RESEARCHERID
THOMSON REUTERS

[Selvakumar, 5(8): August 2018]
DOI- 10.5281/zenodo.1407448

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

PRIME FACTOR ENCRYPTION SECURITY FRAMEWORK FOR ENSURING OUTSOURCED DATA PROTECTION IN SECURED CLOUD STORAGE

K. Selvakumar*[1] & Dr. M. Prabakaran[2]

*[1]Research Scholar of Bharathidasan University, Department of Computer Science, Government Arts College, Ariyalur, Tamil Nadu, India.

[2]Research Supervisor, Asst. Professor, Department of Computer Science, Government Arts College, Ariyalur, Tamil Nadu, India

ABSTRACT

Cloud computing provides a secure data management to provide various services to the clients for improving the data security. The cloud platform offers a scalable service in cloud computing in service orientation. Mostly the protection against the file in centralized storage is more problematic because of data leakage, cryptography security concerns, key leakages forums in authentication also mitigated. The advancement need for effective utilization of cloud service needs more securable cryptography policy for data storage and access. The outsourced data contains sensitive and privacy statements of personal information that are stored and organized by cloud service provider in the centralized cloud. The implementation overcome attained issues, we propose a prime factor encryption security(PFES) and shuffle random block key (SBRK) cryptographic method is used to improve the data security. Both the techniques ensure the data integrity in secured data storage with auditing confidentially. The proposed way concentrated encryption strategy on multi-factor authentication before the data owner gives access rights to the authenticated user. This improves the crypto invention against unauthorized access to provide high security.

Keywords: *security, cloud storage, encryption and decryption, cloud service, auditing. Data authentication.*

I. INTRODUCTION

Cloud computing was having the number of advantages, yet the most associations are concerned for tolerating it because of security issues and difficulties having with a cloud. Security prerequisites required at the endeavor level powers to configuration models that fathoms the authoritative and conveyed parts of data use. In information security processing the cloud servers be outsourcing the data at verifiable cloud server. The auditing purpose enhance the world wide security issues in many security challenges against the privacy. Attained security of auditing service to check the information uprightness in the cloud. Some current remote respectability checking strategies can serve for static file information and, subsequently, can't be connected to the auditing service since the data in the cloud can be powerfully refreshed. In this way, practical and secure unique auditing provided to the user by checking the integrity of the cloud service provider. To integrate a cloud verifiable out sourcing Clair policy to verify the integrity of data from the right authentication requestors a practical and protection saving auditing convention. At that point, the encryption challenges have the conventions of privacy to help the dynamic information tasks, and this produces a high-security mechanism to integrate the auditing that is shown in figure 1. Analyzing security furthermore extend our auditing tradition to help group auditing for both distinctive proprietors and different clouds, without using any trusted in the organizer. The examination and reenactment results exhibit that implementation auditing traditions are secure and valuable. Prominently, it reduces the figuring expense of the analyst.

ISSN 2348 – 8034
Impact Factor- 5.070

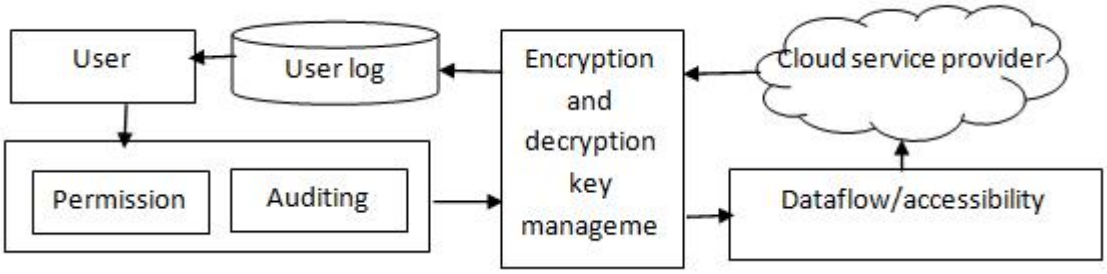


Figure 1 secured cloud storage crypto policy

Trust Evaluation systems to some degree, helps in building up the connection between cloud shoppers and service suppliers rapidly and securely. As trust is a social issue, not merely a specific issue it is hard to assess and oversee the assurance viably. The security policy regrets privacy to get a handle on the significance of confidence in the cloud and how connections are settled amongst shopper and supplier. In this paper, a trusted display is exhibited which can be embraced by any outsider to prescribe a service supplier to the client as per his prerequisites. The instrument for trust assessment thinks about inputs from clients and outsider to assess the trustworthiness of service suppliers. Be that as it may, the productivity of their plan stays hazy. Even though the current proposals go for giving respectability confirmation to various information storage frameworks, the issue of supporting both open auditability and information progression has not been wholly tended to risks. The most effective method to accomplish a protected and productive plan to coordinate these two essential parts for information storage service flawlessly remains an open testing assignment in Cloud Computing.

II. LITERATURE SURVEY

As grown new technology in data security in equal way to abuse privacy resources in outside the security of evaluations. The main disadvantage is not verifiable log cloud storage, owner ship, key leaked and soon [1]. That security is one of the traditional policy to secure central issues of cloud figuring. Numerous security arrangements have been proposed, be that as it may, a significant portion of them just concentration one phase of information lifecycle, for example, stockpiling stage [2], which isn't sufficient to tackle cloud information security issue as dangers exist in the entire information lifecycle. In this paper, we contend that the cloud information security issue ought to be understood shape information lifecycle. Openly auditable cloud data accumulating can help this creating cloud economy end up being at last settled. With open audit ability [3], a trusted in substance with capacity and limits data proprietors don't can be appointed as an outside survey gathering to assess the peril of outsourced data when required. Such a looking into organization not simply helps save data proprietors. The CTrust structure that watches out for the security opening in cloud enrolling by solidifying the power of virtualization advancement [4] with the arrangement of secure processor models.

The worldview likewise attain risk for the requesters and verifiers. Individually, there are various privacy security issues arise in data storage including encryption losses [5], suppose the encrypted data be unapproved get to, loss of security, information replication and administrative infringement that necessitate adequate consideration. Security beyond to access the provable resource encryptionis a method for guaranteeing the trustworthiness of information away outsourcing [6]. Crypto policy address the growth security in an active encryption issues for dispersed centralized cloud storage to help the information theft in administration rights to control the secured data [7]. Cloud stockpiling supplier asserts that they can ensure the information, yet nobody trusts security. In this privacy resembles a structure to guarantee information are privacy in centralized cloud storing framework.

The TPA integrates the customer request through the information accesses from the cloud server. This is discriminated by accessing the resource scale of cloud privacy by unsecured way of access [8]. This factor intent a cloud service choosing preference to differentiate the security policy but time complexity arrives to access this information also easy to decrypt [9]. By utilizing bunch signature and dynamic communicate access by crypto

encryption standard procedures. A trust assessment show is introduced that can be taken as a construct to set up trust in light of specialist co-ops [10]. This model prescribes a specialist co-op to the client as per his prerequisites.

To formalize the security of evaluating security privacy in cryptographic technique with key security policy for evaluating strength and develop new security on policy with an agreement [11].In the proposed plan, the parallel tree structure and the pre-arrange traversal system is utilized to refresh the mystery keys of the customer. Cloud administration constrained the file security and information in encryption standard with differential key sizes. The remote authentication doesn't provide enhanced security to frequent access. So termination of requester have the problem to deal the approach also retains to need additional auditing purpose [12]. Along these lines, some multi-control technique's resembles the originality file from encrypted storage, in which different powers autonomously holds the key characteristic with derived intruders [13]. Regardless, the cipher policy introduce the attribute scheme for basis retain with storage service security. Disseminated stockpiling. Sharing of EHRs has unique advantages is most used resources [14], given that such records contain parcel of touchy data, secure sharing of EHRs is of foremost significance. Difficult to access the time series real data straightforwardly by attribute encryption standard plans to information get to access control in storage stockpiling frameworks due to the attribute repudiation problem [15]. This outline meaningful, productive and revocable information get to control plot for multi-authority cloud storing contexts.

The need of utilizing Cloud administrations from numerous Clouds with different quality attributes and evaluating models has been raised as of late [16]. Even though the administration portion in light of Service Level Agreement a safe appropriated document framework which can be layered straightforwardly on existing open cloud stockpiling infrastructure [17]. Multi-cloud offers the attribute key revocation problem of sign entry are verified by attribute based encryption policy by every request this may leads authentication problem[18, 19]. By and massive proposed the entrance control convention in light of the owner authentication be utilized characteristics to scramble the message, and decode the signal through approved accreditation focus [20], to give a multi-authority privacy needs resembles the fine grained access control leads the review problem**.**

III. IMPLEMENTATION OF THE PROPOSED SYSTEM

Security in cloud registering is a standout amongst the most basic angles because of the significance and affectability of information put away in the cloud. There are different security issues come up in a cloud. A portion of the security issues and their answers of them are depicted underneath. Because of offering registering assets to another organization physical security is lost. The user does not have information and control of where the assets run and put away.

In this work, we utilized prime factor calculation for encryption and unscrambling of information, and part based access control display is used to give access as indicated by the pretended by the client. This paper additionally demonstrates the numerical model for figuring the trust of the client. This model provides the transferring rights to the client when he/she prescribed by the Administrator and Owner when clients surpass the predefined experience and trust limit esteem. Another significant issue is the manner by which to oversee client access to cloud stockpiling framework. For that different access control system can be implemented for cloud clients. Access Control is only giving the expert to clients to get to the particular assets, applications, and framework.

ISSN 2348 – 8034
Impact Factor- 5.070

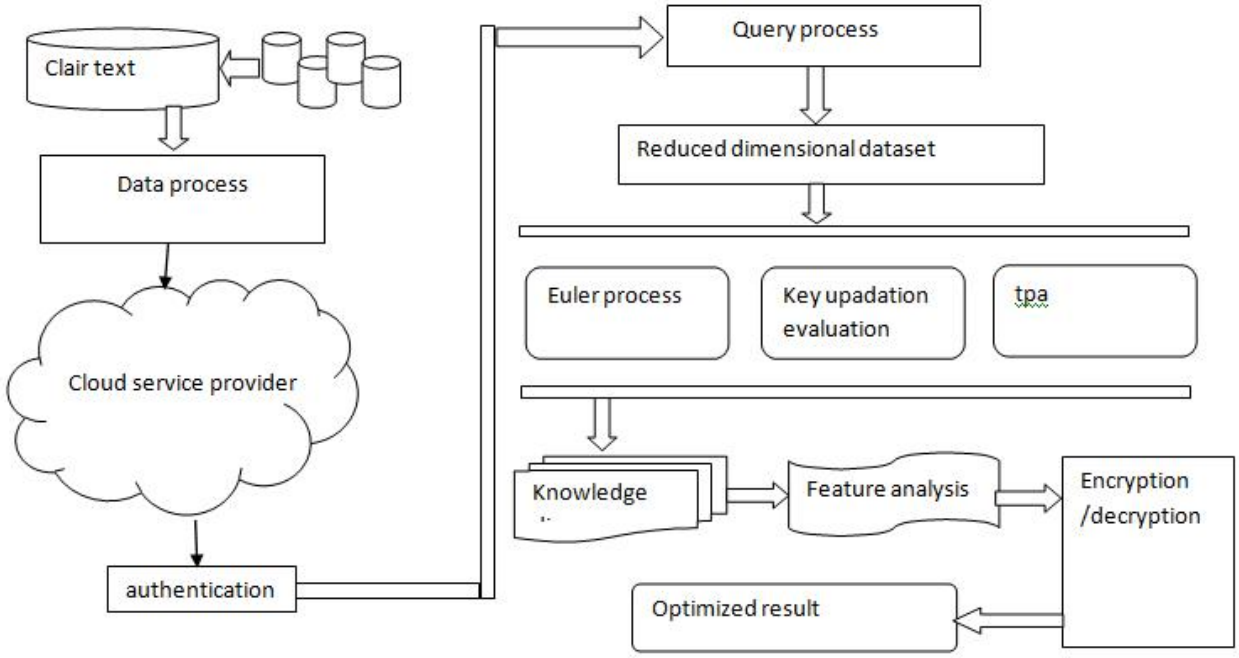


Figure 2 Architecture for the proposed system

The security performance enhance the performance data storage and critical risks are arise by access control in various online resources. The cipher policy standards to provide the encryption with prime factor exponential evaluation in multi authority privacy concerns like TPA, public and private key auditing. The attribute based security maintains the privacy standard in cloud storage depends authenticity cloud management.

A) Privacy concerns in secured auditing in cloud storage.

Due to the security in data storage, the crypto policy enhance the auditing information to the privacy assets. The security resources are auditing to resemble the clients data that are structured with logs entry encryption. Privacy is differed from others that are virtually verified through cloud auditability. By generating the key to protect the data accessibly from centralized storage have the right assurance. The cloud register have specific id to access the cloud storage by authenticated persons. By the right concerns the data verification is auditability by the client access who have specific intention to confirm the data privacy.

Be aware the empowering logs to verify the cloud storage through auditing is the primary concern. The client resource be secured to encryption standard policy by the out reviewer directly to outsourcing the storage content by CSP. To create a security with supportive auditing TPA procedure to protect the client information. The vulnerabilities are unwanted access y accessing through online creative issues. The safeguard providence has the impact of ordinary fact provided by the content service provider (CSP). In addition the key enhance the security conformation in data security logs. The storage resembles the owner permission with outsourcing auditability provided to the clients who want to access this data. The encrypted data be safe on broad security against the intruders does not access the cloud storage centrally.

B) Problematic issues and identification factors

Most cases the security failed in key leakage problems addressed by the authorized rights to access permission. The comprehended issues created by attackers to access the key to decrypt the data against auditing resource. At this time of evacuation the auditing resource failed to resigns the crypto policy which can accessed by the attribute relevance case by encrypt and decrypt policy. The more over system automaticity creates the problem of service acceptance against the auditing security.

C) Contributions

To implement a new intent security system called prime factor crypto policy which is for privacy concerns in secured data storage in cloud environment. To develop the prime content encryption for standard updating to enrich the auditing source of requestor which they want to access rights. This implements the exponential for of key validation with verifiable out sourcing auditing. The proposed system envelops the key intent security of server side validation from cloud content provider. This make effort against privacy to deal key leakage problems met to unwanted access block contents. The auditing resource make end to end encryption at the point of private and public auditing with maintained least complexity to provide best security services.

3.1 Prime factor security based encryption

The prime factor encryption ensures the security using numerical exponent value based on Euler intent values. The data security provides the first-factor security verification for encrypting the data with a specified public key. The cryptography access the public and private keys to generate through prime numbers .with support of exponentiation the key is derived from original data and secure to store in cloud service. By using the authentication required by the cloud provider to verify the data from the content service provider to enhance the security. The prime factors improve the critical leakage integrity problems in authorized defenders to use the multiplicative shuffling factor to verify the confidentiality.

Initially, the security begins to create the security log through important validation which is for encryption and decryption was done on the fact. All the verification logs are carried out by the TPA auditing and content service provider.

Input: prime numbers, original data.
Output: security log key and encrypted data
Step 1. Initialize the prime numbers are distinctive p(a) and p(b).
For each p(a) and p(b)
Generate random ran→p(a,b)
R→ran c integrates R(a) and R(b)
Step 2: Compute the prime factor multiplicative R(a,b)
Pf(R→p(a)*p(b))
Step 3. Compute the exponential factor of prime indication p(e)
By the probability of ran function p(n)→ Ø(n) = (p(a)-1) * p(b)-1).
Step 4. for each exponent value by Euler rule →p(e)
p(e), resultant of integer value 1 < e < Ø(n)
Divisor of p(e), Ø(n) is even 1 of factor.
P(n)→e is the exponential public key prime factor.
End for
Step 5 Determinative factor d=p(e)-1 by the multiplicative factor 1 (mod Ø(m))
Compute random point r(d) as private prime factor
The multiplicative R(d) *p(e)= 1 mod Ø(m).
Step 6 compute reversible of p(m,n)to padding the new enc bit t.
For each Compute the cipher policy Clair text p(c)→m^e(mod n)
P(c)→P(m,n)
End
Step 7 return P(c)

The above algorithm encrypts the data with supportive random prime factor generation which encrypts the data securely to defend with the key. The encryption remains the public and private key with a service-oriented platform attains the privacy level in content service provider.

3.2 Cloud updating prime content

The cloud performs the storage process with the downstate policy of important security tostore in CSP owner authentication logs. The encrypted data is appended with logs contains the secured key. To transmitting the

communicational request and response, the registered logs of data are updated to the owner has given rights to access. Otherwise, CSP manages the data centralized to right authentication from the corresponding user. Using this key, the data can encrypt and decrypt based on the authentication.
Algorithm:
Input: Clair text Ct, private key P(pk), public key P(c)
Output: centralized storage log.
Step1: Start
Step2: To initialize the user log in CSP
Step3: Verify the general registration in states in account open.
Step4: update eccentric data to the cloud account
Step5: While Ct, corresponding record R(c)
Receive key logs P(k) and P(c)
Update the key whenever modified;
Update Clair text c.
Return →C=p(k), p(c)
End
Step6: Stop

The above algorithm specifies the attention of key logs with the corresponding owner account in centralized cloud storage. The corresponding data which have the originality of key has the right authentication to access the data.

3.3Shuffle block random key generation
The key generation is performed using the polynomial algorithm, and the generated key will be given to the user. The original key generated is nothing but a number which specifies the location or index of the key in the key set maintained by the user and the service. Also, the key will be valid until the integer value generated by the polynomial algorithm only.

The public key cryptography attains the open security for key verification and validation for which the person has rights to access the data. In this shuffle state process which is intended to service level of public and private key logs are randomized to create a new state of the randomized key the index of each core is stored on specific logs in content service provider. The key index is updated the owner authentication and the additional security to improve the performance of data privacy in cloud storage.
Algorithm:
Input: owner log, Clair text index, public key P(c), private key P (k)
Output: Key Index K.
Step1: initialize the owner log, data tabled(t)
Step2: for each record in d(t);
Choose key log K(L)→P(k),P(c);
Shuffle S(kn)=p(k,c)→ran d(t);
Step3 For each record update d(t) update;
S(kn)← d(t);
End.
End
Step 4: Return S(n)

The above algorithm aggregate the shuffle random state which has each data d(t)by specifying the additional key to be stored for authentication.

3.4Verifiable outsourcing and auditing
The auditing performs each user based on the request and response to give the answer which has the authenticity permits to access the data. The key provided by the owner to the right person from the verifiable outsourcing auditing, the third-party auditor, verifies the cloud authentication has access rights to similar zed forms. The

verification resembles the frequent access rights or other rational access to check the key and data which they want rights. The owner provides the permission of access rights whether TPA integrates verifiable auditing purposes. For this efficiency consideration, the accessible outsourced data be strictly needed for authentication by auditing the data.

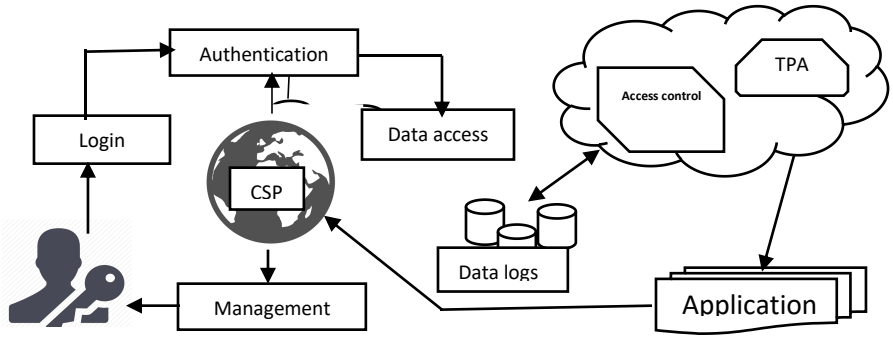


Figure 3 Structure of security access control

The above figure 3 shows the security access outsourcing client security to attain the privacy of needs the authentication given to the right user to verify the authentication of right accessible from cloud authenticated data storage. To maintain the cost quality of service having the privacy needs depends to the storage logs
TPA auditing and Request up dating.
Input: Resource log request Rt
Output: verified authentication.
Step 1 Start
Compute request log from client Ri
Step 2
Compute the request type = upload req status then
Access Retain the key from resource table Rt
Request resource →Rt = K(service log Ri→ resource log Rt)
Else if
Request is accessed to proceed
Step 3 accessible to match the key with Verify with TPA.
Step 4 originate the security file.
If True then
Step 5 Return valid authentication.
End
End
Stop.

The request accessible from the stored data by verifying log have stored in log table. If it is tempered by any issues the request is rejected. I.e. the key matches to proceed to verify the integrity. The data owner accept the request to provide the permission to the client with verifiable auditing evaluation.
Algorithm:
Input: user data UD, Outsider auditing OA
Output: Integrity check result ICR
Step 1 Begin
Get UD for Req.
Step 2 verify the request from the requestor from the cloud.
Verify the security to file storage cloud access
Step 3 computes the time of access
CS = ∑ ⟦(CSi∈\time)∪Req.Resource⟧
Receive UD

ISSN 2348 – 8034
Impact Factor- 5.070

Step 4 compute to verify the key value
Step 5 verify the integrity
If check user key = OA key.
Verify the integrity to originate the file.
Step 6 Return integrity status
End
Stop.

To verify the integrity using the security policy ant privacy identifies the key validation is considered proficient to adopt the calculating discontent from service provider, vicious information adjustment attack, and the server make auditable profile against attacks.

To confirm public auditing resource is point the storage of privacy content in cloud service provider and to intent a conventional outsourcing supporting for unique information activities, mainly to help square addition, which is absent in most existing plans. To pointing security in encrypted file by verifying key validation. Precisely, this method accomplishes to verify the originality of data from various appointed examining undertakings from multiple access can be verified by TPA auditing. To propose exponential form of security development and legitimize the execution of our plan through substantial usage and correlations with the best in class. We stretch out the way to deal with help the performance while accomplishing useful information elements. We enhance the current evidence of capacity models.

3.5 Outsourced prime factor decryption

The necessary verifications begin to selected prime factor evaluation, the value to get the cipher text of key text to identify the Clair text and resembles permission from TPA auditing. The method reverses the Clair text into original version by reducing the key substitution fact of authentication by the right policy standard of the selected key.

Input: selective file Pf→Trans
Output : .plain text
Step 1 Start
For (Pf1←encrypton)
Step 2 For each file Pf = retain auditing.
Map the point Pf from the clear text
Step 3 Get the key from verifiable access.
k = $\int Key(R) \in dec \rightarrow Pf1$
Step 4 decrypt the value and convert to a chipper.
Identify the key→Pf→fy(Clair text)
Step 5 Perform reverse decrypt.
Return plain text
Stop.

The above-discussed algorithm selects the key being used to encrypt the data from the prime factor of privacy, and the selected key is used to encrypt the data. Encrypted data is converted into a cipher whenever the auditing is verified.

IV. RESULT AND DISCUSSION

The advanced prime factor encryption is designed to improve the security by minds the fact of accuracy, time complexity on the user roles had the significant impact of security access to the cloud environment. The resultant prove the prime factor privacy of security standard which has been tested with client server role request response verifiable access control. Test case generated by configuring the Microsoft intent framework tool designed to process with SQL server database has right user access permission which to access with private and public users. The users can access with thousands of files with trust authority and prove the high impact of evaluation sectors on privacy concerns. The table is given below shows processing parameters

ISSN 2348 – 8034
Impact Factor- 5.070

.

Table 1: Details of processed parameters

Parameter	Value processed
Service provider	Cloud service provider
Data processed	File Type, Clair text
File size	25 MB,50mb,75mb nearer
Number of users	1000

Table 1 holds the parameters that are used to calculate security concerns implemented by prime factor crypto policy. The graph given below shows that the analysis of various performance tested by comparison of previous methods.

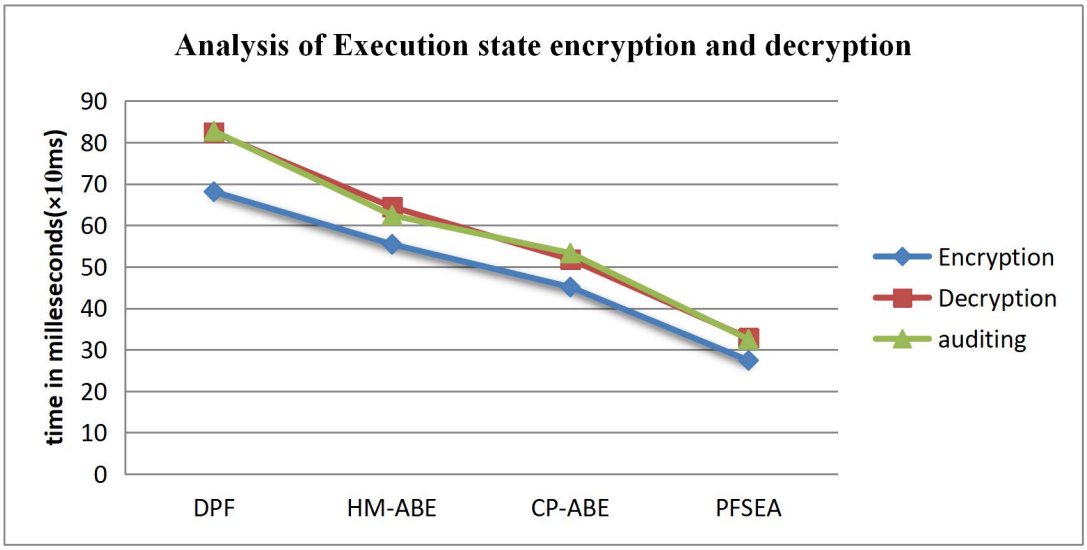


Figure 4.1: Comparison of execution efficiency

Figure 4.1, shows the efficiency of execution state processed between encryption and decryption using prime factor provides a substitution meantime 27.8 ms as well as AES cipher policy. This implementation had much-improved performance compared to previous methods.

Methods/state	Performance analysis of encryption and decryption by auditing in milliseconds			
	DPF	HM-ABE	CP-ABE	PFSEA
Encryption	68.1	55.4	45.1	27.2
Decryption	82.4	64.2	51.8	32.3
Auditing	82.7	66.4	53.4	32.7

ISSN 2348 – 8034
Impact Factor- 5.070

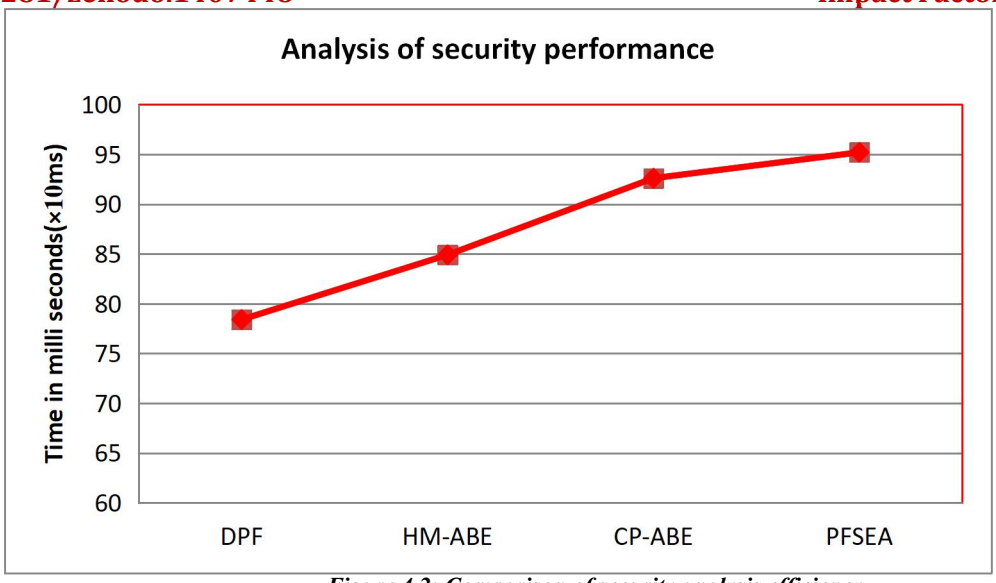
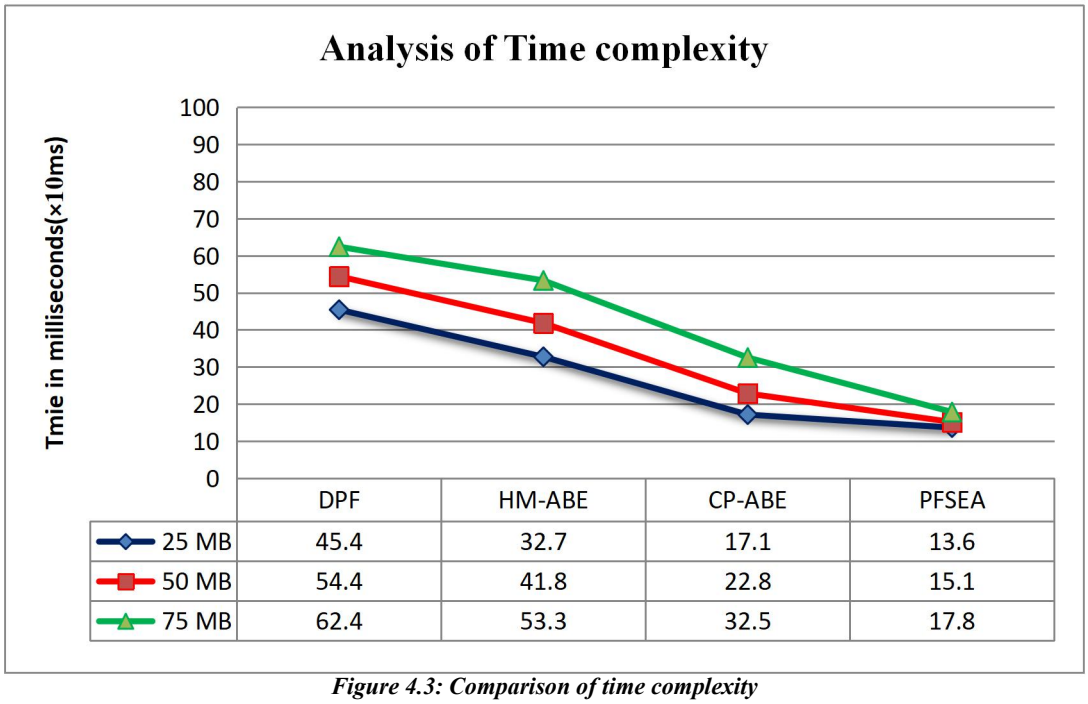


Figure 4.2: Comparison of security analysis efficiency

Security performance can be analyzed through the total number of vulnerabilities of risks carried out by a un-authenticated process that leads to file decryption by getting plain text. Figure 4.2, shows the comparative analysis of security prime factor encryption has 95.2% performance well to different methods, and this implements excellent performance with more efficiency than previous methods.

Time complexity (Ts)=$\frac{Total\ number\ of\ blocks\ per\ bits \times two\ phase\ encryption}{time\ taken\ (s)}$



	DPF	HM-ABE	CP-ABE	PFSEA
25 MB	45.4	32.7	17.1	13.6
50 MB	54.4	41.8	22.8	15.1
75 MB	62.4	53.3	32.5	17.8

Figure 4.3: Comparison of time complexity

The above Figure 4.3 shows the processing time taken executed by different state by different file size, and prime factor encryption provides the least time 17.8 ms as well as previous cipher policy. This implementation had much-improved performance compared to prior methods.

False occurrence state (FS) = $\frac{Repeated\ block\ of\ the\ cipher}{Total\ number\ of\ cipher\ block\ occurrence}$

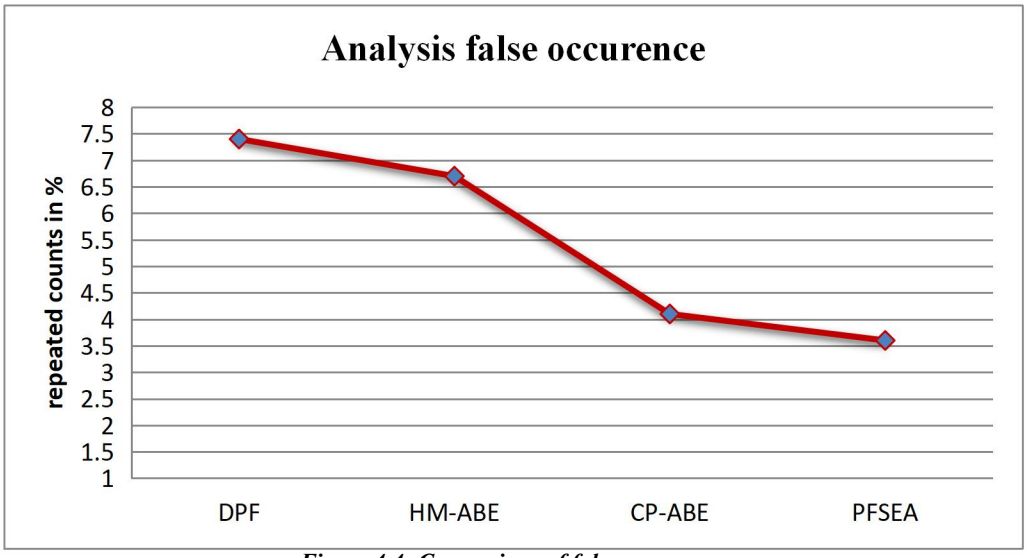


Figure 4.4: Comparison of false occurrence

The above Figure 4.4 shows the false appearance of crypto policy encryption cipher text that is compared by different methods, and it shows clearly our implementation of prime factor crypto method has produced active redundant false rate state than previous methods.

V. CONCLUSION

The prime factor crypto policy enhance the security through outsourcing auditing by given right access to the data. The TPA integrated policy are outsourced to key factor encryption to secure the data storage. the performance of exponential prime factor encryption improve the security.By implementing the prime factor hides the critical security to enhance the authentication of crypto policy whenever right needs by owner policy. Thereversing decryption authenticated by TPA auditing resembles the permission to access the data security. The proposed system of prime factor evaluates proves the security performance as 95.4% a well in lower time complexity. Also, the protection demonstrates the right authentication to the source of crypto policy in higher permission to the right of access.

REFERENCES

1. *Goyal, O. Pandey, A. Sahai, And B. Waters, Attribute-Based Encryption For Fine-grained Access Control Of Encrypted Data,‖ In Acm Conference OnComputer And Communications Security, 2006,*
2. *Xiaojun Yu; Qiaoyan Wen, "A View about Cloud Data Security fromData Life Cycle," Computational Intelligence and Software Engineering(case), 2010 International Conference on, vol., no., pp.1-4, 10-12 Dec. 2010.*
3. *C. Wang, K. Ren, W. Lou, J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services,"* IEEE Network*, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.*
4. *Satyajeet N SrujanKotikela, MahadevanGomathisankaran, "CTrust: A framework for Secure and Trustworthy application execution in Cloud computing," International Conference on Cyber Security, 2012.*

5. *HaralambosMouratidis, Shareeful Islam, Christos Kalloniatis, and Stefanos Gritzalis, "A framework to support the selection of cloud providers based on security and privacy requirements," The Journal of Systems and Software,2013*
6. *Y. Zhu, H. Hu, G. Ahn, M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage,"* IEEE Trans. Parallel and Distributed Systems*, vol. 23, no. 12, pp. 2231-2244, Dec. 2012.*
7. *Xiao Zhang; Hong-tao Du; Jian-qan Chen; Yi Lin; Lei-jie Zeng,"Ensure Data Security in Cloud Storage," Network Computing and Information Security (NCIS), 2011 International Conference on, vol.1, no.,p p.284-287, 14-15 May 2011.*
8. *Q. Wang, C. Wang, K. Ren, W. Lou, J. Li, " Data Dynamics Enabling Public Auditability for Storage Security in Cloud Computing,"* IEEE Trans. Parallel Distributed Systems*, vol. 22, no. 5, pp. 847-859, May 2011.*
9. *Hideaki Ishii, Roberto Tempo, and Er-Wei Bai, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transo n parallel distr, VOL. 24, NO. 06, June 2013.*
10. *S. Singh, D. Chand," Trust Evaluation in Cloud based on Friends and Third Party's Recommendations" in Proceedings of IEEE, recent advances in Engineering and Computational Sciences, 2014.*
11. *Kan Yang, An Efficient and Secure Dynamic Auditing Protocol for Cloud Computing Data Storage, parallel and distributed systems IEEE Trans., on, vol.24, issue 9, pp:1711-1726, 2013.*
12. *N.Praveen Kumarga and D.Sireesha, "Ensuring Data Integrity in Cloud Computing," International Journal of Computer Science and Network Security, Vol.14 No.9, September 2014*
13. *Wei Li, KaipingXue, YingjieXue, and Jianan Hong, "TMACS: A Robustand Verifiable Threshold Multi-Authority Access Control System in PublicCloud Storage," IEEE Transactions on parallel and distributed systems,VOL.24, NO. 06, October 2015.*
14. *Pussewalage, H.S.G. and Oleshchuk, V.A. An attribute-based access control scheme for secure sharing of electronic health records. IEEE 18th International Conference on e-Health Networking, Applications and Services, 2016*
15. *Kan Yang and XiaohuaJia, "Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage, IEEE Transactions on" parallel and distributed systems, IEEE Transactions, Vol. 25, NO. 07, July 2014.*
16. *Farokhi, S. Towards an SLA-based service allocation in multi-cloud environments. 14th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), 2014, 591-594.*
17. *Mar, K.K., Hu, Z., Law, C.Y. and Wang, M. Secure cloud distributed file system. 11th International Conference for Internet Technology and Secured Transactions (ICITST), 2016, 176-181.*
18. *Hashi, Y., Uchibayashi, T., Hidano, S., Kiyomoto, S., Rahim, A., Suganuma, T. and Hiji, M. Data Protection for Cross-Border Live Migration in Multi-cloud Environment. Fourth International Symposium on Computing and Networking (CANDAR), 2016, 681-685.*
19. *Tran Viet Xuan Phuong, Guomin Yang, and Willy Susilo, "Hidden Ciphertext-Policy Attribute-Based Encryption Under Standard Assumptions," Information Forensics and Security IEEE Trans, Vol. 11, NO. 1, January 2016.*
20. *EntaoLuo, Qin Liu, and GuojunWang,"Hierarchical Multi-Authority and Attribute-Based Encryption Friend Discovery Scheme in Mobile Social Networks," IEEE Communications Letters, Vol. 20, NO. 9, September 2016.*