Materials Today: Proceedings 37 (2021) 2818–2821

Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

Self-destruction of data in cloud using asymmetric key with key generator

S. Prasanna [a,*], S. Chinnapparaj [b], D. Devi [c], A. Athithya Janani [c], S. Sophia [c]

[a] Department of Computer Science and Engineering, Mailam Engineering College, Mailam, Tamilnadu, India
[b] Department of ECE, Hindusthan Institute of Technology, Coimbatore, Tamilnadu, India
[c] Department of ECE, Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu, India

ARTICLE INFO

Article history:
Received 14 August 2020
Accepted 25 August 2020
Available online 1 October 2020

Keywords:
Cryptographic-key
Proxy re-encryption
Key separation
Security analysis
Asymmetric key

ABSTRACT

Individuals support the incredible intensity of distributed computing, however can't completely believe the cloud suppliers to have protection delicate information, because of the nonappearance of client to-cloud controllability. To guarantee privacy, information proprietors re-appropriate scrambled information rather than plaintexts. To impart the scrambled documents to different clients, Cipher text-Policy Attribute-based Encryption (CP-ABE) can be used to direct fine-grained and proprietor driven access control. This is accomplished by keeping key position framework and capacity hubs in two unique ways. Over an unreliable channel, an open key is produced alongside the comparing private key and give to number of clients independently. The Key gave is free of different keys for every clients.

Selection and peer-review under responsibility of the scientific committee of the International Conference on Newer Trends and Innovation in Mechanical Engineering: Materials Science.

1. Introduction

The mutual information in cloud servers contains client's touchy data (e.g., individual profile, money related information, well-being records, and so forth.) that are should have been all around secured. The cloud servers may move clients' information to other cloud servers in re-appropriating or share them in cloud looking as the responsibility for information is isolated from the organization of' them. It is a major test to secure the protection of those mutual information in cloud in cross-cloud and huge information condition. When the client characterized time is lapsed the common information ought to act naturally demolished. The capacity of information as a typical scrambled structure is one of the techniques to lighten the issues. The client can't share his/her encoded information at a fine-grained level is the significant detriment of scrambling information. The huge preferred position dependent on the custom open key encryption rather than coordinated encryption is accomplished through the Attribute-based encryption (ABE). The two information security and fine-grained get to control can be accomplished through ABE (Attribute-based encryption) plot. The figure text is named with set of enlightening properties by the key-strategy ABE (KP-ABE) conspire. The encryption administration has been given by the Timed-discharge encryption (TRE) where an encryption key is related with a predefined discharge time, and a collector can just develop the comparing decoding key in this time case Time-Specific [1,2].

Encryption (TSE) plot on the premise, which is utilized to determine a reasonable time stretch with the end goal that the figure text must be unscrambled in this span. The ABE is applied to the mutual information that will acquaint a few issues with respect with time explicit imperative and implosion and applying TSE, will acquaint issues with respect with fine-grained get to control. This paper endeavor to tackle these issues by utilizing KPABE and including a requirement of time span to each quality in the arrangement of decoding properties [3,4].

2. Existing system

Sharing information among clients is maybe one of the most captivating highlights that inspire distributed storage. There are a progression of cryptographic plans which go similarly as permitting an outsider examiner to check the accessibility of documents in the interest of the information proprietor without spilling anything about the information, or without trading off the information

* Corresponding author.
E-mail address: prasannacse@mailamengg.com (S. Prasanna).

https://doi.org/10.1016/j.matpr.2020.08.655
2214-7853/© 2020 Elsevier Ltd. All rights reserved.
Selection and peer-review under responsibility of the scientific committee of the International Conference on Newer Trends and Innovation in Mechanical Engineering: Materials Science.

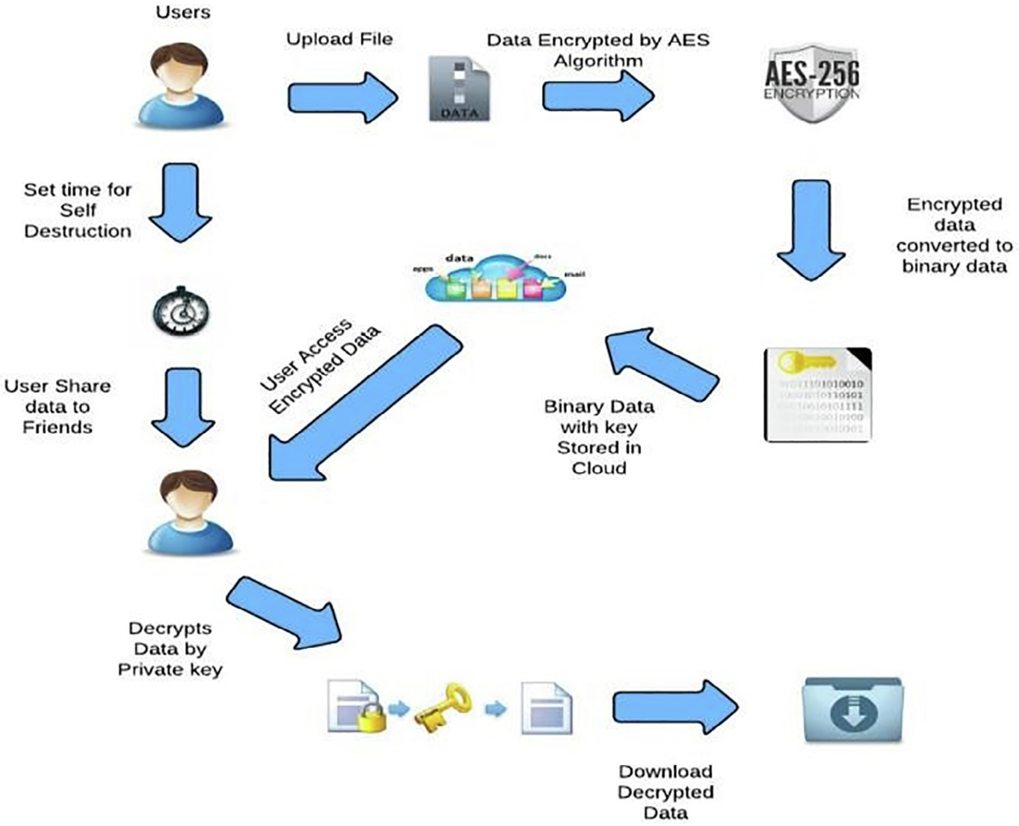

Users
Upload File
DATA
Data Encrypted by AES Algorithm
AES-256 ENCRYPTION
Set time for Self Destruction
Encrypted data converted to binary data
data
apps
docs
email
User Access Encrypted Data
User Share data to Friends
Binary Data with key Stored in Cloud
Decrypts Data by Private key
Download Decrypted Data

Fig. 1. Architecture.

proprietor's secrecy. The issue emerges when a document is shared to numerous clients [5–7].

3. Proposed system

A key-arrangement property based encryption with time-determined characteristics (KP-TSABE), a novel secure information Autolysis of Data conspire in distributed computing is proposed here. Each ciphertext is marked with a period span while private key is related with a period moment in the KP-TSABE conspire. on the off chance that both the time moment is in the permitted time stretch and the properties related with the ciphertext fulfill the key's entrance structure the ciphertext must be decoded. Secure Data Sharing in Clouds (SeDaSC) strategy that gives is proposed here: 1) information classification and uprightness; 2) get to control; 3) information sharing (sending) without utilizing figure serious re encryption; 4) insider danger security; and 5) forward and in reverse access control 6) One time download 7) Share Time Expire 8) Secret Key Management [8–10].

3.1. Authentication and approval

In this module, the User needs to enroll first, and afterward just the person can get to the information base. When the enrollment is finished, the client can login to the site. The approval and validation process is utilized to encourage the framework to secure itself and it too shields the entire system from unapproved use. The Registration includes in getting the subtleties of the clients who needs to utilize this application [11–13].

3.2. File encryption and decryption

In this module, the client transfers the records which he/she needs to share. At first, the transferred documents will be put away in the Local System. Next the client will transfer the document to the genuine Cloud Storage (In this application, Dropbox is utilized). While transferring the record to the Cloud, the document gets encoded by utilizing the AES (Advanced Encryption Standard) Algorithm and the Private Key will be produced. At that point the Encrypted Data will be changed over to Binary Data for Data security and will be put away in Cloud [14–19].

3.3. File sharing

The transferred records will be shared to the companions or clients in this module. The Data Owner will set an opportunity to terminate the information in Cloud. The Private Key of the Shared Data is sent through Email [20–26].

3.4. File decryption and download

In this Module, the client can download the information by decoding strategy. This should be possible by utilizing the AES (Advanced Encryption Standard) Algorithm. The clients must give the relating Private Keys so as to unscramble the information. On the off chance that the client enters the Wrong Private Key for Multiple times, at that point the Data will be erased. A suggestion email will be sent to the Data proprietor, if the document gets erased. The Downloaded Data is put away in the Local Drive [27–34].

3.5. File autolysis of data and access control

In this module, the Data will be erased naturally if the User doesn't download the record effectively inside the time given by the information proprietor. The File Autolysis will be crippled if the client downloads the information. An implication Email will be sent to the Data Owner if the document gets erased by the File Autolysis Scheme. On the off chance that any vindictive is connected to the common record, at that point the mutual client will get a hint i.e., to hinder the regressive access in the site. Model: If a client to logout account at that point can't return our past page [35–37].

4. System architecture

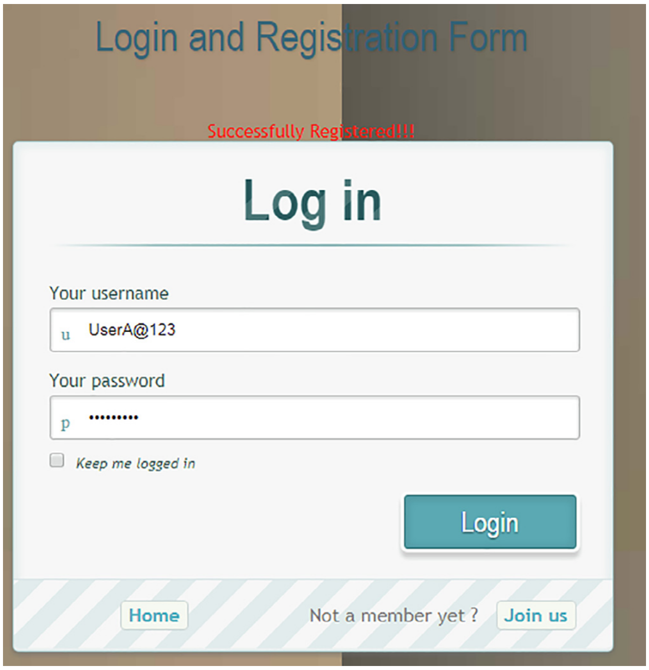
(See Fig. 1).

5. Result

In this venture, the SeDaSC procedure, which is a distributed storage security conspire for bunch information is proposed. The proposed procedure gives information privacy, secure information sharing without re-encryption, get to control for pernicious insiders, and forward and in reverse access control. The SeDaSC technique gives guaranteed cancellation by erasing the boundaries required to unscramble a document [38–41] (see Figs. 2–4).

6. Conclusion

In this undertaking, the SeDaSC strategy, which is a distributed storage security plot for bunch information is proposed. The proposed technique gives information secrecy, secure information sharing without re-encryption, get to control for vindictive insiders, and forward and in reverse access control. The SeDaSC procedure gives guaranteed erasure by erasing the boundaries required to unscramble a file. Since this task is just about sharing documents to companions perform PC activities this undertaking has been structured remembering the future extensions. What this undertaking pointed and accomplished making isn't an item however an instrument to a superior car condition, a device can be utilized to shape numerous things in the Future. Subsequently this undertaking will offer ascent to numerous future adjustments forking every which way. A portion of the not so distant future extents of this undertaking are: There are not many intriguing issues to be kept on reading for the future work. One of them is the client can share a document to multi clients one after another. The AES (Advanced Encryption Scheme) to scramble the Data is utilized in this venture. In future this application can be created utilizing various kinds of cutting edge calculation for Encryption.



Login and Registration Form

Successfully Registered!!!

Log in

Your username

u UserA@123

Your password

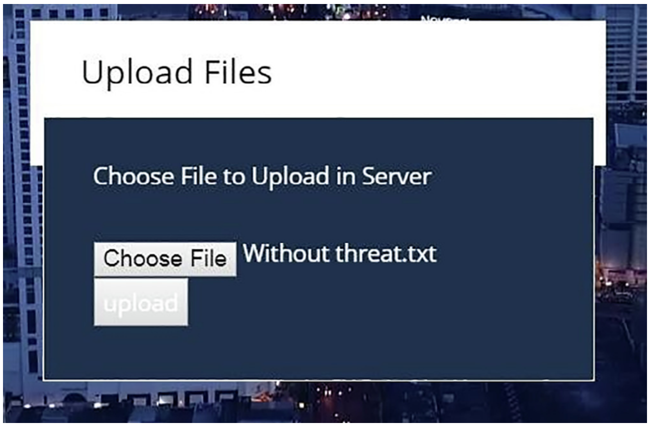
p •••••••••

□ Keep me logged in

Fig. 2. Login Page.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

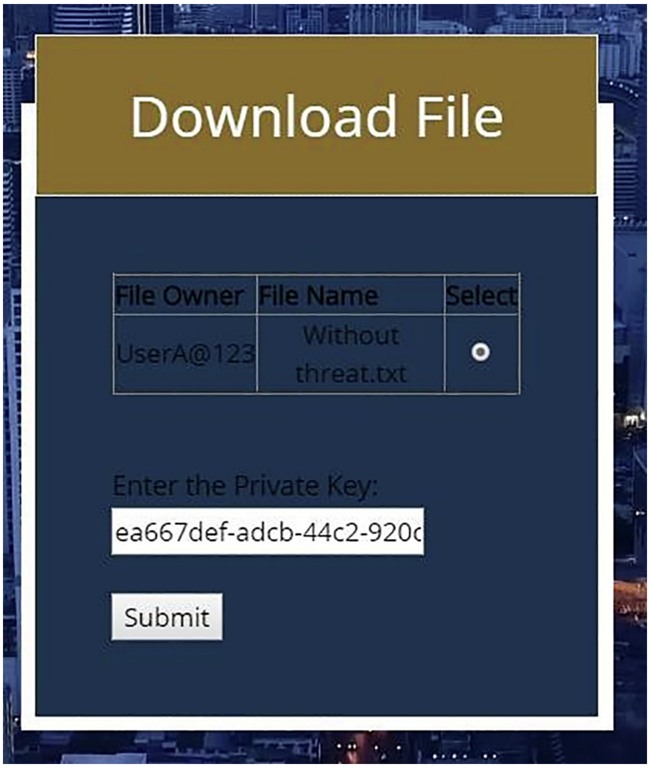


Upload Files

Choose File to Upload in Server

Choose File Without threat.txt

Fig. 3. File Upload.



Download File

File Owner	File Name	Select
UserA@123	Without threat.txt	●

Enter the Private Key:

ea667def-adcb-44c2-920c

Fig. 4. Download file.

References

[1] B. Wang, B. Li, H. Li, IEEE Trans. Cloud Computing 2 (1) (2014) 43–56.

[2] J. Xiong, Z. Yao, J. Ma, X. Liu, Q. Li, J. Ma. KSII Trans. Internet Information Syst. (TIIS), 8 (1) (2014) 282–304.

[3] J. Xiong, F. Li, J. Ma, X. Liu, Z. Yao, P.S. Chen. Peerto-Peer Networking and Applications. [Online]. Available: http://dx.doi.org/10.10 07/s12083-014-0295-x.

[4] P. Jamshidi, A. Ahmad, C. Pahl, IEEE Trans. Cloud Computing 1 (2) (2013) 142–157.

[5] R. Lu, H. Zhu, X. Liu, J.K. Liu, J. Shao, IEEE Network 28 (4) (2014) 46–50.

[6] X. Liu, J. Ma, J. Xiong, G. Liu, Int. J. Network Security 16 (4) (2014) 351–357.

[7] A. Sahaand, B. Waters, Advances in Cryptology–EUROCRYPT 2005, ser. LNCS, vol. 7371. Springer, 2005, pp. 457–473.

[8] V. Goyal, O. Pandey, A. Sahai, B. Waters. Proceedings of the 13th ACM conference on Computer and Communications Security. ACM, 2006, pp. 89–98.

[9] F. Chan, I. F. Blake. Proceedings of the International Conference on Distributed Computing Systems. IEEE, 2005, pp. 504–513.

[10] K.G. Paterson, E.A. Quaglia, Security and Cryptography for Networks, Springer, 2010, pp. 1–16.

[11] Mrs.E. Lavanya, Int. J. Res. Eng., Sci. Technol. (IJREST) 1 (7) (Apr 2016).

[12] Mr.S. Prasanna, Int. Res. J. Adv. Eng. Technol. 3 (5) (Oct 2017).

[13] Q. Li, J. Ma, R. Li, J. Xiong, X. Liu. Security and Communication Networks, 2014. [Online]. Available: http://dx.doi.org/10.1002/sec. 997.

[14] J. Bethencourt, A. Sahai, B. Waters, Proceedings of the 28th IEEE Symposium on Security and Privacy, IEEE, 2007, pp. 321–334.

[15] L. Cheung, C.C. Newport, Proceedings of the 14th ACM conference on Computer and communications security, ACM, 2007, pp. 456–465.

[16] S.A. SivaKumar, R. Naveen, D. Dhabliya et al., Mater. Today: Proc., doi: 10.1016/j.matpr.2020.07.064.

[17] B. Maruthi Shankar, S.A. Sivakumar, B. Vidhya et al., Mater. Today: Proc., doi: 10.1016/j.matpr.2020.07.065.

[18] S.A. Sivakumar, S. Karthikeyan, M. Benedict Tephila, R. Senthil Ganesh, R. Sarath Kumar, B. Maruthi Shankar. IJAST, 29 (8s) (May 2020) 2254–2260.

[19] T. Sathish, Dinesh Kumar Singaravelu, J. Sci. Industrial Res., NISCAIR Publisher 79 (6) (2020) 547–551.

[20] T. Sathish, Dinesh Kumar Singaravelu, J. Sci. Industrial Res., NISCAIR Publisher 79 (5) (2020) 449–452.

[21] T. Sathish, S. Karthick, J. Mater. Res. Technol. Elsevier Publisher 9 (3) (2020) 3481–3487.

[22] Thanikodi Sathish, Singaravelu Dinesh Kumar, Devarajan Chandramohan, Venkatraman Vijayan, Rathinavelu Venkatesh, Therm. Sci., Vinca Inst. Nuclear Sci. 24 (1B) 575–581.

[23] Krishnaswamy Haribabu, Muthukrishnan Sivaprakash, Thanikodi Sathish, Arockiaraj Godwin Antony, Venkatraman Vijayan, Therm. Sci., Vinca Inst. Nuclear Sci. 24 (1B) 495–498.

[24] Muthukrishnan Sivaprakash, Krishnaswamy Haribabu, Thanikodi Sathish, Sundaresan Dinesh, Venkatraman Vijayan, Therm. Sci., Vinca Inst. Nuclear Sci. 24 (1B) (2020) 499–503.

[25] T. Sathish, J. Mater. Res. Technol. Elsevier Publisher 8 (5) (2019) 4354–4363.

[26] T. Sathish, Trans. Canadian Soc. Mech. Eng. 43 (04) (2019) 509–514.

[27] T. Sathish, Trans. Canadian Soc. Mech. Eng. 43 (04) (2019) 551–559.

[28] T. Sathish, J. New Mater. Electrochem. Syst. 22 (1) (2019, 2019,) 5–9.

[29] T. Sathish, Int. J. Ambient Energy, Taylor and Francis Publishers,2019, Accepted, DOI: 10.1080/01430750.2019.1608861.

[30] T. Sathish, J. Jayaprakash, P.V. Senthil, R. Saravanan, FME Trans. 45 (1) (2017) 172–180.

[31] T. Sathish, J. New Mater. Electrochem. Syst. 20 (2017) 161–167.

[32] T. Sathish, Journal of Applied Fluid Mechanics 10 (24) (2017) 41–50.

[33] T. Sathish, J. Appl. Fluid Mech. 11 (2018) 39–44.

[34] T. Sathish, J. New Mater. Electrochem. Syst. 21 (3) (2018) 179–185.

[35] T. Sathish, Mater. Today Proc. Elsevier Publisher 05 (6) (2018) 14416–14422.

[36] T. Sathish. Lecture notes on Mechanical Engineering – Springer, 2018, Accepted, Doi: https://doi.org/10.1007/978-981-13-6374-0_45.

[37] T. Sathish, Int. J. Ambient Energy, Taylor and Francis Publishers, 41 (07) (2020) 1–6.

[38] T. Sathish, Mater. Today Proc. Elsevier Publisher 05 (6) (2018) 14448–14457.

[39] T. Sathish, Mater. Today Proc. Elsevier Publisher 05 (6) (2018) 14545–14552.

[40] T. Sathish, S. Dinesh Kumar, K. Muthukumar, S. Karthick, Mater. Today Proc., Elsevier Publisher 21 (1) (2020) 847–856.

[41] Dr. T. PriyaRadhikaDevi, Int. Res. J. Adv. Eng. Technol. (IRJAET) 2 (6) center000.