IJARIIT
INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 2)
Available online at: www.ijariit.com

An Efficient Framework Security Model of Sharing Data for Privacy Protection and Performance-Based Outsource Data Sharing on Cloud

Kiren Vijai
kiren.vijai@gmail.com
Mangalam College of Engineering, Kottayam, Kerala

Syamamol T
syamamol.t@mangalam.in
Mangalam College of Engineering, Kottayam, Kerala

Merlin Mary James
merlin.james@mangalam.in
Mangalam College of Engineering, Kottayam, Kerala

ABSTRACT

One of the most efficient cryptanalysis systems of elegant data is stored and more data sharing file to be cached through the cloud. Be the part of the unusual weakness is the pivotal administration block of notoriety over the appliances. One of the main disadvantages is the pivotal pledge complication. While transferring the confidential file from one system to another there is a chance to leak the data from the system and can lose the privacy. The front-end gadgets of customers like advanced mobile phones by and large have constrained security assurance, the personal pivotal exist completely maintained and customers hazard pivotal introduction especially not really seen however inalienably existed in past research. Besides, gigantic customer decoding overhead constrains the handy utilization of ABE. The proposed system is that a shared key administration convention in CP-ABE. The development acknowledges disseminated age, drawback along with capacity over personal pivotal left out including some additional framework. The efficient information prompt trait disavowal is accommodated vital pivotal refresh. A synergistic instrument successfully takes care of key escrow issue as well as a key introduction. In the interim, it helps extraordinarily decrease customer unscrambling overhauls. The correlation thus alternative delegate the plans exhibits the plan made to some degree better execution as far as cloud-construct outsourced information partaking in light of cell phones and thus enhance the security and privacy protection. At last, we give evidence of security to the proposed convention.

Keywords: *Efficiency, Security, Data Sharing, Cloud Data Sharing, CP-ABE.*

1. INTRODUCTION

The cost-viability upgrades in computational innovation and expansive scale systems, offering information to others turns out to be correspondingly more advantageous. Also, computerized assets are all the more effortlessly acquired through distributed evaluation, capacity. As information that can be share and stored in the framework such a few associations mutually held, remote stockpiling is by one means or another debilitating protection of information proprietors. Along these lines, upholding the assurance of personal, confidential and delicate information put away in the cloud is to a great degree urgent [23], [25], [26], [36]. The synchronous interest of an extensive number of clients requires fine-grained get to authority while information splitting. One of the most promising security to store the encrypted data to the cloud and fascinating talent for secure and flexible information splitting. One of the main characteristics of these is the one to numerous properties that implies the solitary pivotal are unscrambling diverse complex data distinctive pivotal that decodes identical complex information. The Attribute-Based Encryption is known as ciphertext strategy. The confidential data's are stored in the cloud and while transferring the data from one system to another, there is a chance to leak the file details and also chance to hack the files by the attackers. The data entrances strategies are implanted over the personal pivotal, property maintains to insert to the complex information and enables information proprietors over the data sharing technique is used to maintain the system [2], [36]. Any individual who needs to acquire information must first coordinate the entrance strategy with a property set. Because of the matter, protect the information while sharing the data during the transferring of the file from one system to another [27], [28], [36].

In any case, the considerable measure unenclosed difficulties of data sharing concerning useful acknowledge the data while particularly as far as private key administration. For huge quantities of past ABE plans [2] - [7], pivotal specialist can totally reliable, the unscramble data, the complex information that can be utilize to create personal pivotal after authorization. Getting the data or information without the permission of data from the owner generally known as key escrow issue, the innate disservice helps to debilitates client protection. Development of data sharing over versatile operation, portable data administrations [24], [31], [36] that are presented in the virtual pattern over distributed data flowing. Flow examine job scarcely sees that versatile front-end gadgets, for example, cell phones, are significantly more powerless than servers regarding security assurance [20]. In this way, the helplessness in private key insurance may effectively prompt the presentation of keys to unapproved clients [30], [5] - [29], [36]. The encrypted datas are keep to cloud and protect the file from hacking from attackers and provide more security and authentication to the system.

2. RELATED WORKS

An unique characteristic form entry limitation to an elegant pivotal refresh instrument through presenting trait aggregate pivotal to the overall system [2], [14]. The productive plan underpins much exible quality disavowal also the client repudiation that upgraded in the system also provides to store the data. The complex information capacity also the unscrambling rate i.e. real downsides to pragmatic over the system appliances [5]. To conquer these issues, a unique characteristics of the decoding system is placed an intermediary system is used a large portion through unscrambling data storage of the system to encode the data. While executing decoding, an information collector exchanges a change pivotal also complex information to be an intermediary system also gets an ciphertext. In this way, the plaintext can be extricated through extremely straightforward calculation by the information recipient. With the potential pattern of portable cloud benefit, applying outsourced unscrambling plan notably streamlines client encounter. A fluffy character based encryption (FIBE) in light of great personality based encryption [1].The character of a collector is spoken to by an arrangement of allocate the data, i.e. installed the personal pivotal. In the event that and just separation between quality arrangement over the recipient, another is the owner is encrypt the data through the limitation of the information, collector could remove the ordinary information effectively. A few numerous pivotal highlights over Attribute-Based Encryption, it established hypothetical framework over resulting testing towards Attribute-Based Encryption [21]. The examination effort showed additional development of the pivotal strategy of the Attribute base encryption, that implies every personal pivotal related along the entrance arrangement, every complex information i.e. related to the arrangement over data qualities [6], [25]. An idea over various leveled summed up properties in light of the worldwide property accumulation, and proposed a progressive multiauthority system for CP-ABE. At the point when a client characterizes an entrance structure and demands information encryption, each key age focus (KGA) produces relating access arrangement and personal pivotal for the protection over the pivotal administration are ensured [10], [32]. An Attribute Based Encryption disavowal includes a proposal, cross breed irregular quality build encryption along, mix over immediate data also roundabout renouncement. While executing encryption, every datum sender is permitted to choose which revocable plan is utilized that consolidate points of interest of the two strategies. Nothing that its half and half renouncement has no impact on decoding albeit every datum beneficiary has just a single private key [3], [9]. A solid development where the system information of the owner could adaptably characterized entrance arrangement instead of the information being scrambled [21], [2]. Subsequently, ensures information confidentiality as well as acknowledgment of independent entry constraint. Oualha et al. [35] showed that notwithstanding gigantic calculation assets are required in ABE, heaps of overwhelming calculation should be possible ahead of time. Thinking about constraint of vitality and calculation of hubs over the data utilization presenting calculation procedure that processes also be securing any basic components previously encoding happens [7], [8]. Despite the fact that ongoing calculation overhead is especially diminished, their plan requires confided in substances to store components. Facilitate many, committed network likewise need safely exchange of components wanted to store the data in the hubs. The encode rate, also the decrypt rate increment directly through multifaceted nature over entry strategy makes the complex information to the system [4].

3. EXISTING SYSTEM

Past plans of key administration in quality based information sharing framework basically centers around key refresh, intermediary re-encryption and outsourced decoding. Some examination showed untrusted key specialist may prompt key escrow issue and gave relating arrangements. In any case, challenges are facing to safeguard the data. In the event that personal pivotal totally put away including the systems like cell phone gadgets, more regrettable issue known pivotal introduction happens debilitating secrecy of private keys. In expansion, the greater part of property based information sharing plans improved protection over the system administration rate over the unscrambling reduction through information recipients. With cost-viability changes in computational innovation and expansive scale systems, offering information to others turns out to be correspondingly more helpful. Moreover, computerized assets are all the more effortlessly acquired through distributed evaluation and capacity. Since the information splitting the data framework are held with few associations together, remote stockpiling are some way or another undermining security of information proprietors. Accordingly, implementing the assurance of personal, confidential and delicate information put away in the cloud is amazingly critical [23], [25], [26], [36]. The synchronous interest of an extensive number of clients requires fine-grained get to authority while information splitting. One of the most promising security to store the encrypted data to the cloud and fascinating talent for secure and exible information splitting. One of the main characteristic of these is the one to numerous properties that implies the solitary pivotal are unscrambling diverse complex data distinctive pivotal that decodes identical complex information. The Attribute-Based Encryption known as ciphertext strategy. The confidential data's are stored in the cloud and while transferring the data from one system to another, there is chance to leak the file details and also chance to hack the files by the attackers. The data entrances strategies are implanted over the personal pivotal, property maintain to insert to the complex information and enables information proprietors over the data sharing technique is used to maintain the system [2], [36]. Any individual who needs to acquire information must first coordinate the entrance strategy with a property set. Because of the matter, protect the information while sharing the data during the transferring of file from one system to another [27], [28] [36]. In any case, the considerable measure unenclosed difficulties of data sharing concerning useful acknowledge the data while particularly as far as private key administration. For huge quantities of past ABE plans [2]-[7], [36], pivotal specialist can totally reliable, the unscramble data, the complex information that can be utilize to create personal pivotal after authorization. Getting the data or information without the permission of data from the owner generally known as key escrow issue, the innate disservice helps to debilitates client protection. Development of data sharing over versatile operation, portable data administrations [24], [31] [36] that are presented in the virtual pattern over distributed data flowing. Flow examine job scarcely sees that versatile front-end gadgets, for example, cell phones, are significantly more powerless than servers regarding security assurance [20]. In this way, the helplessness in private key insurance may effectively prompt the presentation of keys to unapproved clients [30], [5] - [29], [36]. The encrypted data is keep to the cloud and protect the files from hacking by attackers and provide more security and authentication to the system.

4. PROPOSED SYSTEM

A novel synergistic key administration convention in ciphertext arrangement trait model is used, improve protection of data and enhance the security for the system model, productivity over pivotal administration of data information model. Fundamental commitments have compressed to takes after: The model communitarian convention are displayed. The data owner can create or upload the file in the system. While uploading the file, the data is encrypted. The encrypted file are kept on cloud server. If the owner wants data, the file is decrypted and the data owner can access the file. In this manner, the protection of pivotal administration are ensured including some additional external foundation. If the client accesses the data from the data owner he / she send a request for the acquire file to the owner. Owner immediately sends three keys i.e. private key, master key, secret key to the client. If clients gets the keys then, the client can access the file also data owner sends a time limit to the client. Within the time limit the client, acquire data from the data owner. If time limit exceeds then again the client sends a request to the data owner. A one of a kind trait assemble key is distributed to each quality gathering that contains customers who share a similar trait. Through refreshing trait bunch pivotal, quick quality denials are given. Demonstrate the key escrow issue as well as key introduction is undermining the classification of personal pivotal, that are not really seen past system model. Contrasted with past key administration conventions for quality based information sharing framework, the convention adequately makes twice issues over the community pivotal administration. Thus, provides more security and protection of files to the whole system. Provides the privacy of the data or files and also provides a key update function to the model.

4.1 System Framework

In the system framework mainly consist of 5 components are engaged with information splitting. One of the main component is the Data Owner. An information proprietor are approved client through framework whose informations are created and uploaded. DOs define their own particular express entry approaches with the goal that lone alluring CLs are allowed authorization to acquire plaintext. Another main component is the Key Authority. The pivotal specialists are crucial segment to framework. Key Authority are in charge of more ascertaining undertakings, especially pivotal age, pivotal refresh, and so on and accept that the KA is semi-confided in the framework, which means i.e. interested regarding estimation through ordinary information however have the goal of altering off. Another important component is the Cloud Server. In the cs, complete information or files can be stored to cs also encrypted file are kept over cs. Another main component is the Decryption Server, an unscrambling system of data have effective registering abilities. It attempts and confines the more data, however completely inadequate all errand unscrambling. Decryption Server gets the network be unreliable, on the grounds i.e. adequate to ensure information security. Finally an important component is the Client, customer i.e. a client whose means of getting the information through distributed network store through system gadgets. The client is collected the data / information through the owner. With the permission of the owner, client can access the data or information. A chance of getting the CL's property set fulfills an entrance approach related to the complex information, client should permitted the data, acquire procure ordinary information and get the decrypted data to the client.

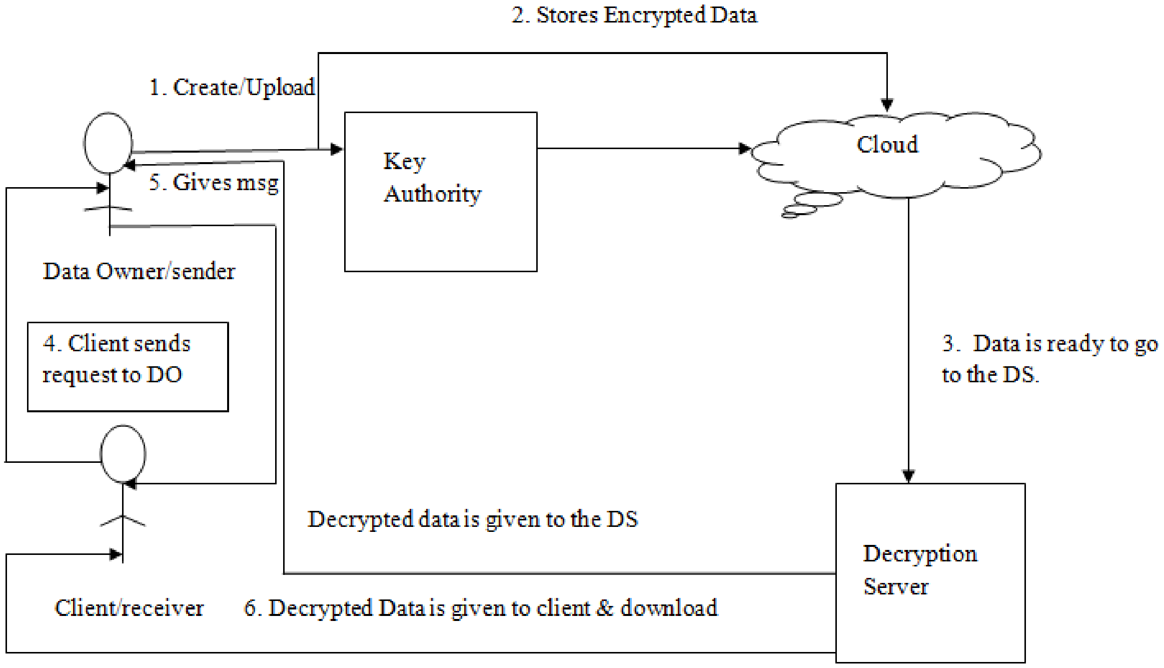
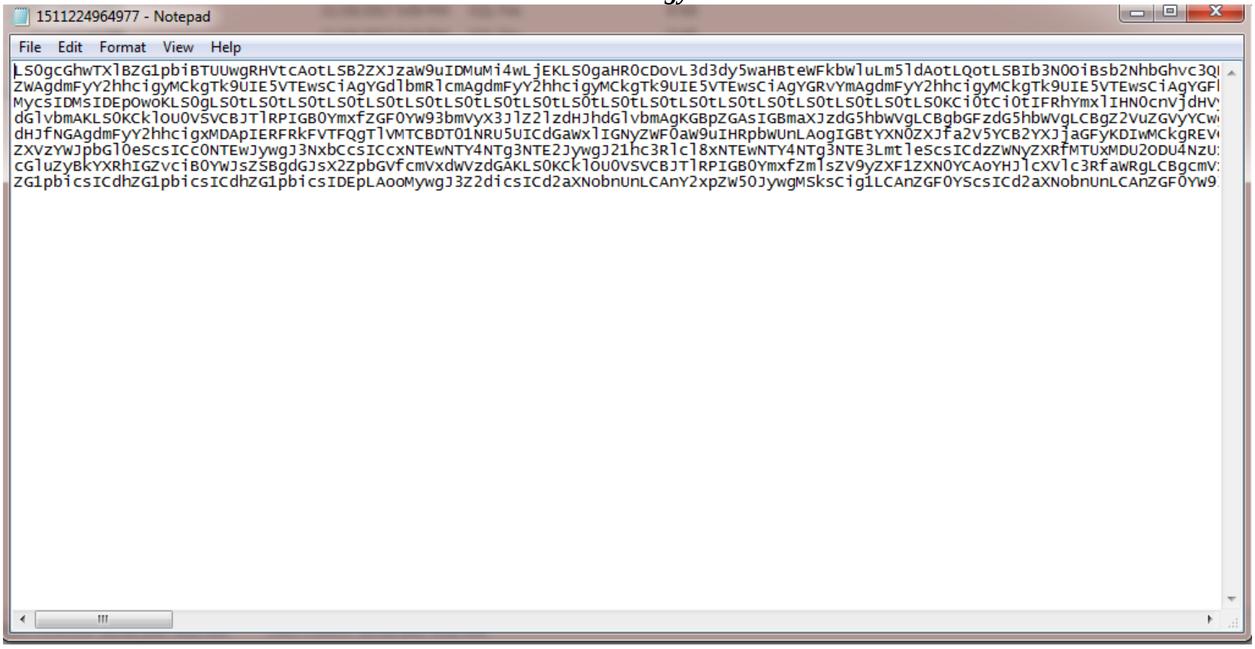
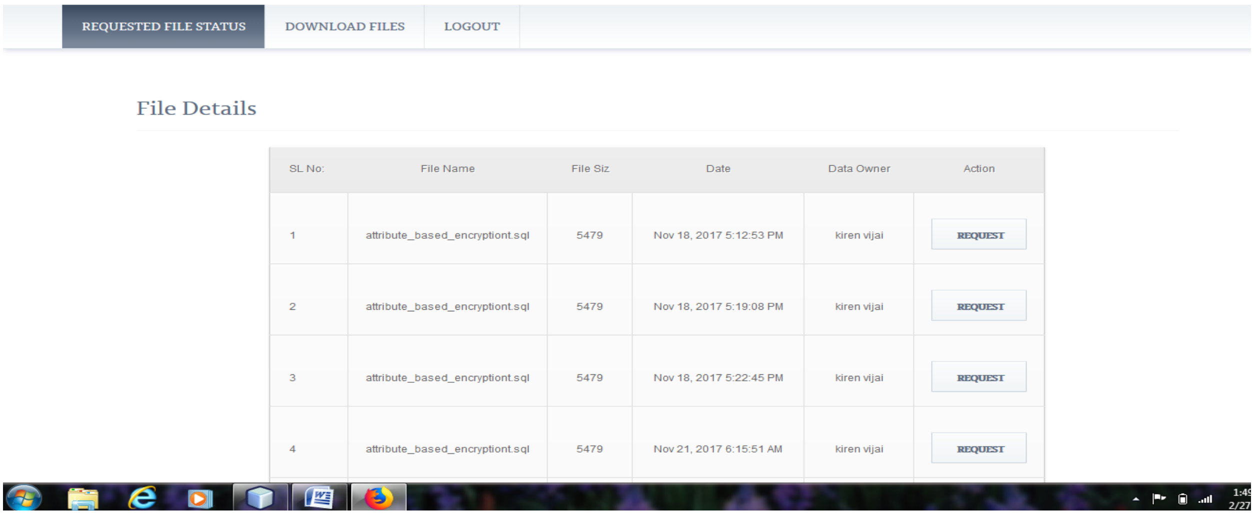

2. Stores Encrypted Data
1. Create/Upload
Key Authority
Cloud
5. Gives msg
Data Owner/sender
4. Client sends request to DO
3. Data is ready to go to the DS.
Decrypted data is given to the DS
Decryption Server
Client/receiver
6. Decrypted Data is given to client & download

Fig 1. Cipher Text Encryption Model



```
LS0gcGhwTXlBZG1pbiBTUUwgRHVtcAotLSB2ZXJzaW9uIDMuMi4wLjEKLS0gaHR0cDovL3d3dy5waHBteWFkbWluLm5ldAotLQotLSBIb3N0OiBsb2NhbGhvc3Q
ZWAgdmFyY2hhcigyMCkgTk9UIE5VTEwsCiAgYGdlbmRlcmAgdmFyY2hhcigyMCkgTk9UIE5VTEwsCiAgYGRvYmAgdmFyY2hhcigyMCkgTk9UIE5VTEwsCiAgYGF
MycsIDMsIDEpOwoKLS0gLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0KCi0tCi0tIFRhYmxlIHN0cnVjdHV
dGlvbmAKLS0KCklOU0VSVCBJTlRPIGB0YmxfZGF0YW93bmVyX3JlZ2lzdHJhdGlvbmAgKGBpZGAsIGBmaXJzdG5hbWVgLCBgbGFzdG5hbWVgLCBgZ2VuZGVyYCw
dHJfNGAgdmFyY2hhcigxMDApIERFRkFVTFQgTlVMTCBDT01NRU5UICdGaWxlIGNyZWF0aW9uIHRpbWUnLAogIGBtYXN0ZXJfa2V5YCB2YXJjaGFyKDIwMCkgREV
ZXVzYWJpbGl0eScsICc0NTEwJywgJ3NxbCcsICcxNTEwNTY4NTg3NTE2JywgJ21hc3Rlcl8xNTEwNTY4NTg3NTE3LmtleScsICdzZWNyZXRfMTUxMDU2ODU4NzU
cGluZyBkYXRhIGZvciB0YWJsZSBgdGJsX2ZpbGVfcmVxdWVzdGAKLS0KCklOU0VSVCBJTlRPIGB0YmxfZmlsZV9yZXF1ZXN0YCAoYHJlcXVlc3RfaWRgLCBgcmV
ZG1pbicsICdhZG1pbicsICdhZG1pbicsIDEpLAooMywgJ3Z2dicsICd2aXNobnUnLCAnY2xpZW50JywgMSksCig1LCAnZGF0YScsICd2aXNobnUnLCAnZGF0YW9
```

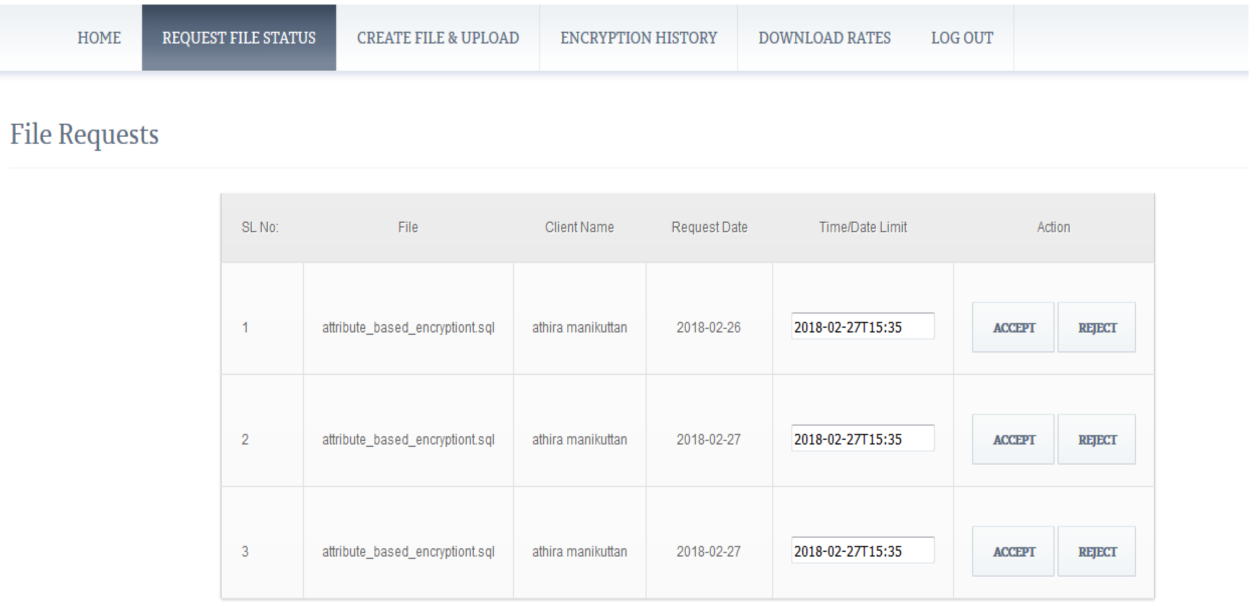
Fig 2. Encrypted File



File Details

SL No:	File Name	File Siz	Date	Data Owner	Action
1	attribute_based_encryptiont.sql	5479	Nov 18, 2017 5:12:53 PM	kiren vijai	REQUEST
2	attribute_based_encryptiont.sql	5479	Nov 18, 2017 5:19:08 PM	kiren vijai	REQUEST
3	attribute_based_encryptiont.sql	5479	Nov 18, 2017 5:22:45 PM	kiren vijai	REQUEST
4	attribute_based_encryptiont.sql	5479	Nov 21, 2017 6:15:51 AM	kiren vijai	REQUEST

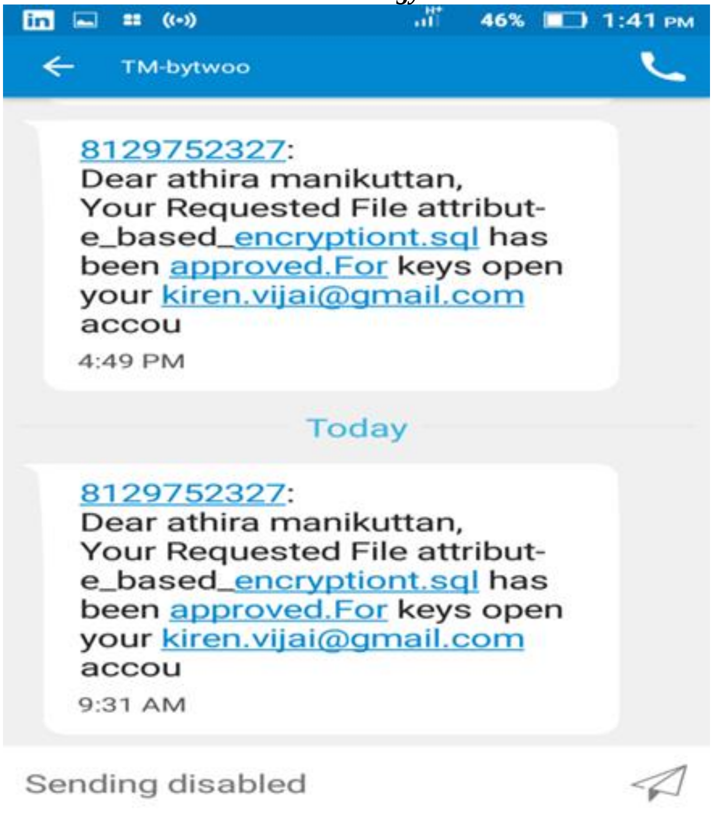
Fig 3. Client Sends a Request to Data Owner



File Requests

SL No:	File	Client Name	Request Date	Time/Date Limit	Action
1	attribute_based_encryptiont.sql	athira manikuttan	2018-02-26	2018-02-27T15:35	ACCEPT REJECT
2	attribute_based_encryptiont.sql	athira manikuttan	2018-02-27	2018-02-27T15:35	ACCEPT REJECT
3	attribute_based_encryptiont.sql	athira manikuttan	2018-02-27	2018-02-27T15:35	ACCEPT REJECT

Fig 4. Data Owner Accept or Reject the Requested File

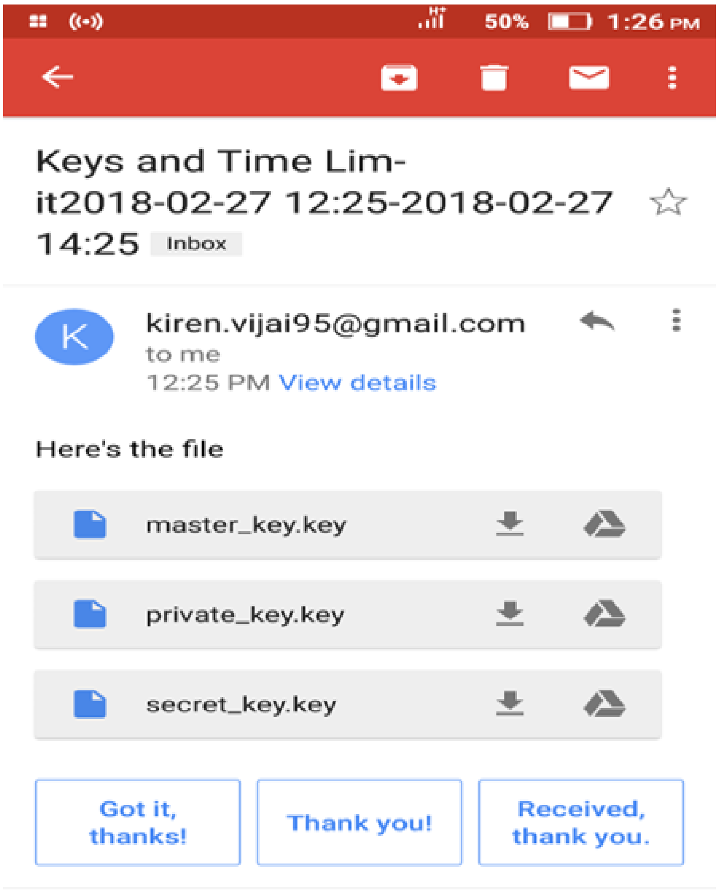


8129752327:
Dear athira manikuttan,
Your Requested File attribute_based_encryptiont.sql has been approved.For keys open your kiren.vijai@gmail.com accou
4:49 PM

Today

8129752327:
Dear athira manikuttan,
Your Requested File attribute_based_encryptiont.sql has been approved.For keys open your kiren.vijai@gmail.com accou
9:31 AM

Fig 5. Approved Message is Send to Client



Keys and Time Limit2018-02-27 12:25-2018-02-27 14:25 Inbox

kiren.vijai95@gmail.com
to me
12:25 PM View details

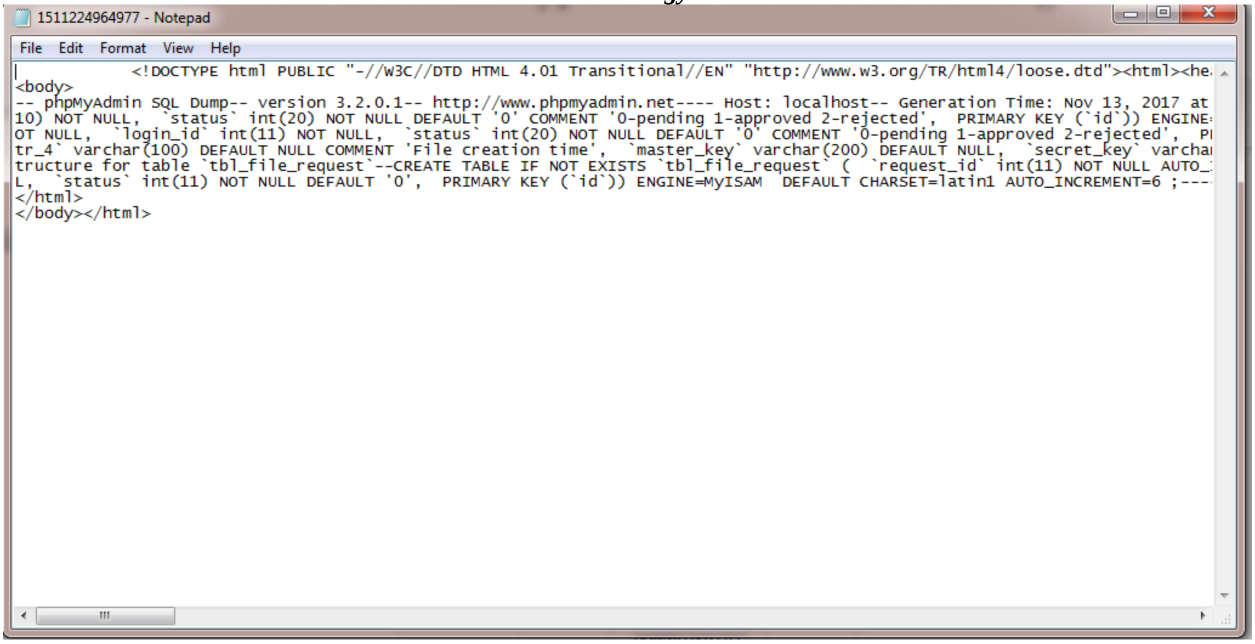
Here's the file

master_key.key

private_key.key

secret_key.key

Fig 6. Also send the keys and time limit to client's mail id by the data owner and an alert is also send to the client's Smartphone



```
|           <!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"><html><he
<body>
-- phpMyAdmin SQL Dump-- version 3.2.0.1-- http://www.phpmyadmin.net---- Host: localhost-- Generation Time: Nov 13, 2017 at
10) NOT NULL,  `status` int(20) NOT NULL DEFAULT '0' COMMENT '0-pending 1-approved 2-rejected',  PRIMARY KEY (`id`)) ENGINE
OT NULL,  `login_id` int(11) NOT NULL,  `status` int(20) NOT NULL DEFAULT '0' COMMENT '0-pending 1-approved 2-rejected',  PI
tr_4` varchar(100) DEFAULT NULL COMMENT 'File creation time',  `master_key` varchar(200) DEFAULT NULL,  `secret_key` varchai
tructure for table `tbl_file_request`--CREATE TABLE IF NOT EXISTS `tbl_file_request` (  `request_id` int(11) NOT NULL AUTO_
L,  `status` int(11) NOT NULL DEFAULT '0',  PRIMARY KEY (`id`)) ENGINE=MyISAM  DEFAULT CHARSET=latin1 AUTO_INCREMENT=6 ;---
</html>
</body></html>
```

Fig 7. Decrypted File

In the model shows, fig 1, firstly the data owner can create or uploaded the data, information or file. Through the Key authority, provides the key to the owner of the system. The sender uploaded a file and encrypted file is kept over cloud fig 2. Whenever the sender wants data, at that time, owner decrypts the data through the decrypted server. Decrypted data can access by the data owner. If receiver acquires the information. The receiver should send a request to data owner Fig 3 and the data owner can accept or reject the request Fig 4. The approved message is sent to the client's smartphone Fig 5.Sender approves the request fig 5, the sender sends a message to the client and also given a time limit to access the file. The time limit is also sent to the client mail id fig 6. Within the time limit, client should access the file. The decrypted file can be accessed by the client Fig 7. After the time limit client can't access the file. Also, the client sends a re-request to the data owner to again access the file.

4.2 Implementation

4.2.1 Base64 Algorithm

- Convert the txt into 8 bit.
- Combine them and Convert them into 6 bit.
- Finally, get the corresponding ASCII string.

4.2.2 RSA Algorithm

- Take two numbers of prime let it be A and B
- Let n be the public key, n= A*B.
- Given a small exponent be e, must be an integer also not be a factor of n.
- $1 < e < \varphi (n)$, n and e are the public key
- Calculate $\varphi (n)$, such that $\varphi (n) = (A-1) (B-1)$
- Calculate greatest common divisor (e, (A-1))
- Calculate greatest common divisor (e, (B-1))
- Calculate greatest common divisor (e, φ (n))
- Calculate ed mod φ (n) =1
- Calculate c = m ^ e mod n, for encryption.
- Calculate m = c ^ d mod n, for decryption.

5. CONCLUSION

Ciphertext arrangement quality systems use the information is mainly kept on the cloud. It is one of the efficient and security provided to the system to avoid attacks from the attackers. An innovative community pivotal administration convention for upgrade the authentication and effectiveness of pivotal administration in figure content approach property based encryption for cloud information sharing framework. Dispersed key age, problems off, capacity over personal pivotal to lack of acknowledgment including the additional visible framework. The acquaint characteristic gatherings with construct the personal pivotal to compute the gathering information and data repudiation to the system to provide more authentication and security to the framework. The proposed collective instrument superbly addresses key escrow issue as well as a more terrible issue called key presentation that past research scarcely took note. In the interim it advances customers client encounter since just a little measure of obligation to makes unscrambling. Hence, information is stored in the cloud framework helping enormous execution limited front-end gadgets concerning over more authentication and also protects the owner's privacy and provide more security. The keys are always updating each time. Thus provide more security to the data owner and also provide authentication. Now expand the preparatory discoveries to build up information plot by diminishing the complex information measure, encode rate, decoding rate, thus as yet unenclosed issues i.e. impede down to earth utilization of trait information sharing. Thinking of some as particular mechanical situations, for example, individual wellbeing record gets to control, plus, the expressiveness of access strategy needs improvement too.

6. REFERENCES

[1] A. Sahai and B. Waters, “Fuzzy identity-based encryption," in Proc. Euro Crypt, 2005, pp. 457_473.
[2] J. Bethencourt, A. Sahai, and B.Waters, “Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Secur. Privacy, May 2007, pp. 321_334.
[3] N. Attrapadung and H. Imai, “Conjunctive broadcast and attribute- based encryption," in Proc. Int. Conf. Pairing-Based Cryptogr., 2009, pp. 248_265.
[4] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Public Key Cryptogr., 2011, pp. 53_70.
[5] M. Green, S. Hohenberger, and B.Waters, “Outsourcing the decryption of ABE ciphertexts," in Proc. USENIX Secur. Symp., 2011, p. 34.
[6] J. Lai, R. H. Deng, C. Guan, and J.Weng, “Attribute-based encryption with veriable outsourced decryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1343_1354, Aug. 2013.
[7] S. Lin, R. Zhang, H. Ma, and M.Wang, “Revisiting attribute-based encryption with veriable outsourced decryption," IEEE Trans. Inf. Forensics Security, vol. 10, no. 10, pp. 2119_2130, Oct. 2015.
[8] M. Chase and S. S. M. Chow, “Improving privacy and security in multi-authority attribute-based encryption," in Proc. ACM CCS, 2009, pp. 121_130.
[9] G. Zhang, L. Liu, and Y. Liu, “An attribute-based encryption scheme secure against malicious KGC," in Proc. TRUSTCOM, Jun. 2012, pp. 1376_1380.
[10] J. Hur, “Improving security and efficiency in attribute-based data sharing,"IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2271_2282, Oct. 2013.
[11] P. P. Chandar, D. Mutkuraman, and M. Rathinrai, “Hierarchical attribute based proxy re-encryption access control in cloud computing," in Proc. ICCPCT, Mar. 2014, pp. 1565_1570.
[12] X. A. Wang, J. Ma, and F. Xhafa, “Outsourcing decryption of attribute based encryption with energy efficiency," in Proc. 3PGCIC, Nov. 2015, pp. 444_448.
[13] L. Cheung and C. Newport, “Provably secure ciphertext policy ABE," in Proc. ACM CCS, 2007, pp. 456_465.
[14] J. Hur and D. K. Noh, “Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, pp. 1214_1221, Jul. 2011.
[15] M. Pirretti, P. Traynor, P. McDaniel, and B.Waters, “Secure attribute-based systems," in Proc. ACM CCS, 2006, pp. 99_112.
[16] A. Boldyreva, V. Goyal, and V. Kumar, ``Identity-based encryption with efficient revocation," in Proc. ACM CCS, 2008, pp. 417_426.
[17] A.-P. Xiong, C.-X. Xu, and Q.-X. Gan, “A CP-ABE scheme with system attributes revocation in cloud storage," in Proc. ICCWAMIP, Dec. 2014, pp. 331_335.
[18] W. Qiuxin, “A generic construction of ciphertext-policy attribute-based encryption supporting attribute revocation," China Commun., vol. 11, no. 13, pp. 93_100, 2014.
[19] S. S. M. Chow, “Removing escrow from identity-based encryption," in Proc. Int. Conf. Pract. Theory Public Key Cryptogr., 2009, pp. 256_276.
[20] M. S. Ahmad, N. E. Musa, R. Nadarajah, R. Hassan, and N. E. Othman, “Comparison between Android and iOS operating system in terms of security," in Proc. CITA, Jul. 2013, pp. 1_4.
[21] V. Goyal, O. Pandey, A. Sahai, and B.Waters, “Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM CCS, 2006, pp. 89_98.
[22] S. Rafaeli and D. Hutchison, “A survey of key management for secure group communication," ACM Comput. Surv., vol. 35, no. 3, pp. 309_329, Sep. 2003.
[23] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1_11, 2011.
[24] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, “A survey of mobile cloud computing: Architecture, applications, and approaches," Wireless Commun. Mobile Comput., vol. 13, no. 18, pp. 1587_1611, Dec. 2013.
[25] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, ``Security and privacy challenges in cloud computing environments," IEEE Security Privacy, vol. 8, no. 6, pp. 24_31, Nov./Dec. 2010.
[26] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362_375, Feb. 2013.
[27] 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 Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131_143, Jan. 2013.
[28] Q. Liu, G. Wang, and J. Wu, “Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," Inf. Sci., vol. 258, pp. 355_370, Feb. 2014.
[29] X. Yao, Z. Chen, and Y. Tian, “A lightweight attribute-based encryption scheme for the Internet of Things," Future Generat. Comput. Syst., vol. 49, pp. 104_112, Aug. 2015.
[30] H. Hong and Z. Sun, “High efficient key-insulated attribute based encryption scheme without bilinear pairing operations," SpringerPlus, vol. 5, no. 1, p. 131, Feb. 2016.

[31] M. R. Rahimi, J. Ren, C. H. Liu, A. V. Vasilakos, and N. Venkatasubramanian, “Mobile cloud computing: A survey, state of art and future directions," Mobile Netw. Appl., vol. 19, no. 2, pp. 133_143, Apr. 2014.
[32] D. Pletea, S. Sedghi, M. Veeningen, and M. Petkovic, “Secure distributed key generation in attribute based encryption systems," in Proc. ICITST, Dec. 2015, pp. 103_107.
[33] X. Xu, J. Zhou, X. Wang, and Y. Zhang, “Multi-authority proxy re encryption based on CPABE for cloud storage systems," J. Syst. Eng. Electron., vol. 27, no. 1, pp. 211_223, Feb. 2016.
[34] S. Easwarmoorthy, S. F, and A. Karrothu, “An efficient key management infrastructure for personal health records in cloud," in Proc. WiSPNET, Mar. 2016, pp. 1651_1657.
[35] N. Oualha and K. T. Nguyen, “Lightweight attribute-based encryption for the Internet of Things," in Proc. ICCCN, Aug. 2016, pp. 1_6.
[36] Guofeng Lin,Hanshu Hong and Zhixin Sun, “A Collaborative key management protocol in Ciphertext policy attribute-based encryption for cloud data sharing”, May 2017.