Implementing Aggregate-Key for Sharing Data in Cloud Environment using Cryptographic Encryption

K.P.Kaliyamurthie, G.Michael, R.Elankavi, Stephen Anto Jijo

Abstract*: Data Information sharing is a fundamental comfort in scattered limit. In this paper, we prompt the best way to deal with safely, advantageously, and adaptably share information with others in appropriated accumulating. We portray new open key cryptosystems that produce relentless size figure messages to such an extent, that fruitful task of translating rights for any strategy of ciphertexts is conceivable. Everything considered, the mystery key holder can discharge an enduring size supreme key for flexible decisions of ciphertext set in dispersed accumulating, at any rate the other blended records outside the set stay classified..Key Words - Short Text Classification, Content based isolating, Policy based personalization, Online Social Networks sharing.

Keywords:Cryptographic,Multi encryption process,Data forwading ,intergrity checking.

I INTRODUCTION

Disseminated figuring has been envisioned as the front line building of IT undertaking, in light of its not immaterial once-over of extraordinary good conditions in the IT history.Instances of power outages and security breaks of basic cloud organizations appear occasionally.To say it evidently, notwithstanding the way that redistributing data into the cloud is monetarily engaging for the cost and unusualness of whole deal far reaching scale data amassing, it doesn't offer any guarantee on data decency and availability.

A. Proposed System Description:

In this paper, our worry declaration is "To design a capable open key encryption plan which supports versatile arrangement as in any subset of the ciphertexts (made by the encryption plot) is dishonor consumable by a relentless size unscrambling key (delivered by the owner of the pro puzzle key)." In KAC, clients scramble a message under an open key, yet besides under an identifier of ciphertext called class. That construes the ciphertexts are in addition coordinated into various classes. The key proprietor holds a professional riddle called star enigma key, which can be utilized to oust mystery keys for various classes

Revised Manuscript Received on June 22, 2019.

K.P.Kaliyamurthie,Department of computer science and engineering ,Bharath Institute of Higher Education and Research, Chennai Thamilnadu, India.

G.Michael,Department of computer science and engineering ,Bharath Institute of Higher Education and Research, Chennai Thamilnadu, India.

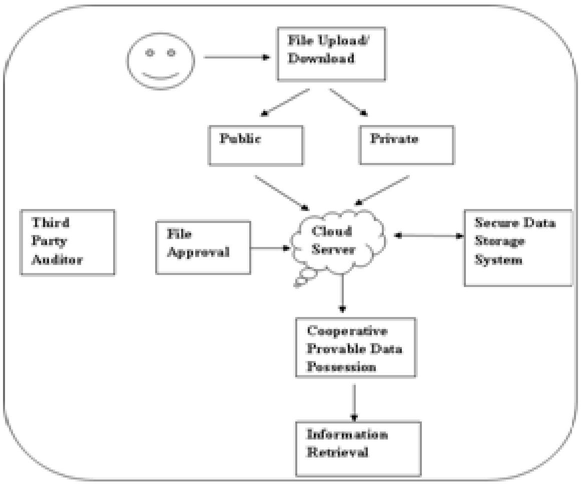
R.Elankavi Department of computer science and engineering,Bharath Institute of Higher Education and Research,Chennai, Thamilnadu,,India.

Stephen Anto Jijo, Department of computer science and engineering,Bharath Institute of Higher Education and Research,Chennai, Thamilnadu,,India.

II. PROPOSED SYSTEM DESCRIPTION:

In this paper, our worry declaration is "To design a capable open key encryption plan which supports versatile arrangement as in any subset of the ciphertexts (made by the encryption plot) is dishonor consumable by a relentless size unscrambling key (delivered by the owner of the pro puzzle key)." In KAC, clients scramble a message under an open key, yet besides under an identifier of ciphertext called class. That construes the ciphertexts are in addition coordinated into various classes. The key proprietor holds a professional riddle called star enigma key, which can be utilized to oust mystery keys for various classes

A.System Architecture



Architecture:

III. SYSTEM ANALYSIS

B. Scope:

This report is the remarkable case that portrays the prerequisites of the structure. It is proposed for the utilization by the authorities, and will in like way by the reason behind supporting the keep going passed on framework. Any developments made to the necessities later on should experience a formal change bolster process.

C. User Characteristics:-

The user of the system will be a member who is registered or administrator.

D. Modules:

- Access Control

Retrieval Number: I32030789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3203.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

- Multi Encryption Process
- Integrity Checking
- Data Forwarding

IV. MODULE DESCRIPTION:

E.Access Control:

the customer enrollment the executive. In case any of the customer needs to modify their information they have present the nuances to the chairman after that the head will update information process.

F. Multi Encryption Process:

The two activities are find the opportunity to control and endorsement control. Access control - MES calculation. Access control procedure depends upon the server control highlights. Endorsement control procedure depends upon the customer control features

G. Integrity Checking:

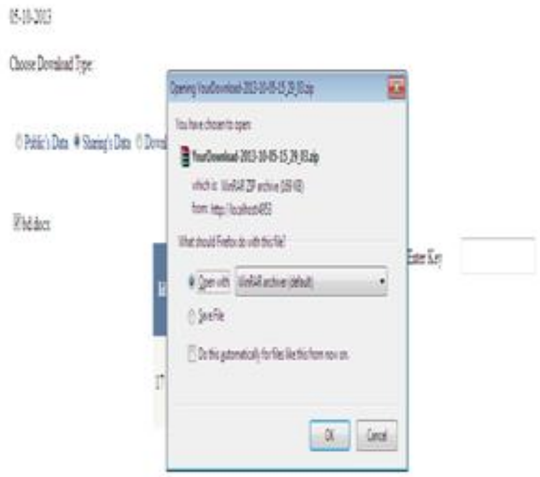
Uprightness toward contrasting the scrambled data and changed figure content. In the event that there is any adjustment in identification will send to the consumer that the encryption procedure isn't done legitimately. In the event that there is no adjustment in recognition implies, at that point it will permit doing the following procedure. The client can see the information and furthermore information.

H. Data Forwarding:

On the off chance that any client needs to impart their data to their companions or somebody they can legitimately advance the encoded information to them. Without downloading the information the client can advance the data to another client.

V. OUTPUT SNAPSHOTS:

I. File downloaded



05-10-2013

Choose Download Type:

○ Public's Data ● Sharing's Data ○ Dow

☑ bd.docx

Enter Key

Opening YouDownload-2013-10-05-15_29_03.zip

You have chosen to open:

YouDownload-2013-10-05-15_29_03.zip

which is: WinRAR ZIP archive (169 KB)

from: http://localhost:4053

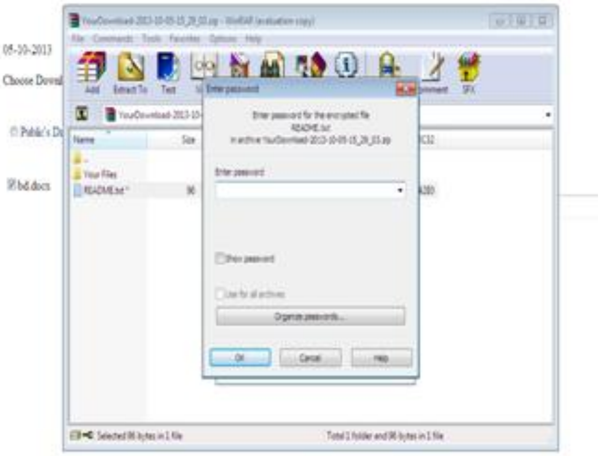
What should Firefox do with this file?

● Open with WinRAR archiver (default)

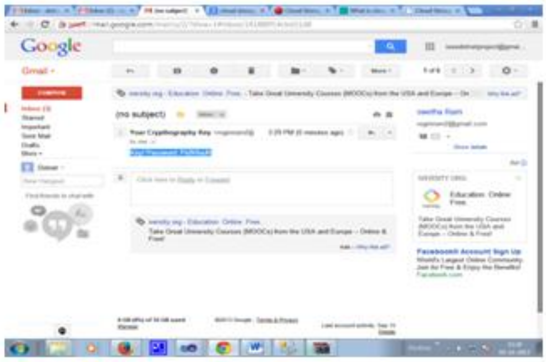
○ Save File

□ Do this automatically for files like this from now on.

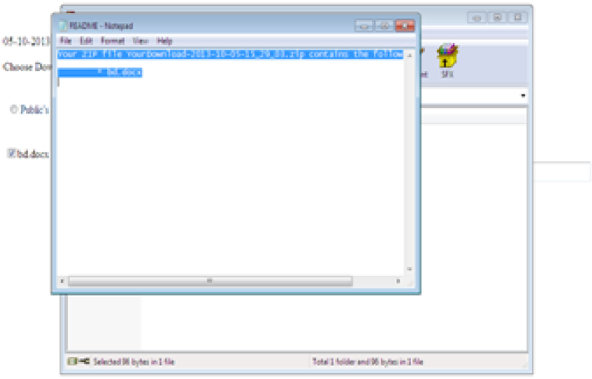
J. Key sent to your mail id



K. Enter the key which you got in your Mail



L .Original data is viewed


README - Notepad
File Edit Format View Help
05-10-2013
Choose Do
Public's
☑bd.docx
SFX
Selected 86 bytes in 1 file
Total 1 folder and 86 bytes in 1 file

```
Your ZIP file YourDownload-2013-10-05-15_29_03.zip contains the follow
        * bd.docx
```

VI.CONCLUSIONS

We improved an attractively implementable modification of the key-through and through cryptosystem(KAC).

We have moreover indicated how the focal KAC structure might be competently extended and summed up for safely passing on the total key among different information clients in a veritable information sharing condition. The outcomes build up that KAC with complete key pass on beats other existing secure information sharing plans concerning execution and scalability

REFERENCES

[1] IDC Enterprise Panel. It cloud services user survey, pt. 3:Whatusers want from cloud services providers, august 2008.

[2] Sherman SM Chow, Yi-Jun He, Lucas CK Hui, and Siu Ming Yiu. Spice–simple privacy-preserving identity-management . In Applied Cryptography and Network Security, pages526–543. Springer, 2012.

[3] Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, and Wenjing Lou. Privacy-preserving public auditing for secure cloud storage. Cryptology ePrint Archive, Report 2009/579, 2009.http://eprint.iacr.org/.

[4] Sherman SM Chow, Cheng-Kang Chu, Xinyi Huang, JianyingZhou, and Robert H Deng. Dynamic secure cloud storage with provenance. In Cryptography and Security: From Theory to Applications, pages 442–464. Springer, 2012.

[5] Erik C Shallman. Up in the air: Clarifying cloud storage protections. Intell. Prop. L. Bull., 19:49, 2014.

[6] Cheng-Kang Chu, Sherman SM Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H Deng. Key-aggregate cryptosystem for scalable data sharing in cloud storage. Parallel and Distributed Systems, IEEE Transactions on, 25(2):468–477, 2014.

[7] Dan Boneh, Craig Gentry, and Brent Waters. Collusion resistantbroadcast encryption with short ciphertexts and private keys. InAdvances in Cryptology–CRYPTO 2005, pages 258–275. Springer,2005.Problem of access control in a hierarchy. ACM Transactions onComputer Systems (TOCS), 1(3):239–248, 1983.

[9] Gerald C Chick and Stafford E Tavares. Flexible access controlwith master keys. In Advances in CryptologyCRYPTO89 Proceedings,pages 316–322. Springer, 1990.

[10] Wen-Guey Tzeng. A time-bound cryptographic key assignmentscheme for access control in a hierarchy. Knowledge and DataEngineering, IEEE Transactions on, 14(1):182–188, 2002.[11] Giuseppe Ateniese, Alfredo De Santis, Anna Lisa Ferrara, andBarbara Masucci. Provably-secure time-bound hierarchical keyassignment schemes. Journal of cryptology, 25(2):243–270, 2012.

[12] Ravinderpal S Sandhu. Cryptographic implementation of a treehierarchy for access control. Information Processing Letters, 27(2):95–98, 1988.

[13] Yan Sun and KJ Liu. Scalable hierarchical access control insecure group communications. In INFOCOM 2004. Twenty-thirdAnnualJoint Conference of the IEEE Computer and CommunicationsSocieties, volume 2, pages 1296–1306. IEEE, 2004.

[14] William C King and Bjorn Hjelm. Centralized key management,March 24 2015. US Patent 8,990,555.

[15] Mikhail J Atallah, Marina Blanton, Nelly Fazio, and Keith BFrikken. Dynamic and efficient key management for access hierarchies. ACM Transactions on Information and System Security(TISSEC), 12(3):18, 2009.

[16] Jeremy Horwitz and Ben Lynn. Toward hierarchical identity-basedencryption. In Advances in CryptologyEUROCRYPT 2002, pages466–481. Springer, 2002.

[17] Dan Boneh, Xavier Boyen, and Eu-Jin Goh. Hierarchical identitybased encryption with constant size ciphertext. In Advances inCryptology–EUROCRYPT 2005, pages 440–456. Springer, 2005.

[18] Brent Waters. Efficient identity-based encryption without randomoracles. In Advances in Cryptology–EUROCRYPT 2005, pages 114–127. Springer, 2005.

[19] Xavier Boyen and Brent Waters. Anonymous hierarchical identitybased encryption (without random oracles). In Advances inCryptology-CRYPTO 2006, pages 290–307. Springer, 2006.

[20] Adi Shamir. Identity-based cryptosystems and signature schemes.In Advances in cryptology, pages 47–53. Springer, 1985.

[21] Dan Boneh and Matthew Franklin. Identity-based encryption fromthe weil pairing. SIAM Journal on Computing, 32(3):586–615, 2003.

[22] Clifford Cocks. An identity based encryption scheme based onquadratic residues. In Cryptography and coding, pages 360–363.Springer, 2001.

[23] Fuchun Guo, Yi Mu, and Zhide Chen. Identity-based encryption:how to decrypt multiple ciphertexts using a single decryptionkey. In Pairing-Based Cryptography–Pairing 2007, pages 392–406.Springer, 2007.

[24] Fuchun Guo, Yi Mu, Zhide Chen, and Li Xu. Multi-identity singlekey decryption without random oracles. In Information Security and Cryptology, pages 384–398. Springer, 2008.

[25] Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In Advances in Cryptology–EUROCRYPT 2005, pages 457–473.Springer, 2005.

[26] Vipul ,Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computerand communications security, pages 89–98. Acm, 2006.

AUTHORS PROFILE

K.P.Kaliyamurthie, Professor, Department of Computer Science & Engineering, Bharath Institute of Higher Education and Research, Chennai, India

G.Michael, Associate Professor,Department of CSE, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu, India.

R.Elankavi, Assistant Professor, Department of Computer Science & Engineering, Bharath Institute of Higher Education and Research, Chennai, India

Stephen Anto Jijo, Assistant Professor, Department of Computer Science & Engineering, Bharath Institute of Higher Education and Research, Chennai, India