International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

# AN EFFICIENT AND SECURED DATA STORAGE SCHEME IN CLOUD COMPUTING

**M. B. Benjula Anbu Malar [1], M. Lawanya Shri [2], M. Deepa [3],**
**K. Santhi [4], G Priya [5]**

[1,2,3,4,5] *School of Information Technology, VIT University, Tamilnadu, (India)*

## ABSTRACT

*The separation between information administration and information possession makes it hard to ensure information security and security in distributed storage frameworks. Customary encryption advances are not reasonable for information assurance in cloud capacity frameworks. A novel multi-power intermediary re-encryption system in view of ciphertext-approach quality based encryption (MPRE-CPABE) is proposed for distributed storage frameworks.*

*MPRE-CPABE requires information proprietor to part every record into two squares, one major piece and one little piece.The little square is utilized to scramble the enormous one as the private key, and at that point the scrambled enormous square will be transferred to the cloud capacity framework. An attacker can hack the file if the file is not protected with keys. Ciphertext-strategy property based encryption (CPABE) is constantly scrutinized for its substantial over-burden and frail issues at the point when disseminating keys or denying client's entrance right.*

*MPRE-CPABE applies CPABE to the multi-power cloud capacity framework, and unravels the above issues. The weighted access structure (WAS) is proposed to bolster an assortment of fine-grained edge access control strategy in multi-power situations, and lessen the computational expense of key dissemination. In the interim, MPRE-CPABE utilizes intermediary re-encryption to decrease the computational expense of access repudiation. Java programming is used with the eclipse IDE and the back-end database is stored with help of MySQL later the data is consumed in cloud (JUSTcloud) .Data is encrypted with big block and small block keys.*

## I.INTRODUTION

### PROBLEM STATEMENT

A malicious user creates multiple fake identities, known as Sybil's, to unfairly increase their power and influence within a target community. To defend against Sybil's, prior Sybil defences leverage the positive *trust* relationships among users, and rely on the key assumption that Sybil's can befriend only few real accounts. Unfortunately, we find that people in real OSNs still have a non-zero probability to accept friend requests of strangers, leaving room for Sybil's to connect real users through sending a large amount of requests.

In this paper we provide the security guarantees of Vote Trust, demonstrating that we limit the number of requests Sybil's can send to real users. Our evaluation over real network shows that Vote Trust is able to detect real Sybil's with high precision, and significantly outperforms traditional ranking systems.

Existing defences focus on using the social graph structure to isolate fakes. Existing network-based Sybil defences are unlikely to succeed in today's OSNs.

**DRAWBACKS IN EXISTING SYSTEM:**

- We found that miscreants start to sell legitimate accounts that have been compromised in Twitter.
- Thus, if attackers are willing to buy friends from miscreants, they could enhance the attack capacity by increasing the number of in-links or the acceptance rate of Sybil's.

## II.SYSTEM ARCHITECTURE

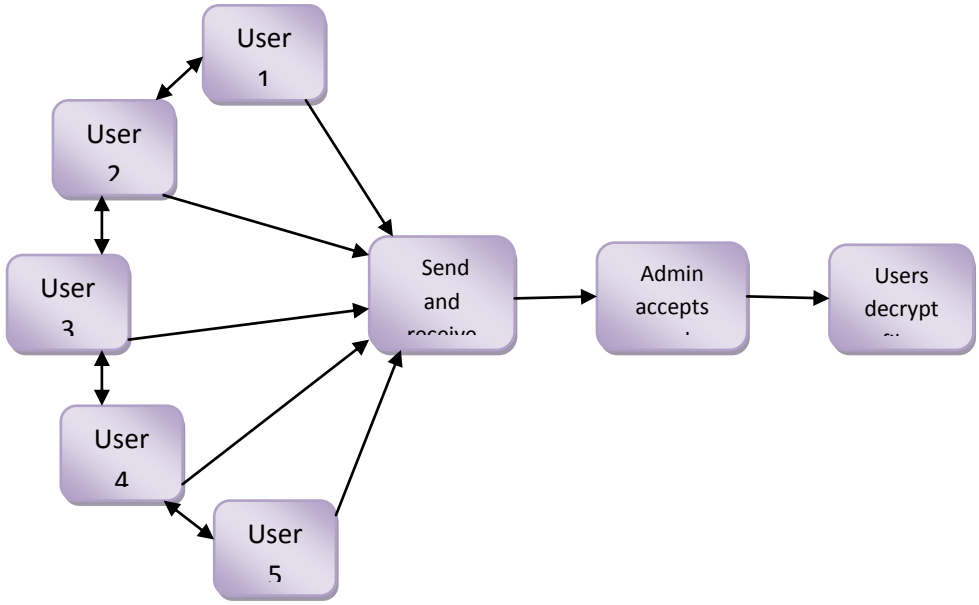


**Fig 1: system architecture**

### 2.1 STEPS INVOLVED

- USER INTERFACE DESIGN
- USER INTERACTION & FILE REQUEST
- SYBIL DETECTION
- KEY GENERATION
- ADMIN CHECKING & REJECT THE SYBIL'S

**2.1.1 USER INTERFACE DESIGN:**

This is the first module of our project. The important role for the user is to move login window to data owner window. This module has created for the security purpose. In this login page we have to enter login user id and password. It will check username and password is match or not (valid user id and valid password). If we enter any invalid username or password we can't enter into login window to user window it will shows error message. So we are preventing from unauthorized user entering into the login window to user window. It will provide a good security for our project. So server contain user id and password server also check the authentication of the user. It well improves the security and preventing from unauthorized data owner enters into the network. In this paper we are using SWING for creating design. Here we validate the login user and server authentication.

**2.1.2 USER INTERACTION & FILE REQUEST**

This Module is user interaction and Sybil detection. First one is User Interaction Normally User's interact to another user. Interact means one user send request to another user. This particular user Accept/Reject the Friend request. Second one is Sybil Detection. Sybils means the malicious user create multiple fake accounts. The fake user's sent to large number of friend request to real user. The real user finds to Sybils and vote to reject the Sybils

**2.1.3 SYBIL DETECTION**

Sybil's means the malicious user create multiple fake accounts. The fake user's sent to large number of friend request to real user. The real user finds to Sybil's and vote to reject the Sybil's. The real users find the Sybil's. The real user how to find the Sybil's. Normally fake user (Sybil's) sent to large number of request to real users but all request mostly rejected this way to find the Sybil's to real user.

**2.1.4 KEY GENERATION**

There are two piece of keys i.e bigblock key and smallblock key.Big block key is generated on admin side and small block key on receiver side. If a user wanted to access a file of a friend,he needs both piece of key to decrypt the file and download.The is key is generated randomly by the combination of the 4 alphabets and 4 integers.

**2.1.5 ADMIN ACCEPTS & REJECT THE SYBIL'S**

This Module is Admin checking. The admin checking all positive and negative results for all users in online social networks. The admin find the Sybils and reject the Sybils in the online social networks.

This is Admin reject the Sybils. The real user vote to another user in positive and negative votes . The admin check the all negative vote for Sybils. Finally to reject/delete the Sybils and a Sybil community detection in online social networks.

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

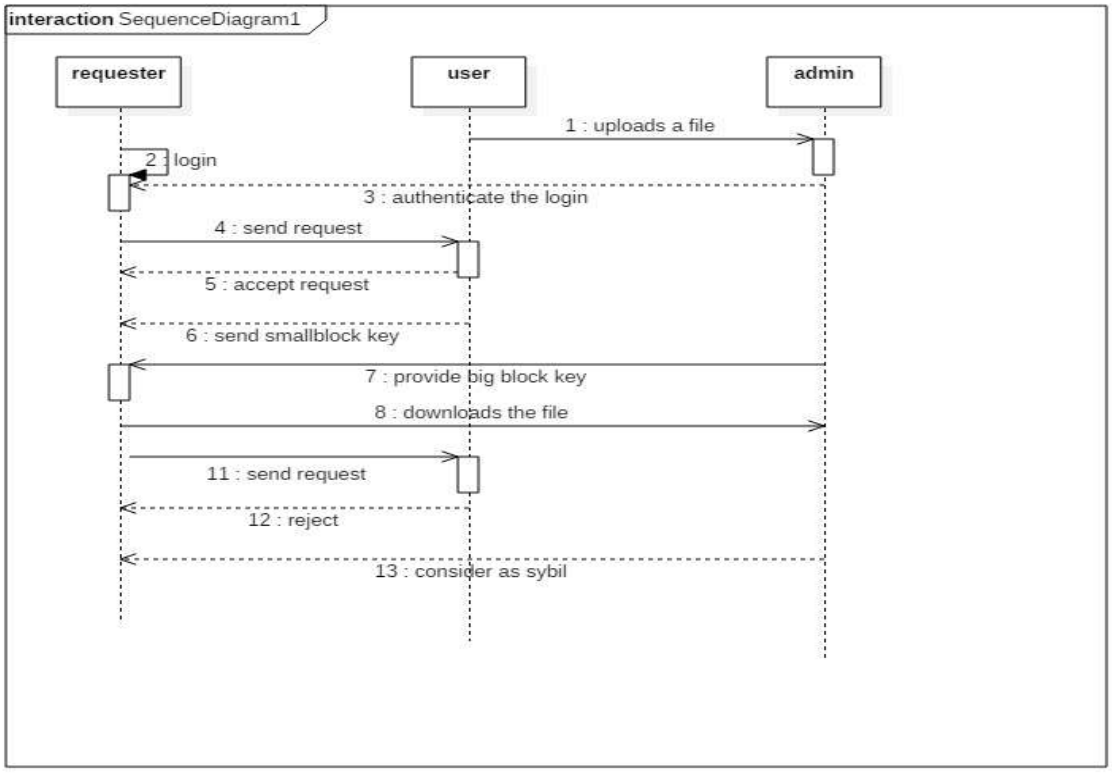


**Fig 2: sequence diagram**

## III. RESULTS AND SCREEN SHOTS

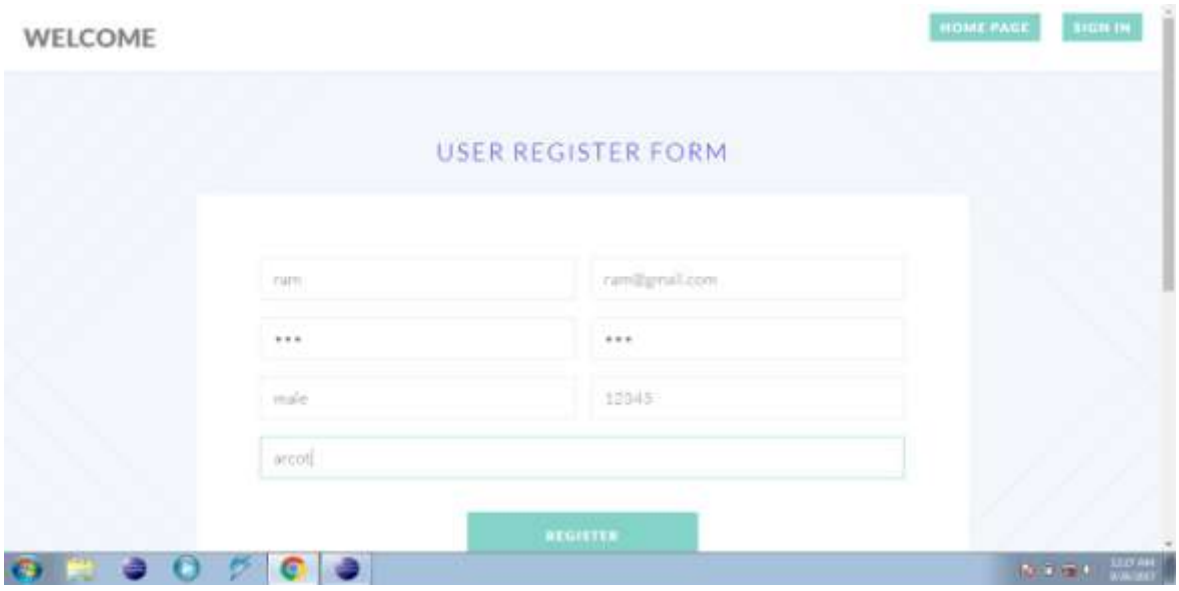


**Fig 3: user register form**

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354


**Fig 4: file upload**

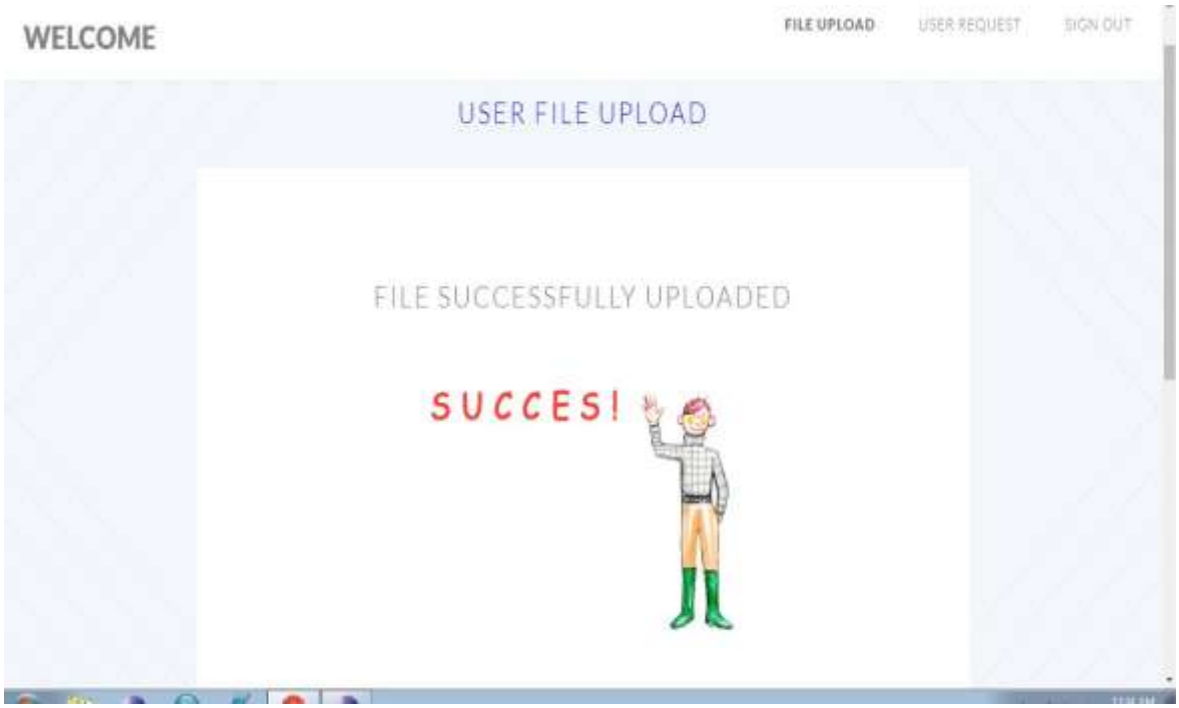


**Fig 5: file upload**

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

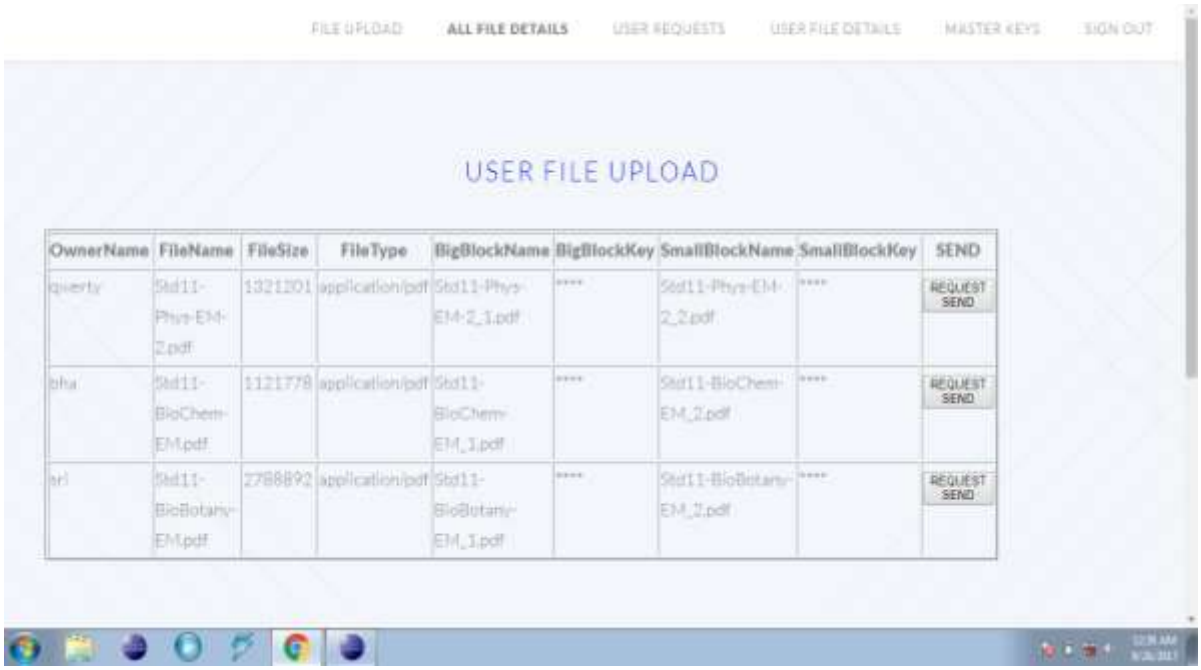


**Fig 6: sending request**

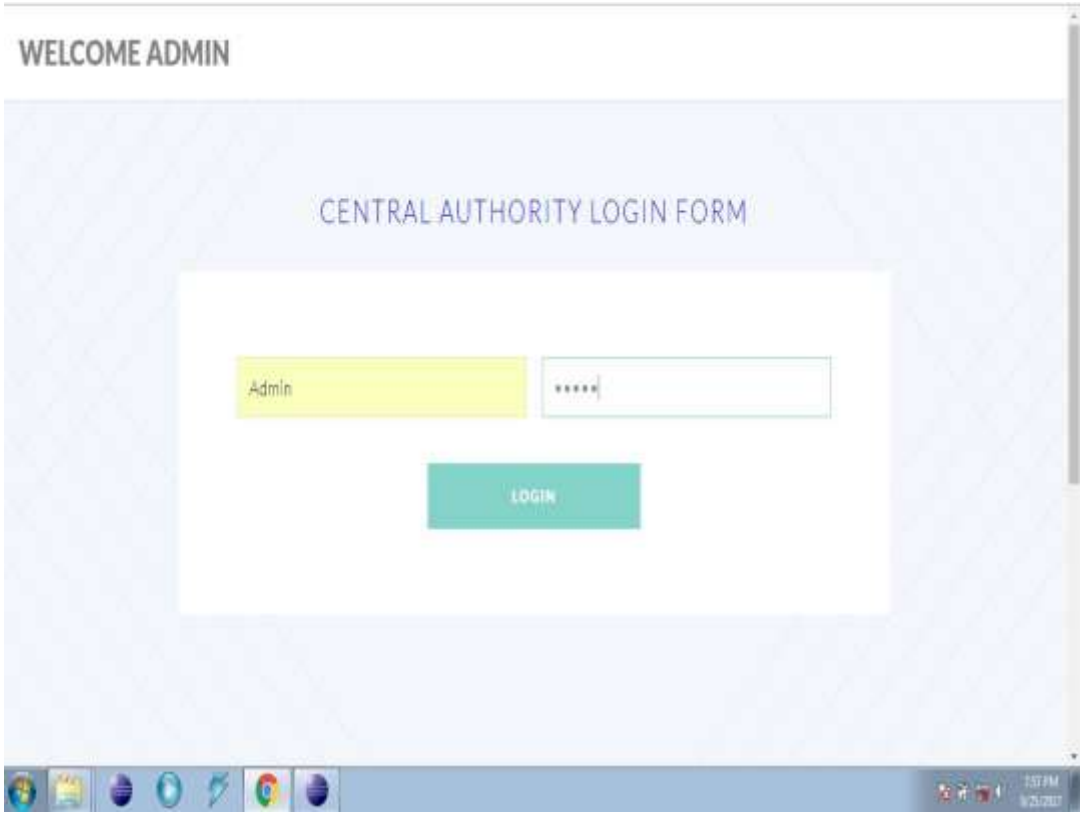


**Fig7: central authority**

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354


**Fig 8: file keys**

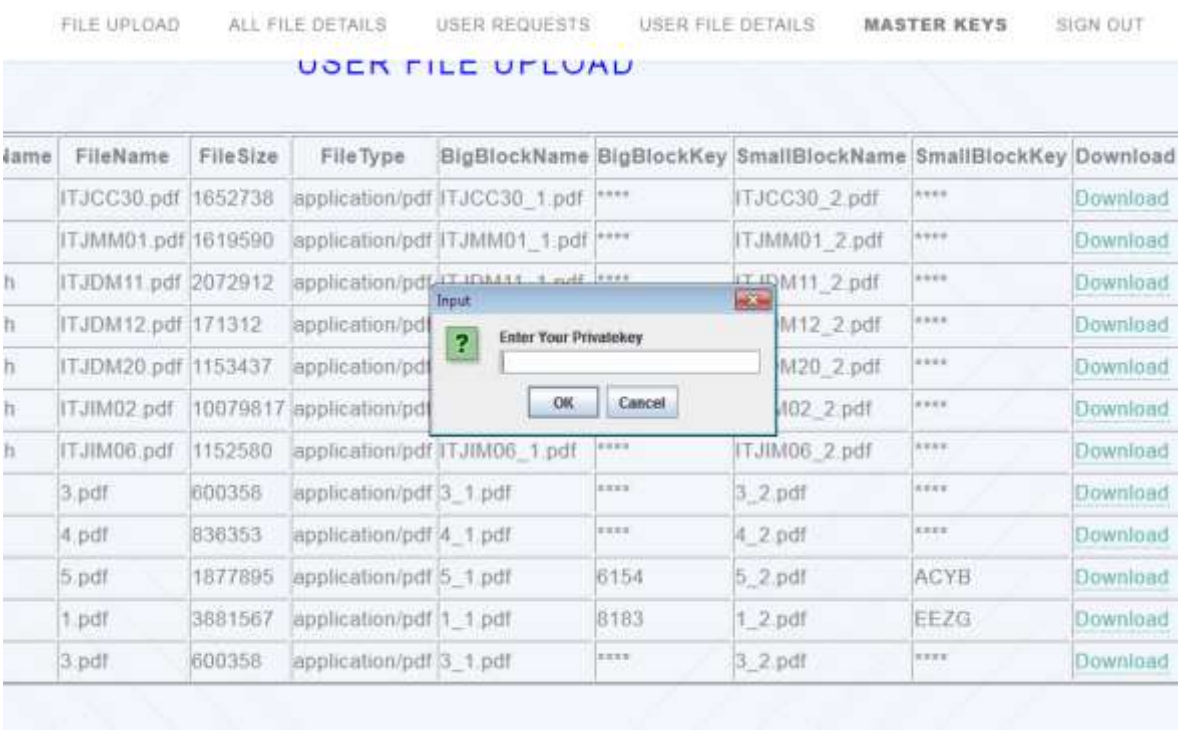


**Fig 9: file download (private key)**

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

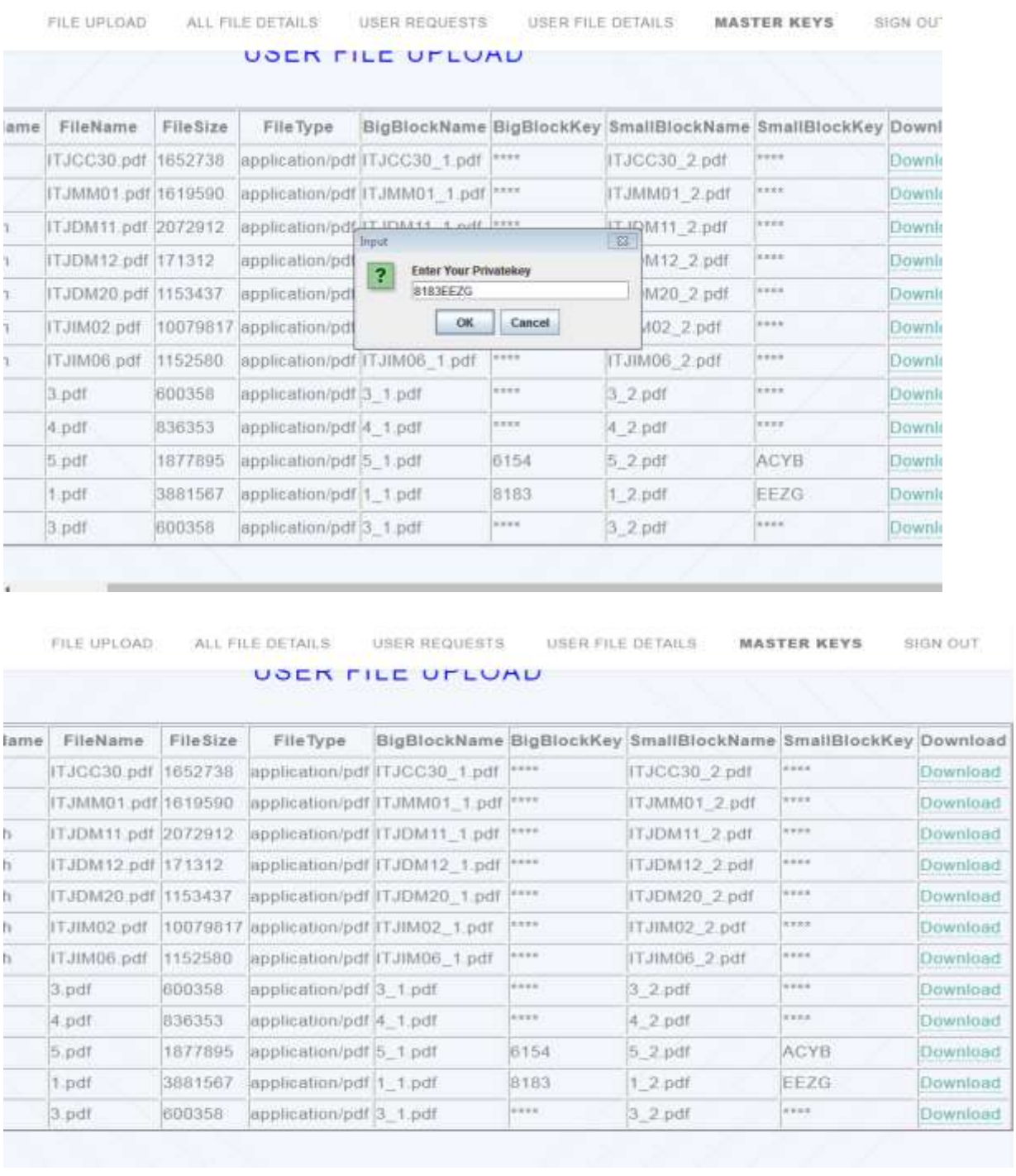


**Fig 10. file download (block keys)**

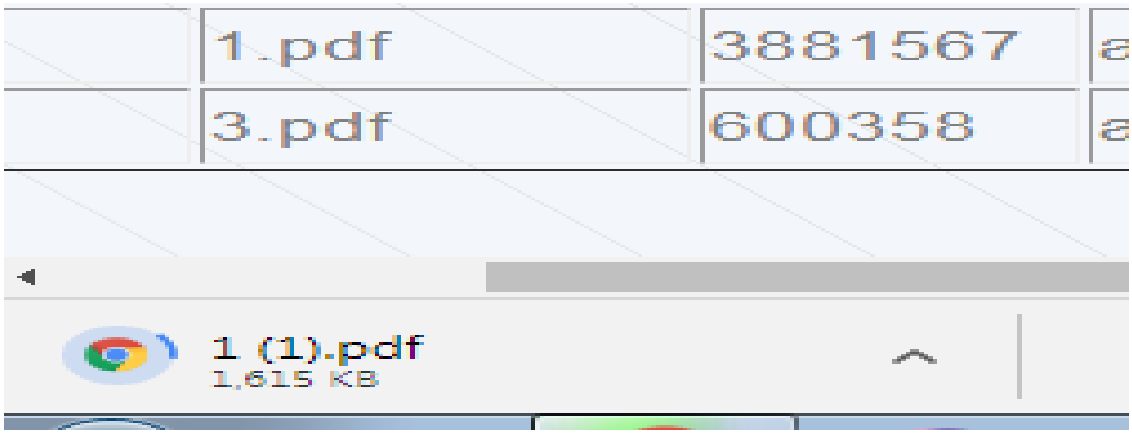


**Fig 11 :file downloaded**

## IV.RESULT AND DISCUSSIONS

MPRE-CPABE is proposed to protect user's privacy for cloud storage system in this paper. With MPRE-CPABE,a file is partitioned into two blocks before uploaded. The big block is symmetrically encrypted by the small one, so that user has to decrypt ciphertext of symmetric key first.If a malicious user tries to decrypt ciphertext without decrypting its related symmetric key, he/she cannot get

the complete file, which enhances the data security.

We created a system for Ciphertext-Policy Attribute Based Encryption. Our system allows for a new type of encrypted access control where user's private keys

specified by a set of attributes and a party encrypting data can specify a policy over these attributes specifyingwhich users are able to decrypt.

This structure makes themulti-authority system able to perform complicated ,fine-grained and efficient access control operations, and can share risks when an authority is cracked.

## V.CONCLUSION AND FUTURE WORK

### 5.1 CONCLUSION

When a user'saccess is revoked, the proxy re-encryption is used to move some tasks to the data storing and processing module,so that the cloud resources can be fully used and the Computational costs at the client side will be reduced. The proposed scheme can be further improved into the searchable MPRE-CPABE. The file names in the cloudare also encrypted. Users search the key words of file names, and the files that have the corresponding names would be found.

### 5.2 FUTURE WORK

In the future, it would be interesting to consider attribute-based encryption systems with different types of expressibility. While, Key-Policy ABE and Ciphertext-Policy ABE capture two interesting and complimentary types of systems there certainly exist other types of systems. The primary challenge in this line of work is to find a new systems with elegant forms of expression that produce more than an arbitrary combination of techniques.

In the future, Renren would execute VoteTrust periodically to detect newly Created Sybils. After the detection threshold if has been bootstrapped, Renren can use an adaptive feedback scheme to dynamically tune the threshold on the fly. The adaptive feedback is drawn from the customer complaint rate to Renren's support department. For example, Renren can raise or lower the threshold to maintain an acceptable complaint rate..

### REFERENCES

[1] J. R. Douceur, "The Sybil attack," in Proc. of IPTPS, March 2002.

[2] Z. Yang, C. Wilson, X. Wang, T. Gao, B. Y. Zhao, and Y. Dai,"Uncovering social network sybils in the wild," in Proc. of IMC,2011.

[3] H. Gao, J. Hu, Wilson, Z. Li, Y. Chen, and B. Y. Zhao, "Detecting and characterizing social spam campaigns," in Proc. of IMC, 2010.

[4] C. Grier, K. Thomas, V. Paxson, and M. Zhang, "@spam: the underground on 140 characters or less," in Proc. of CCS, 2010.

[5] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybil guard: defending against sybil attacks via social networks," in Proc. Of SIGCOMM, 2006.

[6] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, "Sybil limit: Anear-optimal social network defense against sybil attacks," in Proc. of IEEE S&P, 2008.

[7] W.Wei, F. Xu, C. C. Tan, and Q. Li, "Sybil defender: Defend against sybil attacks in large social networks," in Proc. of INFOCOM, 2012.

[8] G. Danezis and P. Mittal, "Sybil infer: Detecting sybil nodes using social networks," in Proc of NDSS, 2009.

[9] N. Tran, B. Min, J. Li, and L. Subramanian, "Sybil-resilient online content voting," in Proc. of NSDI, 2009.

[10] B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove, "An analysis of social network-based sybil defenses," in Proc. of SIGCOMM,2010.

[11] J. Xue, Z. Yang, X. Yang, X. Wang, L. Chen, and Y. Dai, "Vote trust: Leveraging friend invitation graph to defend against social network sybils," in Proc. of INFOCOM, 2013.

[12] J. Jiang, C. Wilson, X. Wang, P. Huang, W. Sha, Y. Dai, an dB. Y. Zhao, "Understanding latent interactions in online social networks," in Proc. of IMC, 2010.

[13] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All your contacts are belong to us: automated identity theft attacks on social networks," in Proc. of WWW, 2009.

[14] Y. Boshmaf, D. Logothetisy, G. Siganosz, J. L. Jorge Ler´ıax, M. Ripeanu,and K. Beznosov, "´Integro: Leveraging victim prediction for robust fake account detection in osns," in Proc. of NDSS, 2015.

[15] Z. Gyongyi, H. Garcia-molina, and J. Pedersen, "Combating web spam with trust rank," in VLDB. Morgan Kaufmann, 2004, pp.576–587.

[16] Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro, "Aiding the detection of fake accounts in large scale social online services, "in nsdi, 2012.

[18] L. G. Valiant, "A bridging model for parallel computation,"Commun. ACM, vol. 33, no. 8, pp. 103–111, Aug. 1990.

[19] A. Cheng and E. Friedman, "Sybil proof reputation mechanisms, "in Proc. of P2PECON, 2005.

[20] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigen trust algorithm for reputation management in P2P networks," in Proc. of WWW, Budapest, Hungary, May 2003.