryption techniques, the proposed scheme is better suited to the cloud outsourcing model and enjoys efficient user reversal, overturning, annulment. On the other hands, we make the entire search process verifiable and data user can be sure of the authenticity of the returned search effect. We also formally show the proposed scheme semantically secure in the picky model.

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

VI. RESULT

The proposed system result is as shown in the given below:

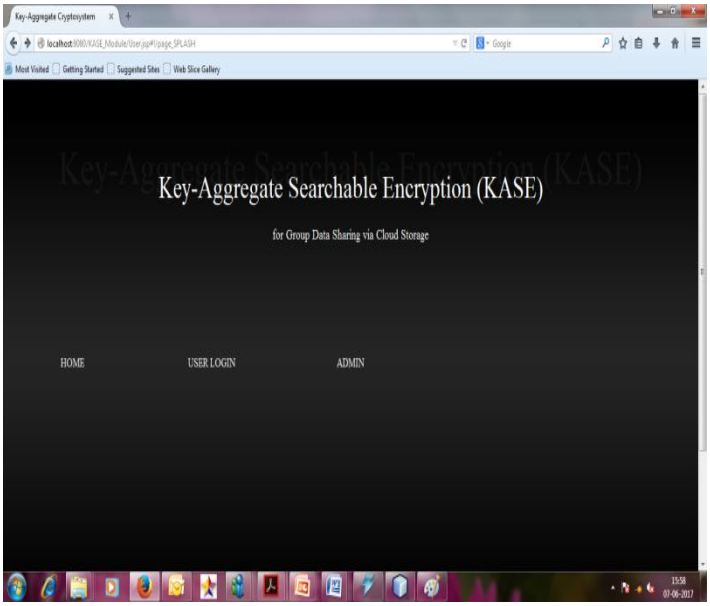


Figure: Home Page

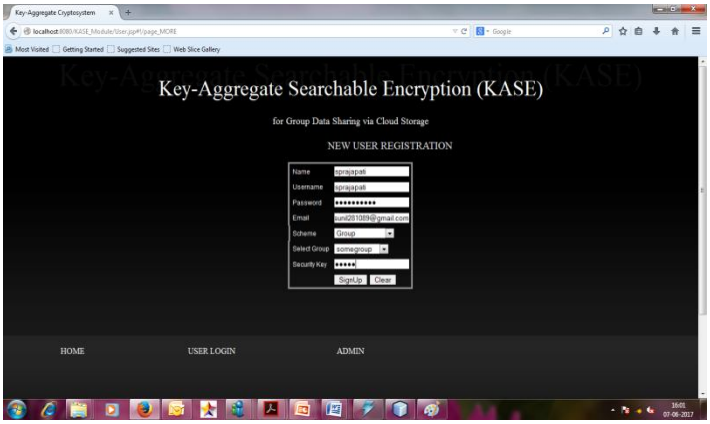


Figure: User Registration

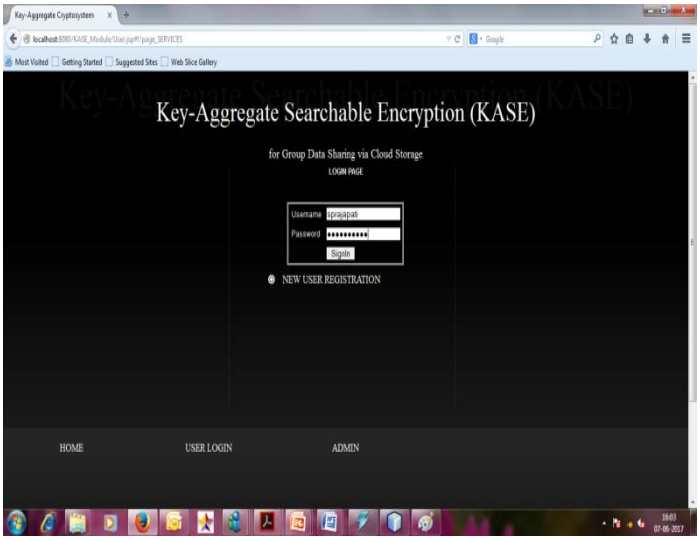


Figure: User Login

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

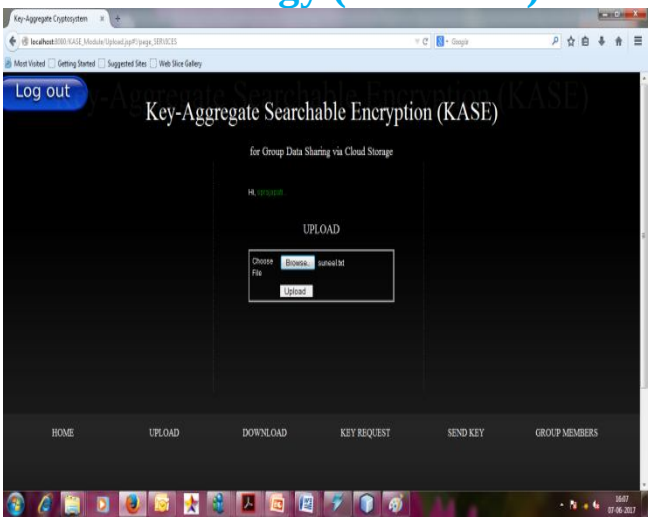


Figure: File Uploading

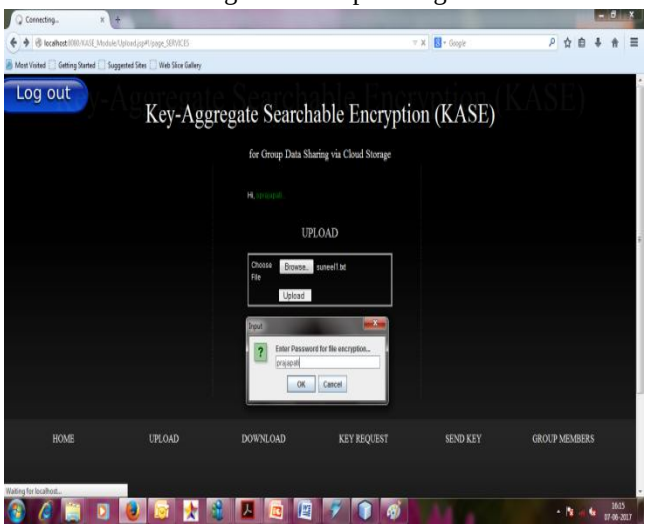


Figure: Enter file encryption key while uploading the file.

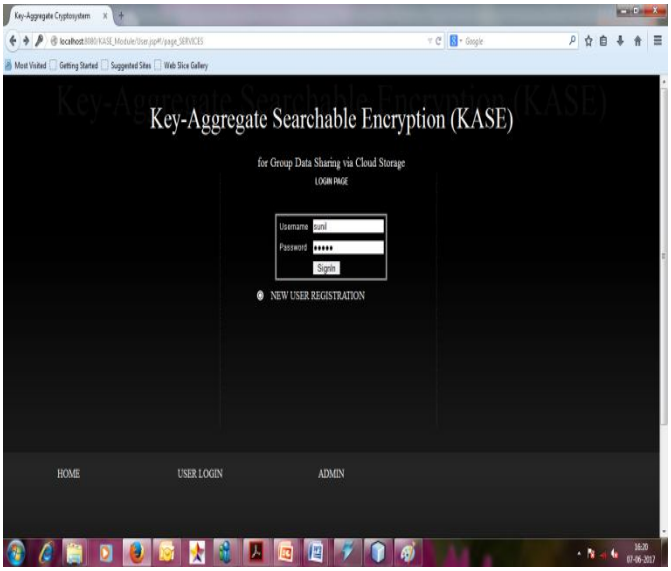


Figure: New user login for key request

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

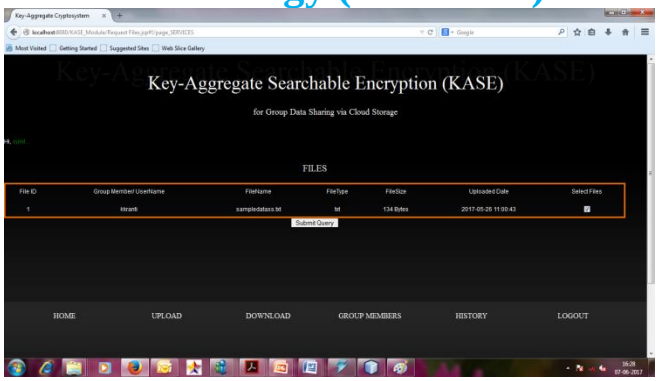


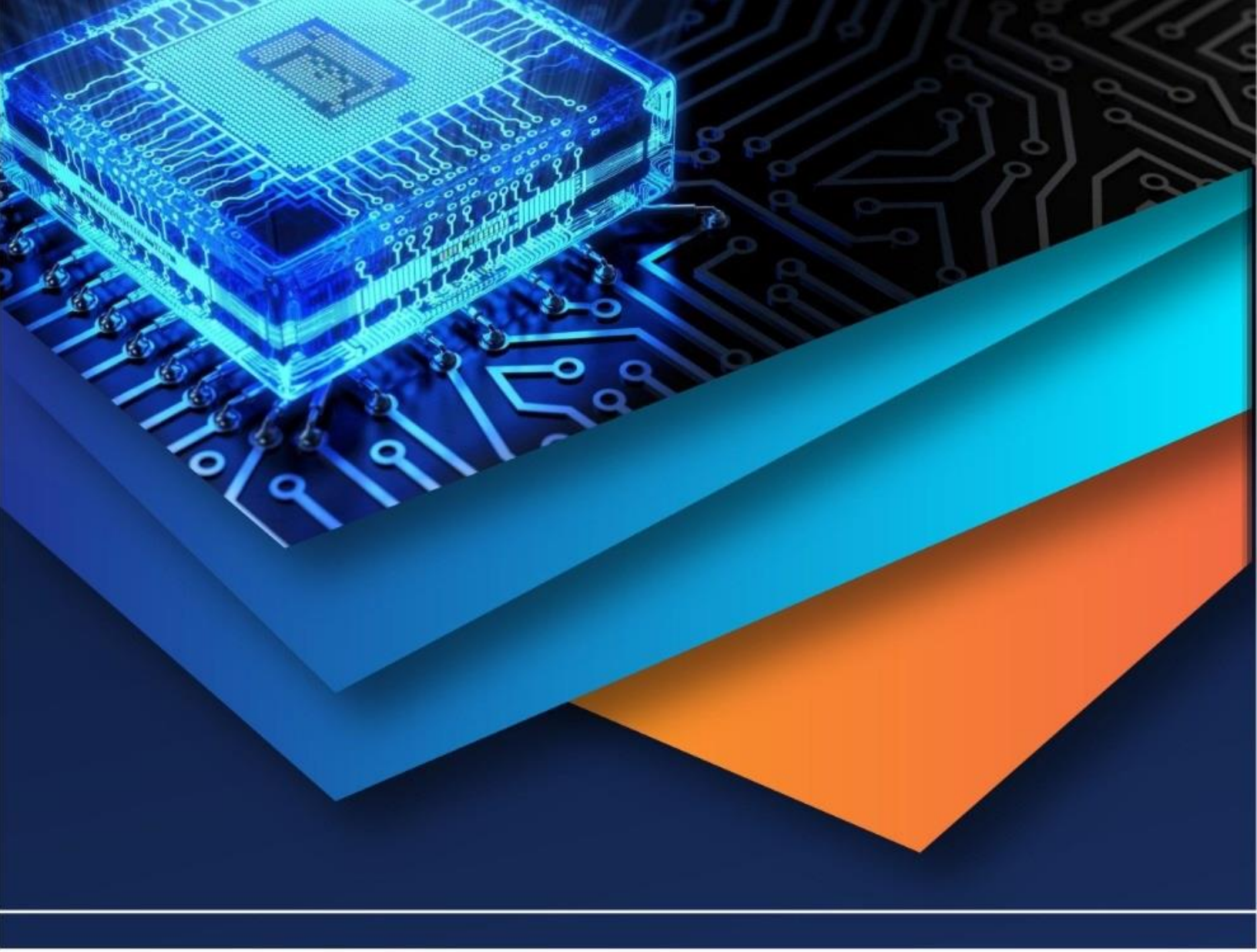
Figure: Select one or more file for key request

VII. ACKNOWLEDGEMENT

With immense pleasure, we are publishing this paper as a part of the curriculum of M.E. Computer Engineering. It gives us proud privilege to complete this paper work under the valuable guidance of Principal for providing all facilities and help for smooth progress of paper work. We would also like to thank all the Staff Members of Computer Engineering Department, Management, friends and family members, Who have directly or indirectly guided and helped us for the preparation of this paper and gives us an unending support right from the stage the idea was conceived.

REFERENCES

[1] Wenhai Sun, "Protecting Your Right: Verifiable Attribute- based Keyword Search with Fine-grained Owner-enforced Search Authorization in the Cloud", DOI 0.1109/TPDS.2014.2355202, IEEE Transactions on Parallel and Distributed Systems
[2] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, "Protecting Your Right: Attribute-based Keyword Search with Fine-grained Ownerenforced Search Authorization in the Cloud," in IEEE INFOCOM, pp. 226-234, 2014.
[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. of IEEE INFOCOM, pp. 1-9, 2010.
[4] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE TPDS, vol. 24, no. 1, pp. 131- 143, 2013.
[5] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Financial Cryptography and Data Security, pp. 136–149, 2010.
[6] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of IEEE S&P, pp. 44-55, 2000.
[7] Y. Huang, D. Evans, J. Katz, and L. Malka, "Faster secure two party computation using garbled circuits," in USENIX Security Symposium, vol. 201, no. 1, 2011.
[8] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009.
[9] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. of ACM CCS, pp. 79-88, 2006
[10] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic searchable symmetric encryption," in Proc. of ACM CCS, pp. 965-976, 2012.
[11] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in Proc. of IEEE INFOCOM, pp. 829-837, 2011.
[12] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in Proc. of ACM ASIACCS, pp. 71-82, 2013
[13] F. Bao, R. H. Deng, X. Ding, and Y. Yang, "Private query on encrypted data in multi-user settings," in Information Security Practice and Experience, Springer, pp. 71-85, 2008.
[14] Y. Yang, H. Lu, and J. Weng, "Multi-user private keyword search for cloud computing," in Proc. of IEEE CloudCom, pp. 264-271, 2011.
[15] Y. H. Hwang and P. J. Lee, "Public key encryption with conjunctive keyword search and its extension to a multi-user system," in Proc. of Pairing, pp. 2-22, 2007.
[16] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Proc. of EUROCRYPT, pp. 127-144, 1998.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY