Research Article

ACCENTS Transactions on Information Security, Vol 5(19)
ISSN (Online): 2455-7196
http://dx.doi.org/10.19101/TIS.2020.517008

An efficient data security mechanism with data sharing and authentication

Md. Farooque[1*], Kailash Patidar[2], Rishi Kushwah[2] and Gaurav Saxena[2]
M.Tech Scholar, Department of Computer Science, School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India[1]
Assistant Professor, Department of Computer Science, School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India[2]

©2020 Md. Farooque et al. This is an open access article distributed under the Creative Commons Attribution (CC BY) License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract
In this paper an efficient security mechanism has been adopted for the cloud computing environment. It also provides an extendibility of cloud computing environment with big data and Internet of Things. AES-256 and RC6 with two round key generation have been applied for data and application security. Three-way security mechanism has been adopted and implemented. It is user to user (U to U) for data sharing and inter cloud communication. Then user to cloud (U to C) for data security management for application level hierarchy of cloud. Finally, cloud to user (C to U) for the cloud data protection. The security analysis has been tested with different iterations and rounds and it is found to be satisfactory.

Keywords
Cloud computing, AES-256, RC6, U to U, C to U, U to C.

1.Introduction
Cloud computing is a platform which in trending now a days with wide applicability due to on demand resource availability services [1]. It provides the data center in terms of platform, infrastructure and software resources [2─5]. It is also cost effective due to on-demand availability as per the customer depend on the customer needs [6]. There are lot of advantages including on demand, cost effective, better resource availability along with the minimum infrastructure [7─9].

The one of the major challenges in cloud computing environment is the cloud security. In terms of resource sharing there is the chances of data violation and different denial of service attack [10]. As in the cloud computing environment the data sharing along with the interthread communication are the major requirement [11]. So, there is the need of data security when data will be shared and it should be on the user control. It should be transparent and the activities must be under the control of the user or the data owner [12]. So, data control is the major aspect which should be done in all the scenario. The main objective of this paper is to achieve the inter cloud data sharing security.

*Author for correspondence

2.Literature survey
In 2020, Singh and Saroj [13] discussed about the cloud computing aspects. It has been discussed in terms of authenticity and reliability. The have suggested a public auditing scheme. It includes privacy authentication, reliability and integration. They have used AES-256 algorithm. IT has been used for encryption purpose. For further integrity check they have applied SHA-512 algorithm. They have used RSA-15360 for public key encryption.

In 2020, Mohiuddin and Almogren [14] discussed about pervasive computing services. It has been applied for cloud outsourced storage and computation. It provides an integration of IoT with cloud data. It shows high scalability and flexibility. It has been discussed in terms of cloud storage provides. They have also discussed regarding the data integrity maintenance. They have investigated the strategies for the safe transition and IoT applications.

In 2020, Mondal et al. [15] discussed about the development of cloud computing aspects. They have suggested security and privacy issues as the big challenges in the cloud computing environment. They have reviewed and analyzed the cryptography, multitenancy, key management etc. along with the impact.

In 2020, Shah et al. [16] discussed about the cloud storage. They have suggested that blockchain is also a cloud storage system which is decentralized. They have suggested blockchain to achieve privacy and security on decentralized storage mechanism.

In 2020, Djigal et al. [17] discussed about efficient workflow scheduling algorithm. But they want to ensure the security requirements also to maintain privacy. They have considered the security aspect in terms of task prioritization and workflow scheduling. They have evaluated the performance based on real world applications.

In 2020, Gupta et al. [18] discussed about the smart applications emergence. They have suggested cloud computing due to on demand availability but worried in terms of security concern. Their main objective is to ensure the confirmed clients. It has been ensured regarding data access. So that sensitive information can only be accessed within organization.

In 2020, Mughal and Joseph [19] discussed about the capacity limit of the client terminal. They have also discussed in terms of cloud stage assistance. They have proposed a cloud storage with blockchain for proper security assistance.

In 2020, Shaohua and Nanfeng [20] discussed about internet traffic. They have discussed the security risk for the same. They have used Hadoop. They have suggested that it supports reliable and scalable development. So, they have proposed an efficient abnormal traffic monitoring system in cloud computing environment. It is based on Hadoop.

In 2020, Priyanka and Ramakrishna [21] discussed about trending technologies in terms of cloud computing environment. They have discussed the cloud healthcare system. They have suggested that these types of system may be helpful in timely diagnosis with reduced system cost. But they have raised the security concern. They have analyzed attribute-based encryption also.

In 2020, Barhate and Dhore [22] discussed about the security features of private cloud. They have discussed about the hybrid cloud and its interoperability. They have provided the combination of three broker policies. It also provides a detail study of cost involve in memory usage and bandwidth.

In 2020, ManJiang et al. [23] discussed about the poor security and performance problem in traditional algorithms. They have proposed a hybrid encryption algorithm. They have applied advanced encryption standard algorithm. It has been used in case of uploaded file. It has been divided into several blocks. Their results show that it is efficient in terms of anti-attack ability and provide high efficiency in terms of file upload and download.

In 2020, Kumar et al. [24] discussed about cloud storage. They have suggested security issue in terms of data storage. They have proposed a hybrid cryptography system. They have used RSA algorithm. They have implemented their approach in Java. They have suggested that this system can be useful for Internet of Things also.

In 2020, Ke et al. [25] discussed about the system daemon service. They have applied grey relational Analysis. It has been done for the optimization problem. They have suggested the service-aware flow scheduling. It has been done through the data center networks. It provides better traffic load balancing along with the conserve table space and data recovery.

In 2020, De et al. [26] discussed about the wide cloud applicability and security aspect. They have reviewed different scheduling algorithms. They have also finalized scheduling algorithms that uses particle swarm optimization. They have considered CPU, memory and disk for the further calculation.

In 2020, Ucuz [27] discussed about different cloud providers vendors like Microsoft Azure, Amazon Web Services, and Google Cloud. They have compared these providers in terms of Internet of Things cloud platform. They have considered the constraints. These are hubs, analytics, and security. Their study is helpful in the selection of the cloud vendors based on the specific requirement and need.

3.Methods

In this paper a data security mechanism has been adopted and developed based on AES-256 and RC6 with two round key generation. The implementation has been done in Java. Apache servers have been used for the different inter connections server availability. It has been selected by the users based on the resource and on demand requirement of services. The virtualization mechanism has been developed in such manner that it will provide optimal storage automatically. It has the capability of auto shrinkage and grow. It has been developed based on Java Collection framework and multithreading

concepts have been utilized. The encryption algorithms have been applied in such manner that it will achieve the maximum randomization. *Figure 1* shows the block diagram of the approach. The following security mechanism has been adopted.

- U to U security: It is user o user security. It has been applied in case of data sharing, intercommunication and inter-node data exchange. It has been applied based on AES-256 and RC6 with two round key generation. Here key generation for the same data for different user is different.
- C to U security: This security has been maintained based on the communication from cloud to user. It may be helpful in the protection of user data from different cloud providers as the complete data protection control is on the hand of cloud users. Here application-based security with authentication have been adopted.
- U to C Security: This security mechanism has been adopted between the communication process of user to cloud. Here security mechanism has been applied on the application but it is for the cloud. So that only restricted part of the shared resources can be controlled by the user and the user of the cloud don't breaches any cloud security protocol.

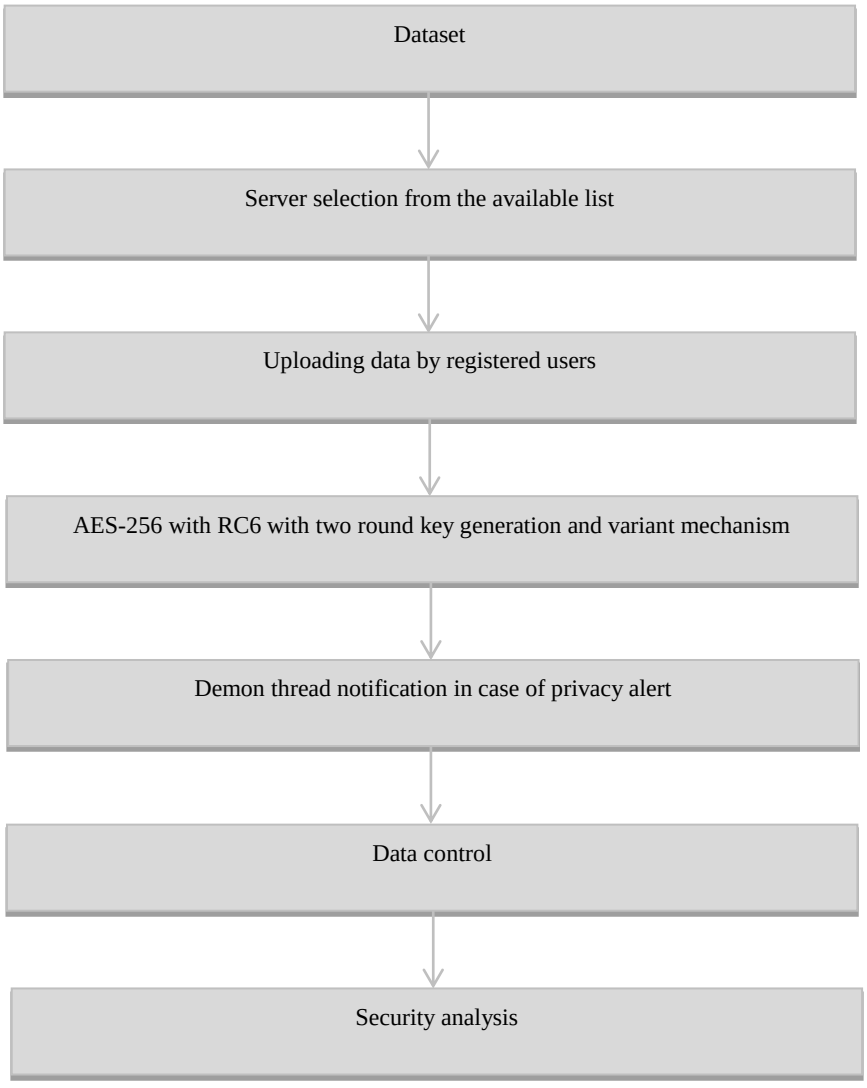

Figure 1 Proposed approach working procedure

4.Results

Figure 2 shows the key variability comparison based on 30 iterations. *Figure 3* shows the key variability comparison based on 90 iterations. *Figure 4* shows the key variability comparison based on 200 iterations. The results from the below comparison shows that the variations in different iterations are found to be minor. It clearly indicates that our proposed approach has the capability of key variations properly. Although the time increases in different iterations but the security mechanism has been improved significantly.

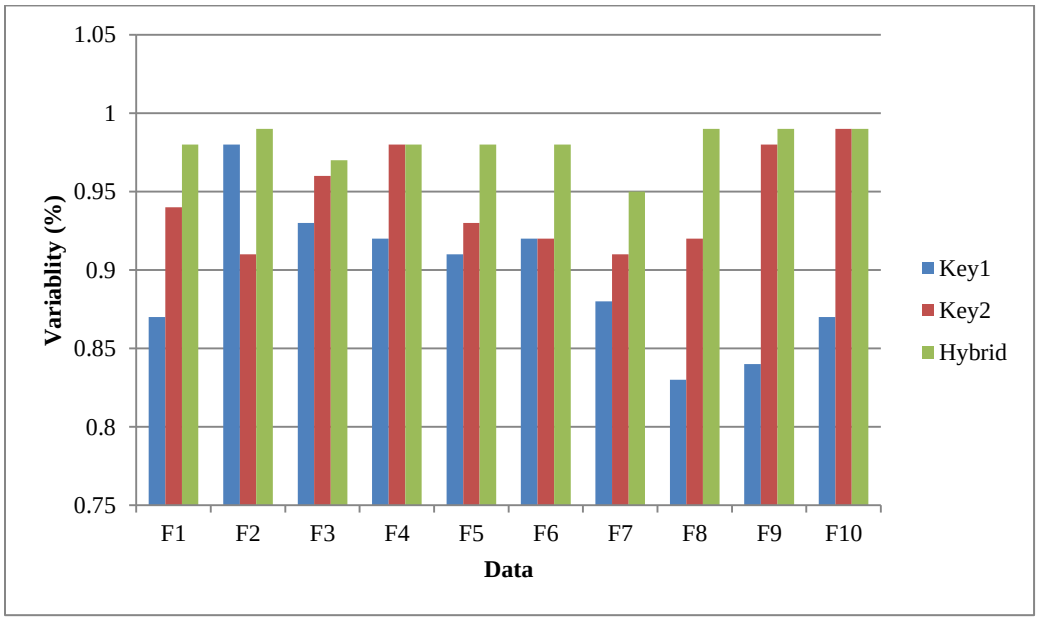

Figure 2 Key variability comparison based on 30 iterations

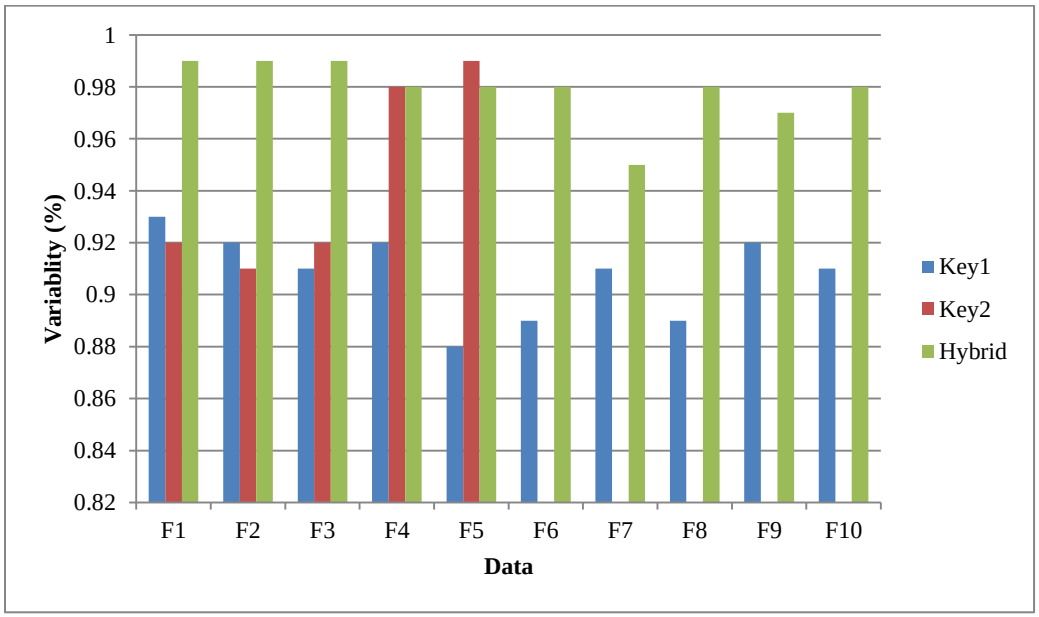

Figure 3 Key variability comparison based on 90 iterations

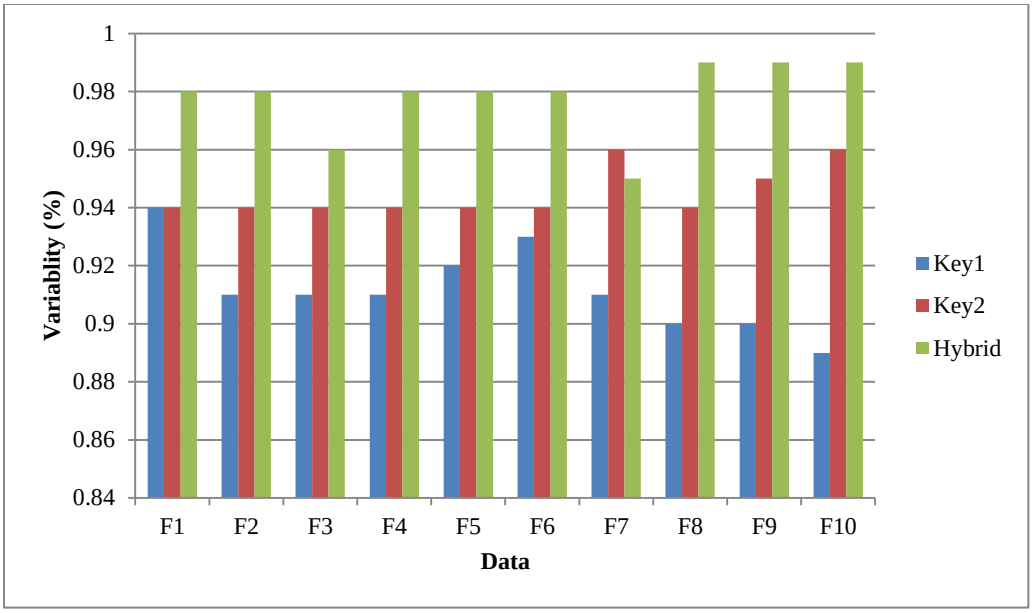

Figure 4 Key variability comparison based on 200 iterations

5.Conclusion

In this paper a data security mechanism has been adopted and developed based on AES-256 and RC6 with two round key generation. Three-way security mechanism has been adopted and implemented. It is U to U for data sharing and inter cloud communication. Then U to C for data security management for application level hierarchy of cloud. Finally, C to U for the cloud data protection. The results are found to be useful in key applicability, variability, block size and round key generations. It provides better security in terms of traditional algorithms. It has been validated with number of iterations and rounds.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Saroj SK, Chauhan SK, Sharma AK, Vats S. Threshold cryptography based data security in cloud computing. In international conference on computational intelligence & communication technology 2015 (pp. 202-7). IEEE.

[2] More S, Chaudhari S. Third party public auditing scheme for cloud storage. Procedia Computer Science. 2016; 79:69-76.

[3] He K, Meng X, Pan Z, Yuan L, Zhou P. A novel task-duplication based clustering algorithm for heterogeneous computing environments. IEEE Transactions on Parallel and Distributed Systems. 2018; 30(1):2-14.

[4] Dubey AK, Dubey AK, Namdev M, Shrivastava SS. Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment. In CSI sixth international conference on software engineering (CONSEG) 2012 (pp. 1-8). IEEE.

[5] Sasubilli SM, Dubey AK, Kumar A. A computational and analytical approach for cloud computing security with user data management. In international conference on advances in computing and communication engineering (ICACCE) 2020 (pp. 1-5). IEEE.

[6] Sasubilli SM, Dubey AK, Kumar A. Hybrid security analysis based on intelligent adaptive learning in Big Data. In international conference on advances in computing and communication engineering (ICACCE) 2020 (pp. 1-5). IEEE.

[7] Bhute S, Arjaria SK. An efficient AES and RC6 based cloud-user data security with attack detection mechanism. International Journal of Advanced Technology And Engineering Exploration. 2016; 3(21):110.

[8] Abdelkader YM, Ahmed M. A new strong user authentication scheme with local certification authority for internet of things based cloud computing services. International Journal of Advanced Technology and Engineering Exploration. 2019; 6(58):217-24.

[9] Shrimali B, Bhadka H, Patel H. A fuzzy-based approach to evaluate multi-objective optimization for resource allocation in cloud. International Journal of Advanced Technology and Engineering Exploration. 2018; 5(43):140-50.

[10] Gabi D, Dankolo NM, Ismail AS, Zainal A, Zakaria Z. Non-preemptive chaotic cat swarm optimization scheme for task scheduling on cloud computing environment. International Journal of Advanced Computer Research. 2019; 9(43):186-96.
[11] Kalangi RR, Rao MC. A novel multi-user fingerprint minutiae based encryption and integrity verification for cloud data. International Journal of Advanced Computer Research. 2018; 8(37):161-70.
[12] Zhe D, Qinghong W, Naizheng S, Yuhan Z. Study on data security policy based on cloud storage. In 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids) 2017 (pp. 145-9). IEEE.
[13] Singh P, Saroj SK. A Secure data dynamics and public auditing scheme for cloud storage. In international conference on advanced computing and communication systems (ICACCS) 2020 (pp. 695-700). IEEE.
[14] Mohiuddin I, Almogren A. Security challenges and strategies for the IoT in cloud computing. In international conference on information and communication systems (ICICS) 2020 (pp. 367-72). IEEE.
[15] Mondal A, Paul S, Goswami RT, Nath S. Cloud computing security issues & challenges: a review. In international conference on computer communication and informatics (ICCCI) 2020 (pp. 1-5). IEEE.
[16] Shah M, Shaikh M, Mishra V, Tuscano G. Decentralized cloud storage using blockchain. In international conference on trends in electronics and informatics (ICOEI)(48184) 2020 (pp. 384-9). IEEE.
[17] Djigal H, Feng J, Lu J. Performance evaluation of security-aware list scheduling algorithms in IaaS Cloud. In IEEE/ACM international symposium on cluster, cloud and internet computing (CCGRID) 2020 (pp. 330-9). IEEE.
[18] Gupta A, Mehta A, Daver L, Banga P. Implementation of storage in virtual private cloud using simple storage service on AWS. In 2nd international conference on innovative mechanisms for industry applications (ICIMIA) 2020 (pp. 213-7). IEEE.
[19] Mughal A, Joseph A. Blockchain for cloud storage security: a review. In international conference on intelligent computing and control systems (ICICCS) 2020 (pp. 1163-9). IEEE.
[20] Shaohua H, Nanfeng X. Abnormal traffic monitoring methods based on a cloud computing platform. In 5th international conference on cloud computing and big data analytics (ICCCBDA) 2020 (pp. 85-9). IEEE.
[21] Priyanka J, Ramakrishna M. Performance analysis of attribute based encryption and cloud health data security. In 4th international conference on intelligent computing and control systems (ICICCS) 2020 (pp. 989-94). IEEE.
[22] Barhate SM, Dhore MP. Hybrid cloud: a cost optimised solution to cloud interoperability. In international conference on innovative trends in information technology (ICITIIT) 2020 (pp. 1-5). IEEE.
[23] ManJiang D, Kai C, ZengXi W, LiPeng Z. Design of a cloud storage security encryption algorithm for power bidding system. In 4th information technology, networking, electronic and automation control conference (ITNEC) 2020 (pp. 1875-9). IEEE.
[24] Kumar A, Jain V, Yadav A. A new approach for security in cloud data storage for IOT applications using hybrid cryptography technique. In international conference on power electronics & IoT applications in renewable energy and its control (PARC) 2020 (pp. 514-7). IEEE.
[25] Ke W, Wang Y, Ye M. GRSA: service-aware flow scheduling for cloud storage datacenter networks. China Communications. 2020; 17(6):164-79.
[26] De Silva WF, Spolon R, Lobato RS, Júnior AM, Humber MA. Particle swarm algorithm parameters analysis for scheduling virtual machines in cloud computing. In 15th iberian conference on information systems and technologies (CISTI) 2020 (pp. 1-6). IEEE.
[27] Ucuz D. Comparison of the IoT platform vendors, microsoft azure, amazon web services, and google cloud, from users' perspectives. In international symposium on digital forensics and security (ISDFS) 2020 (pp. 1-4). IEEE.