Research Article

An Efficient Improving Cloud Data Storage Security using Failure Aware Resource Scheduling Algorithm

S. Surya Parkavi [a], S. Varshini [b], R .Naresh[c*]

[a,b] B.Tech, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Chennai, Tamilnadu, India-603 203.
[c*]Associate Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Chennai, Tamilnadu, India-603 203.
E-Mail: sj5039@srmist.edu.in, vs7370@srmist.edu.in, nareshr@srmist.edu.in
*Corresponding Author: R. Naresh

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 4 June 2021

Abstract: Cloud computing, provides the delivery of on-demand computing resources, it is displayed as an innovative platform, provides a high-performance computing environment for the user. The need for cloud computing is increasing gradually every day. Cloud computing, data storage security is a big problem since the data in the cloud must be sent via the Internet, data security is a big problem. Integrity, accountability, privacy, access control, authentication, must be to maintain an important mechanism for data protection, such as approval. To overcome this problem, the proposed Failure Aware Resource scheduling (FARS) to reduce the failure leading and reduced system performance tasks. The proposed method is clients send data using encryption for protecting the highly confidential files because the files or data unauthorized persons cannot be stolen or view the files so the files or data protected then generate the One-Time Password (OTP) for decrypting the files. Nodes with relatively low computing power and a low failure rate can provide better performance and reduced resources. The method is based on failure aware scheduling, especially for users who want to move the collective frequently, which can reduce the discovery time of the cloud service rather than the failed resource planning methods. That the crowdsourcing model is an effective way to solve huge co- tasks.

Keywords: One-Time Password (OTP), Failure Aware Resource scheduling (FARS), Cloud Service Provider (CSP), Plain Text (PT), Cipher Text (CT).

1. Introduction

Cloud computing is a new generation that offers cloud services via the Internet. These offerings include things like storage, software, hardware and community programs. Cloudy cloud computing more than one service issuer Cloud Service Provider (CSP) approach via a cloud carrier. User-oriented IT services are provided by using cloud computing. The advantage is two big garage abilities and a powerful computing cloud. Now, with cloud computing step by step humans are used to store their photos, contacts, or different files to the development of cloud servers. At an equal time, powerful computing functionality is also used by individuals or agencies. For the benefit of daily existence, many new programs made cloud computing.

In one factor, the cloud consumer/terminal may additionally outsource via their information storage or a server computing cloud to hold their feet, and the cloud user/terminal is simplest to be considered as a "device" enter and output. To reduce the computational value of the deciphering set of rules of ABE, if it want to use the powerful computing energy of the cloud server or a few proxies, Green has presented the idea of outsourcing deciphering and ABE have been called methods. In order to spend a small value to decrypt the encrypted records through the cloud server, the wishes of the consumer, and a big quantity entire the calculation of their gadget. That is, by the cloud server's first output calculates delegation conversion key and the authentic encrypted text, the person subsequently converted cipher text through the calculation of the "decryption" set of rules, it is feasible to acquire the corresponding plaintext, and to mention. This calculation model additionally poses some challenges while a person outsources sensitive statistics to the cloud server protection and privacy of data. Many packages use complicated access manipulation mechanisms to protect encrypt sensitive facts. This new public encryption key raw in order that are able to via the use of the personal key related to the cipher text or get entry to policies, get admission to manage in an encrypted file. Layered encryption scheme proposed report series.

Encryption is the Plain Text (PT) is converted to data called Cipher Text (CT) and the code is unable to handle one decryption algorithm is used to reverse the original CT. Cloud data for encrypting and decrypting files. If the key attribute set to meet the cipher text associated access structure user to decrypt the cipher text. Obviously, this system is closer to the traditional access control method in concept. On the other hand, a system in the ABE, circuits for general access policy may be any program as the strongest form of a fixed operating time of the policy can be expressed in expression circuit. Under these situations, healthcare agencies use encrypt for files that store records in the cloud through particular access rules. Users who want to

get right of entry to the data files have selected no longer to address the complex decryption method regionally due to aid constraints. Instead, a number of the maximum probable outsourced decryption packages to cloud servers. Although each person can study something about the national delegation that may be converted to the authentic cipher text on a simple untrustworthy cloud server. With the rapid improvement of cloud computing technology, the amount of facts in cloud generation, especially images, movies, and multimedia documents, is increasing exponentially. In recent years, image storage and sharing clouds were attracting interest. However, it also poses many problems with the safety of photographs and different multimedia files within the cloud.

2. Related work

Green processing is the environment reliable and recyclable utilization of resources. The unpracticed cloud organizations can diminish their cost or energy prerequisites through adjusting its general presentation, streamlining sources the executives and administrations [3]. The technique isn't proficient for the cloud worker inside the green cloud organizations [2]. To consider recyclable use of assets for the cloud worker, it prescribe another and comfortable way to deal with diminish general overhead of the cloud worker while numerous clients satisfying a get admission to strategy require the re-appropriated decoding for the indistinguishable code literary substance aside from lessening the unscrambling calculation esteem for clients [4].

The arising cloud-based absolutely Internet of Things (IoT) worldview permits IoT gadgets to immediately add their accumulated realities to the distant cloud and permits data proprietors to advantageously control the ones records through cloud APIs, which has generously diminished framework subsidizing and data the board cost in bunches of IoT programs [11]. Taking into account that the re-appropriated data are out of the in essence control of and the cloud worker can't continually be totally believed, an approach to safely erase the unneeded sensitive data put away in cloud to forestall potential records spillage inconveniences is a major task [9] [13]. Distributed computing turns into an expanding number of well-known for realities proprietors to re-appropriate their records to public cloud workers simultaneously as permitting implied data clients to recover those records put away in cloud [6] [14] [16]. This type of registering model carries difficulties to the security and privateers of records put away in cloud. Property based encryption period has been utilized to design quality-grained admittance control framework, which bears the cost of one genuine procedure to cure the wellbeing inconveniences in cloud setting [5] [7].

Characteristic based absolutely encryption is a promising cryptographic apparatus for data proprietor to see top notch grained date partaking in the distributed computing [12] [17] [8]. In the encryption of most current plans, a boundless scope of secluded exponentiations are frequently required; the computational expense of its miles developing directly with the intricacy of the get admission to inclusion [9] [18]. Also, inside the greatest present ABE with redistributed unscrambling, the calculation cost of creating change mystery's growing straightly with the scope of characteristics identified with customer individual key; those calculations are restrictively high for cell gadget clients, which transforms into a bottleneck limiting its utility. To address the above issues, it exhort a comfortable redistributing calculation for secluded exponentiation in a solitary unmarried untrusted worker model and a fresh out of the plastic new strategy to produce the change key. In view of these procedures and Brent Waters' code literary substance strategy plot, it advocate an conspire with undeniable redistributed every encryption and unscrambling, which could safely re- appropriate encryption and decoding to untrusted encryption administration organization and decoding transporter guarantor, separately, leaving most straightforward a steady number of simple tasks for the and qualified clients to perform Territorially [20] [19].

3. Materials and methods

Cloud computing is to provide a variety of services on the Internet, the rapidly growing technology. This is, on the basis of the payment amount, based on the needs, function, network services, and other resources, increase infrastructure, platforms and the like, or it can reduce the requirement. When the enterprise store high-confidential files on the cloud server, there is a problem. Case, high-confidential files on the cloud server there is a problem with the store of the company.

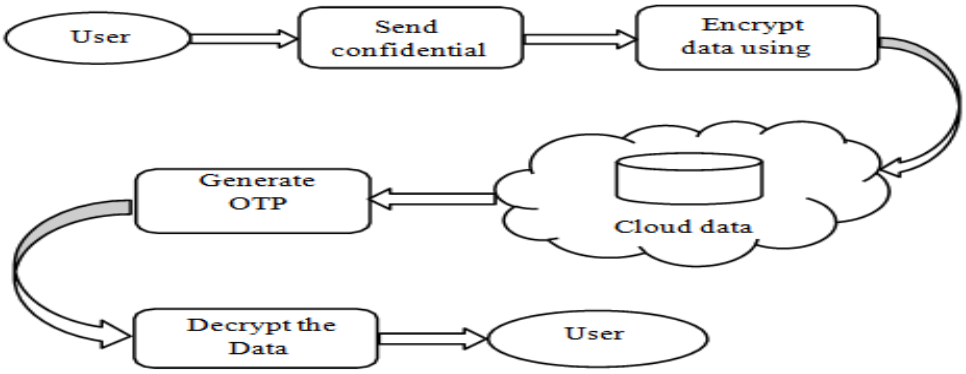

Figure 1: Proposed Diagram

Figure 1 describes Encryption is any type of conversion of data into a form that has not been understood. It converts the encrypted data into understandable format encryption instead, and decodes. The user, if it provides the correct login credentials during server authentication [2]. Unauthorized users are not allowed to access the uploaded private files by other users.

3.1 Cloud storage

Cloud storage is a cloud computing model. Managing data storage services on the Internet as stored data, the operation of cloud computing providers. It is delivered in the capacity and cost of just in time, there is no need to buy, it have to manage their own data storage infrastructure. This is, "anytime, anywhere," agility of data access, and provides the globality and durability.

3.2 Secure data Encryption

Data encryption in the cloud is the process of encoding data before it is moved to the cloud for conversion or transfer. The data owner encrypts the first file, and store it in the cloud. Typically, encryption mechanism files contain metadata attached to protected objects contain information about how to decode the protected object. This meta- data is a part of the file header, which is encrypted, always inserted at the beginning of the file. This metadata can be a single user to access the file. Encryption is any type of conversion of data into a form that has not been understood [13] [14] .

3.3 Data Decrypt

Users select files to read or edit from shared folders in their cloud account. Now, the application running on the client is trying to generate and decrypt a one-time password (OTP) by it. An application to check if the login username is in the header of an encrypted file in the file header to see if there is a match between the group and the users in the group, then the group If the first attempt to perform the name belongs to the logged-in user is part of a match between some group or an existing group and the group to which the user belongs, then the user Get the private key of the group. Once the user gets the key, it can be used by the application to automatically update it from memory. Instead, it transforms and decrypts the encrypted data into a format that is easy to understand.

3.4 Verification and download

Users upload the confidential files to the cloud server. The file will be encrypted before it starts the actual upload process. It needs to make sure the process of downloading the encrypted files. The contents of the file must not be damaged during the encryption and decryption. In order to test such a function, some of the test file is selected; all these files will be uploaded to encryption. When the file is downloaded, the file size must be exactly the same at the byte level, and the content must be decrypted. This will ensure that it can be decoded into the original format of the encrypted file.

4. Result and discussion

Distributed storage is an innovation that permits it to backup files and then gets these records through the cloud. It wants to separate this definition. First of all, the potential is the capability to backup files and exceptional asset PC use. This functionality generally includes a difficult pressure, USB flash pressure, or any other power. Since the force community statistics may be harmed or stolen, questioning produced by using the actuator in gadget ability facts.

No. of data	FARS %	CPCPA %	DSSE%
10	75	70	69
20	78	75	70
30	83	79	75
40	92	86	80

Table 1: Accuracy performance of cloud storage

Table 1 describes the accuracy performance of cloud storage in these the proposed algorithm of Failure Aware Resource scheduling (FARS) it achieved high performance with 92% of result and it is compared to existing algorithms of Cipher printed content-Policy Attribute (CPCPA) it gains 86% of result and with Dynamic Searchable Symmetric Encryption (DSSE) it achieves 80% of result.

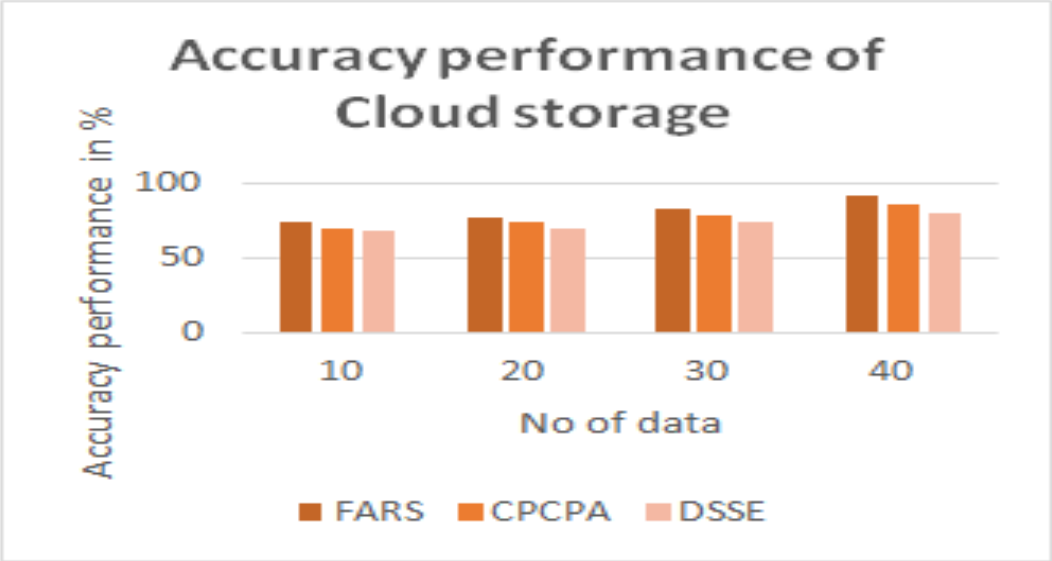

Figure 2 Accuracy performance of cloud storage

Figure 2 describes the accuracy performance of cloud storage the proposed algorithm of Failure Aware Resource scheduling (FARS) it achieved high performance with 92% of result and it is compared to existing algorithms of Cipher printed content-Policy Attribute (CPCPA) it gains 86% of result and with Dynamic Searchable Symmetric Encryption (DSSE) it achieves 80% of result.

No. of data	FARS %	CPCPA %	DSSE%
10	35	40	50
20	30	35	48
30	22	30	42
40	18	28	39

Table 2: Performance of Time complexity

Table 2 describes the time complexity performance in these the proposed algorithm of Failure Aware Resource scheduling (FARS) it achieve its task within short time performance so that the proposed it gives superior performance compared to existing algorithms.

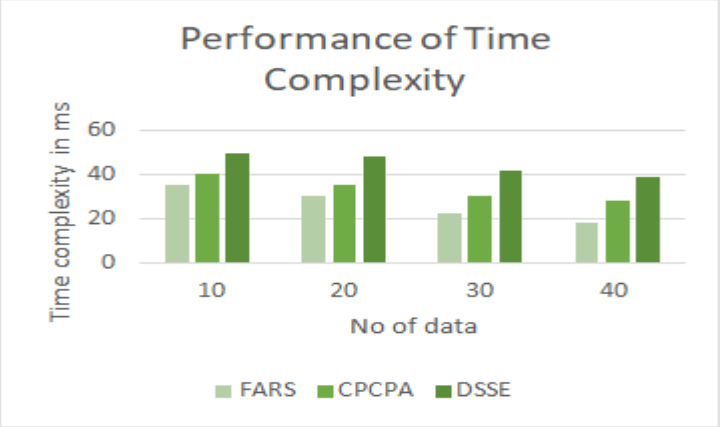

Figure 3 Performance of Time complexity

Figure 3 describes the time complexity performance the proposed algorithm of Failure Aware Resource scheduling (FARS) it achieved high performance with 18 ms of result and it is compared to existing algorithms of Cipher printed content-Policy Attribute (CPCPA) it gains 28 ms of result and with Dynamic Searchable Symmetric Encryption (DSSE) it achieves 39 ms of result.

5. Conclusion

Cloud computing is growing into a new thing, it really is a new trend and many organizations. The perceived failure of the proposed Failure Aware Resource scheduling (FARS) algorithm is the data owner and its users to share sensitive data secure data sharing scheme. Instead, the user sends a private decryption key, the decryption key data owners are assigned to shared authority and trusted users. Public cloud data by receiving the decryption key from the trusted authority decrypts half. Then authorized users authorized to decrypt the received decryption key to decrypt the data half a trusted authority. As a result, between cloud service providers and a large number of users to calculate the cost of distribution in a safe manner.

References

1. 1. J. Yu, K. Ren, C. Wang, Enabling cloud storage auditing with verifiable outsourcing of key updates, IEEE Trans. Inf. Forensics Secure. 11 (6) (2016) 1362-1375.
2. A.Saranya, R.Naresh "Cloud Based Efficient Authentication for Mobile Payments using Key Distribution Method", Journal of Ambient Intelligence and Humanized Computing, Springer, 02 January, 2021. DOI: 10.1007/s12652-020-02765-7
3. Y. Fan, Y. Liao, F. Li, S. Zhou, G. Zhang. Identity-based auditing for shared cloud data with efficient and secure sensitive information hiding. IEEE ACCESS, 7(2019), 114246-114260. DOI:10.1109/ACCESS.2019.2932430
4. Q. Su, J. Yu, C. Tian, H. Zhang and R. Hao, How to securely outsource the inversion modulo a large composite number, J. Syst. Softw. 129 (C) (2017) 26-34.
5. R.Naresh, P.Vijayakumar, L. Jegatha Deborah, R. Sivakumar, "A Novel Trust Model for Secure Group Communication in Distributed Computing", Special Issue for Security and Privacy in Cloud Computing, Journal of Organizational and End User Computing, IGI Global, Vol.32, No. 3, Septemer 2020, Pp. 1-14. DOI: 10.4018/JOEUC.2020070101
6. J. Li, F. Sha, Y. Zhang, X. Huang, J. Shen, Verifiable outsourced decryption of attribute-based encryption with constant ciphertext length, Secur. Commun. Netw. 2017 (2017) doi:10.1155/2017/3596205.
7. A.Saranya, R.Naresh "Efficient mobile security for E health care application in cloud for secure payment using key distribution", Neural Processing Letters, Springer, 2021, DOI: 10.1007/s11063-021-10482-1
8. R.Naresh, M.Sayeekumar, G.M.Karthick, P.Supraja, "Attribute-based hierarchical file encryption for efficient retrieval of files by DV index tree from cloud using crossover genetic algorithm",Soft Computing, Springer, Vol.23, No. 8, 2019, Pp. 2561-2574. Doi: https://doi.org/10.1007/s00500-019-03790-1
9. C. Zuo, J. Shao, G. Wei, M. Xie, M. Ji, CCA-secure ABE with outsourced decryption for fog computing, Future Generation Computer Systems, Volume 78, Part 2, 2018, Pages 730-738, https://doi.org/10.1016/j.future.2016.10.02.8.

10. P.Vijayakumar, R.Naresh, L. Jegatha Deborah, SK Hafizul Islam, "An efficient group key agreement protocol for secure P2P s", Security and Communication Networks, Wiley, Vol.9, No.17, pp.3952–3965, 2016. http://onlinelibrary.wiley.com/doi/10.1002/sec.1578 /abstract
11. V. Sandor, Y. Lin, X. Li, F. Lin, S. Zhang, Efficient decentralized multiauthority attribute based encryption for mobile cloud data storage, Journal of Network and Computer Applications, Volume 129, pp. 25-36, 2019.
12. J. Li, N. Chen and Y. Zhang, "Extended File Hierarchy Access Control Scheme with Attribute Based Encryption in Cloud Computing," in IEEE Transactions on Emerging Topics in Computing. doi: 10.1109/TETC.2019.2904637.
13. P.Vijayakumar, R.Naresh, SK Hafizul Islam, L. Jegatha Deborah "An Effective Key Distribution for Secure Internet Pay-TV using Access Key Hierarchies", Security and Communication Networks, Wiley, Vol.9, No.18, pp.5085–5097, 2016. http://onlinelibrary.wiley.com/doi/10.1002/sec.1578/full
14. R. Naresh, M Meenakshi, G Niranjana, "Efficient study of Smart Garbage Collection for Ecofriendly Environment", Journal of Green Engineering, Vol.10, No.1, pp.1-10, Feb 2020.
15. J. Li, X. Lin, Y. Zhang and J. Han, "KSF- OABE: Outsourced Attribute Based Encryption with Keyword Search Function for Cloud Storage," in IEEE Transactions on Services Computing, vol. 10, no. 5, pp.715-725, 1 Sept.-Oct. 2017.
16. R Divya Mounika, R.Naresh, "The concept of Privacy and Standardization of Microservice Architectures in cloud computing", European Journal of Molecular & Clinical Medicine, Vol 7, No 2, Pages 5349-5370, Dec 2020.
17. Y. Liao, Y. He, F. Li, S. Zhou, Analysis of a mobile payment protocol with outsourced verification in cloud server and the improvement, Comput. Stand. & Interfaces 56 (1) (2018) 101-106.
18. R.Naresh, AyonGupta, Sanghamitra, "MALICIOUS URL DETECTION SYSTEM USING COMBINED SVM AND LOGISTIC REGRESSION MODEL", International Journal of Advanced Research in Engineering and Technology (IJARET), Vol.10, No.4, pp. 63-73,May 2020.
19. M Meenakshi, R Naresh, S Pradeep "Smart Home: Security and Acuteness in Automation of IOT Sensors", International Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol. 9, No. 1 , pp. 3271- 3274 , Nov 2019.
20. J. Li, F. Sha, Y. Zhang, X. Huang, J. Shen, Verifiable outsourced decryption of attribute-based encryption with constant ciphertext length, Secur. Commun. Netw. 2017 (2017) doi:10.1155/2017/3596205.