International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August 2019

An automated cloud security framework based on FCM in user-cloud environment

Dheresh Soni, M. Kumar

Abstract*: In this paper an efficient secure cloud computing framework has been developed. This framework consists of data grouping based on fuzzy c-means (FCM). It has been used for the individual and associative rankings of uploaded text data on the cloud. For the decision selection ranking of the data simple additive weighting (SAW) method have been used. For data security RC6, RSA and AES algorithms have been used collectively and individually based on the condition. RC6, AES and RSA algorithms have been used as a combination for the complex key security. Based on the decision performance ranking top higher rank which supports are >=50% adopted all the three security algorithms, only one key is applied for the remaining data. The maximum number of keys applied is 5 but there are total three key variants mainly applicable. So we have considered three keys. It has been clear from our results that the keys spreading are automatically increased on the basis of number of files. So in case of high risk the keys are increased automatically and applied.

***Keywords*: FCM, RC6, AES, RSA.**

I. INTRODUCTION

In today's era the services which have been accessible easily by cloud computing on demand with the ease of applicability and reduced cost [1−3]. It has been fulfilled based on the resource requirement and the systems conditions and applicability [4, 5]. The ease of applicability and business performances makes this platform very suitable in current era [6−10].

There are several protocols and applications which have been used widely with these applications. These protocols can be helpful in different communication scenario with the help of data aggregation and specialization. Figure 1 shows the cloud computing resources. The main motivation of our paper is to provide an efficient security protocol for the cloud user authentication and data aggregation at the time of data communication. The communication scenario is mainly affected by the security threats in the cloud computing environment.

The paper objectives are as follows:

1. To provide data categorization for the purpose of data separation and aggregation in cloud computing environment for the purpose of secure communication.
2. To apply decision making process for the security requirement checking in the way that it can be cope the security needs.
3. To apply the separations of the security needs for the concurrent crypto system application and adaptions.
4. To apply data key hybridization for the requirement of complex security system for the cloud data also.

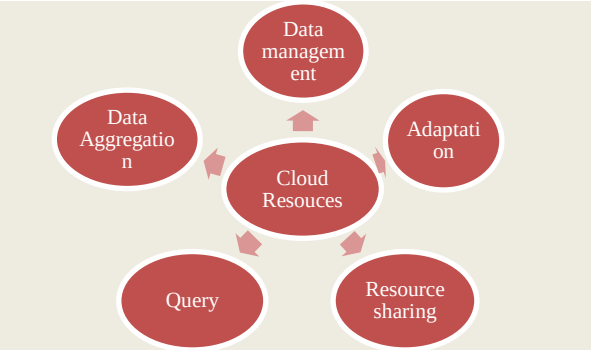

Figure 1 cloud computing resources

II. RELATED WORK

In 2018, Surbiryala and Rong [11] discussed the involvement of cloud computing in case of individuals and organizations. They have suggested that the important factors for using the cloud computing platform are low costs, computational power, and storage services over the Internet. They have suggested the main specialty is the data recovery, according to the authors it is the backbone. They have suggested that the confidential data can be recovered even if the data is deleted. They have discussed the security concerns based on the tools used for recovery in the cloud computing environment. They have proposed a rename method.

In 2018, Bharadwaj et al. [12] discussed the operation ability of the cloud computing environment. They have suggested that like other technology there are also several security risks in cloud computing. They have explored security related issue in cloud computing. They have investigated in the direction of dynamic cloud environment and provides different solutions for the real time challenges.

In 2018, Chandel et al. [13] discussed the enterprise cloud technology and data storage services. They have suggested that due to the security issue several companies do not trust for their sensitive data. They have discussed on the exponential growth of the cloudbased services in China focusing the security concern and applicability.

Revised Manuscript Received on August 30, 2019.
* Correspondence Author
Dheresh Soni*, Research Scholar, Mewar University, Chittorgarh, Rajasthan, India.
M. Kumar, Retired Professor, MANIT, Bhopal, India.

They have also discussed the risk and challenges. In 2019, Koo et al. [14] discussed security issue in cloud computing. They have suggested that the current security system is not sufficient for the national defense information system. They have suggested the need of security architecture based on cloud computing for the national defense command control system. They have also analyzed the U.S. military security requirement need on the cloud computing environment. Based on the Korea national defense information system and they have insight the security requirements needs.

In 2018, Abdullah and Bakar [15] suggested that the cloud computing provides an intermediate act for providing the virtualization synergy support. They have also suggested that the security in case of data storage is a bigger challenge in case of cloud computing. It is mainly in case of illegal access and shared network environment. They have suggested that several research works has been done in this environment but less work has been done on the anonymity of user and identity. They have identified the fundamental requirements of the security. They have discussed the Risk-Adaptable Access Control (RAdAC) for the user protection. They have proposed two-factor authentication scheme in RAdAC.

In 2018, Seo et al. [16] discussed the cloud as network function virtualization (NFV) and the security aspects in cloud computing. They have suggested there are lot of works has been presented but the problem has not been elaborated in terms of what problems. Based on the problem of security based on the communication between cloud computing services they have proposed three approaches. First they have proposed an integrative identification system. It is in a single cloud service. Second is action based token authorization, and finally partially encrypted communication between the identification system and cloud services. They have proved the utility of their approach.

In 2017, Cordova et al. [17] discussed the security aspects like confidentiality, integrity and data protection of electronic resources in a workplace. They have suggested that the need of strong encryption and decryption techniques to ensure private corporate information that dwell and are imparted over the cloud. They have compared the AES, Blowfish and RSA algorithms. Their results show that Blowfish shows higher time efficiency.

In 2017, Alshammari et al. [18] discussed cloud computing in terms of distributed computing, grid computing, and virtualization. They have discussed the safety of the cloud computing environment. They have investigated and discussed the security attacks and possible solutions.

In 2017, Agarkhed and Ashalatha [19] discussed the cloud computing capabilities to its users. They have suggested that several peoples store their data onto the cloud. So there is the need of security to verify distributed storage framework with autonomous productive evaluating administration to check the accuracy of redistributed information. Huge clients continue sending the information over Internet and they are made put away in cloud information focuses remotely. The information documents can be gotten to by unapproved clients or programmers in the unbound cloud organize. This leads in spilling of classified information or information misfortune during the transmission over the system. Henceforth verifying the cloud assumes a significant job in cloud condition. The information move over remote system over the globe must be shielded securely from unapproved utilization over the cloud. The information documents and the remote server farms must be given additional security too as support abilities from programmers or outsider gatecrashers. In such manner, information reviewing alongside security protecting, honesty and dynamic capacities plays as a capable technique for keeping from different cloud attacks which are considered in this work. They have evaluated the current verification and validation prospective.

In 2018, Gayatri et al. [20] discussed the flexibility and scale of IT processes in prospect of cloud computing. They have discussed security aspect in the cloud computing. They have suggested the security concern in terms of data storage as it is stored remotely. They have suggested that the comparative analysis is needed based on the utility of cloud computing and the security for the complete cloud computing impact. Thy have summarized the issue and discuss the feasible and accessible solutions

In 2017, Arora et al. [21] discussed the adoption of cloud computing due the economic benefits. They have suggested that there are several cloud service providers for hosting applications onto cloud. But the main concern is still the cloud security and it is the major obstacle according to the authors. They have presented a hybrid cryptographic system (HCS). It combines the encryption mechanism of symmetric and asymmetric. They have focused on Cloud ecosystem for the multifactor authentication using the hashing and encryption. They have used CloudSim simulator.

In 2018, Halgaonkar et al. [22] discussed the traffic and the security issue in vehicular adhoc network (VANET). They have used algorithm-I is used for detecting malicious node in VANET. They have suggested that because of dynamic change in VANET, it needs advance level security. They have used road side unit for the data sharing. They communicated vehicles directly through the cloud for cost reduction of cost and security.

III. PROPOSED METHOD

The system structure is designed and developed for providing data security of the uploaded stream for the communication and data processing for the data sharing. The major drawbacks of the existing system are not efficient in cloud data security with missing security applicability selection procedure for the applicability of the security needs for the reliable cloud communication. This situation provokes the need of data security along with the clustering approaches which will provides the grouping of data for finding the data security need for the individual data. It may be helpful in effective data handling also. We have proposed an efficient approach based on the cluster selection with the confirmation data security to all the data with the calculative risk associated with the data. In the first phase the data pre-processing is applied based on the weight assigned. The weight assigned is based on the data values presented in the uploaded text data. There are total 10 data categories for the data attribution; it is completely unbiased as it depends of the data frequency.

The complete range considered here are 1 to 10. It has been used for the grouping based on the risk similarity or the associated weights. This phase provides the mathematical ability of the calculative weights for the further process and assignments. It may be helpful in finding the ranking based on the individual or associative weights through SAW. In the next phase clustering algorithm has been applied. FCM provides clustering in simple and computationally deeper [23, 24]. FCM is considered as the success rate is high in complex data also [23, 24]. After the data preprocessing on the uploaded data from the cloud computing, FCM has been applied. The weigh matrix of 1-10 range has been considered for the data grouping. Grouping has been performed based on the security similarity requirement or based on the weight aggregation. The seeds process in case of centroid mechanism is completely random. FCM algorithm has been presented in form of Algorithm 1. Then SAW method has been applied for the data selection and their ranking order.

Algorithm 1: Fuzzy c-means algorithm

Let D = $\{d_1, d_2, d_3 ..., d_n\}$ are the data point values in the complete set and C = $\{c_1, c_2, c_3 ..., c_n\}$ be the set of centers.

Step 1: Select the cluster centers randomly for the biasness.

Step 2: Fuzzy membership value has been computed:

$$U= \sum_{i=1}^{c} u_{ij} = 1, \forall j = 1,...,n$$

Step 2: Distance value has been computed based on Euclidean approach:

$$J(U, c_1, c_2, ..., c_c) = \sum_{i=1}^{c} J_i = \sum_{i=1}^{c} \sum_{j=1}^{n} {u_{ij}}^m {d_{ij}}^2$$

The range for the membership value is {0,1};

c implies the Centroid.

d_{ij} is the Euclidian distance between i^{th} centroid(c_i) and j^{th} data point;

m ϵ [1,∞] is a weighting exponent.

Step 3: Then membership value has been calculated:

$$c_i = \frac{\sum_{j=1}^{n} {u_{ij}}^m x_j}{\sum_{j=1}^{n} {u_{ij}}^m}$$

$$u_{ij} = \frac{1}{\sum_{k=1}^{c} \left(\frac{d_{ij}}{d_{kj}} \right)^{2/(m-1)}}$$

Step 4: Based on the termination criteria Step 2 and Step 3 are repeated.

Step 5: Finish.

IV. RESULTS AND DISCUSSION

Figure 2 show the automatic key applied on data based on decision ranking (set 1). Figure 3 shows the automatic key applied on data based on decision ranking (set 2). Figure 4 shows the automatic key applied on data based on decision ranking (set 3). Figure 5 shows the automatic key applied on data based on decision ranking (set 4). Figure 6 shows the automatic key applied on data based on decision ranking (set 5).

The set chosen here is completely random. So the chances of biasness are very less. Key grades show the numbers of keys applicability on the concern data. The maximum number of keys applied is 5 but there are total three key variants mainly applicable. So we have considered three keys. It has been clear from our results that the keys spreading are automatically increased on the basis of number of files. Means in case of high risk the keys are increased automatically.

Figure 7 shows the comparative study based on parameters. The messages shows the total number of key messages generated, key shows the total number of keys used and randomness shows the randomization process in key generation for each iteration. It is clear from Figure 7 that our approach has better capability in comparison to reference [25]. Figure 8 shows the comparative study based on key size. It is clear from this comparison that the key size (min/max) variability is better in case of our approach. The maximum key variability and authentication shows the higher security in terms of the higher risk possibility. It shows that our automated approach based on FCM with three standard security algorithms have the capability of complex security.

V. CONCLUSIONS

In this paper an efficient and secure framework based on fuzzy c-means (FCM) algorithm along with the security constraints have been proposed. First the data preprocessing has been performed based on the key selection mechanism. Then FCM algorithms have been applied on the weight matrix for clustering the data based on security risk factors. Then simple additive weighting (SAW) process has been applied for the weight categorization and final decision performance ranking calculation. Clustering performance depicted based on the parameters used for the selected attributes in terms of computational weights. Then based on the performance matrix security constraints have been applied. There are total three encryption standards have been considered in our dissertation. RC6, AES and RSA algorithms have been used as a combination for the complex key security. The results show that it is better in messages, keys and randomness parameters along with the key size.

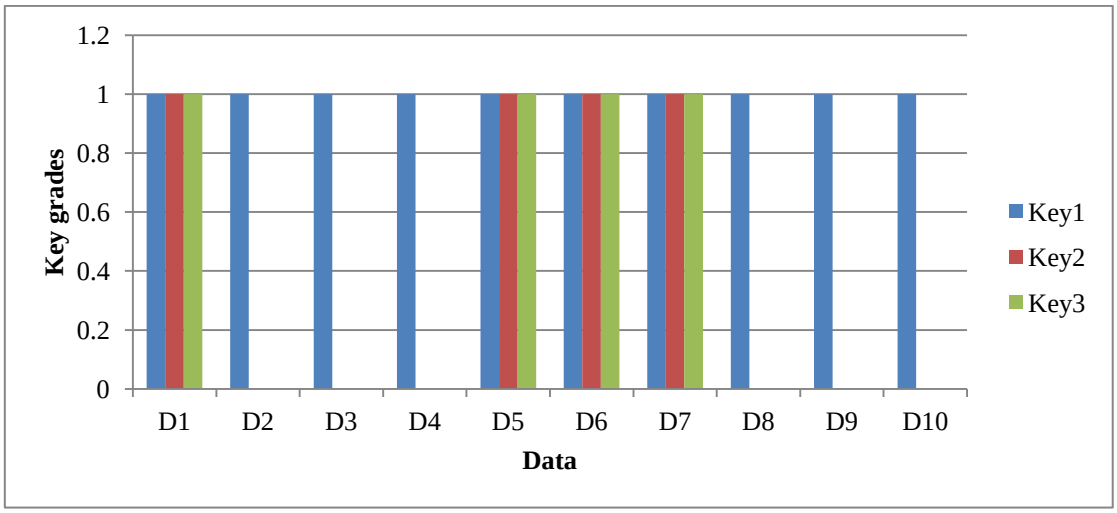

Figure 2 Automatic key applied on data based on decision ranking (Set 1)

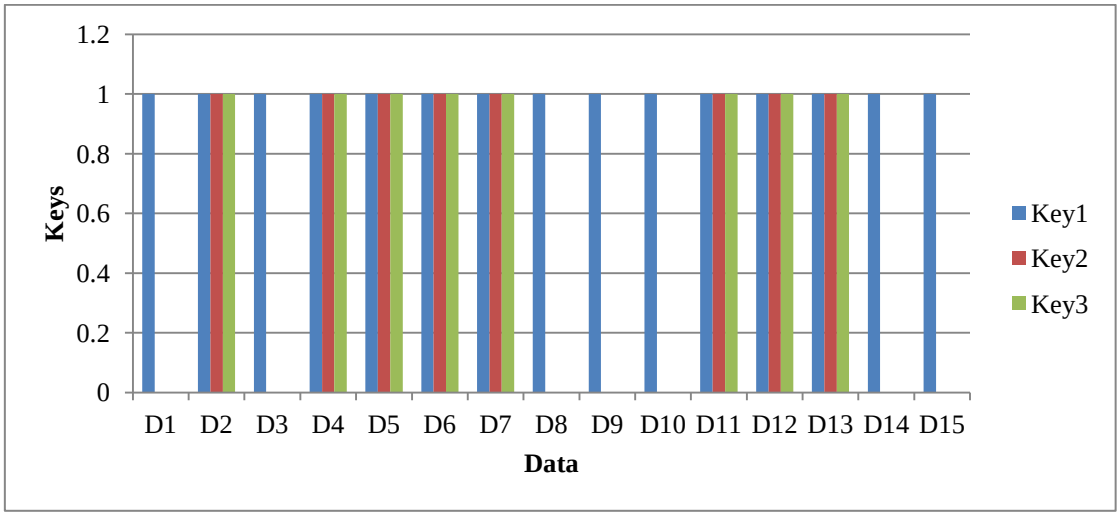

Figure 3 Automatic key applied on data based on decision ranking (Set 2)

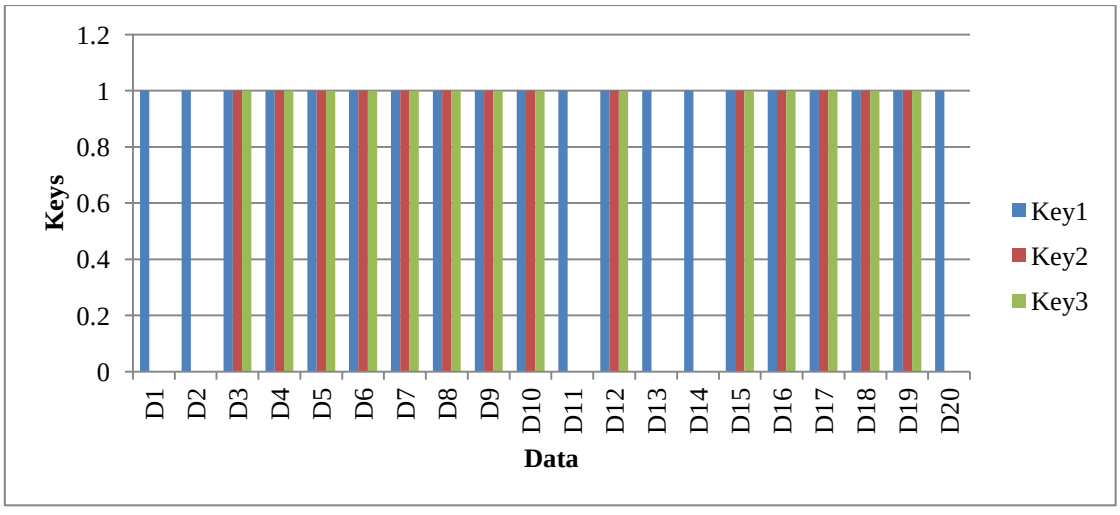

Figure 4 Automatic key applied on data based on decision ranking (Set 3)

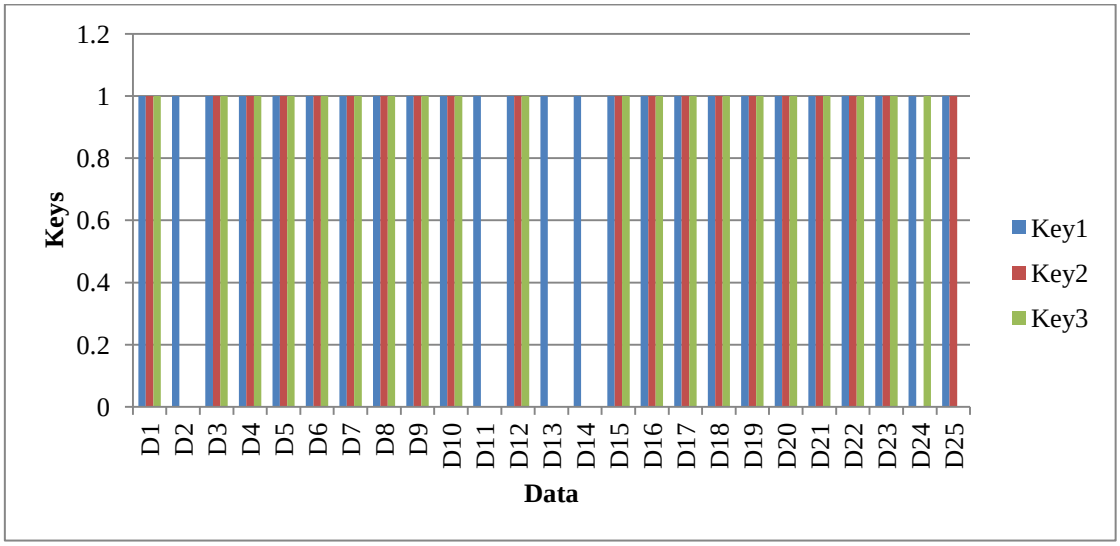

Figure 5 Automatic key applied on data based on decision ranking (Set 4)

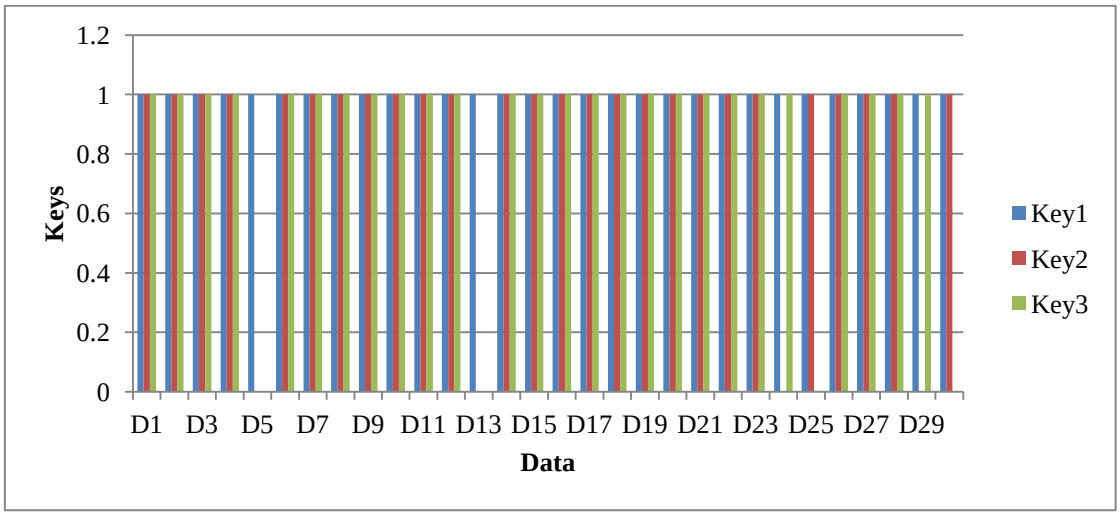

Figure 6 Automatic key applied on data based on decision ranking (Set 5)

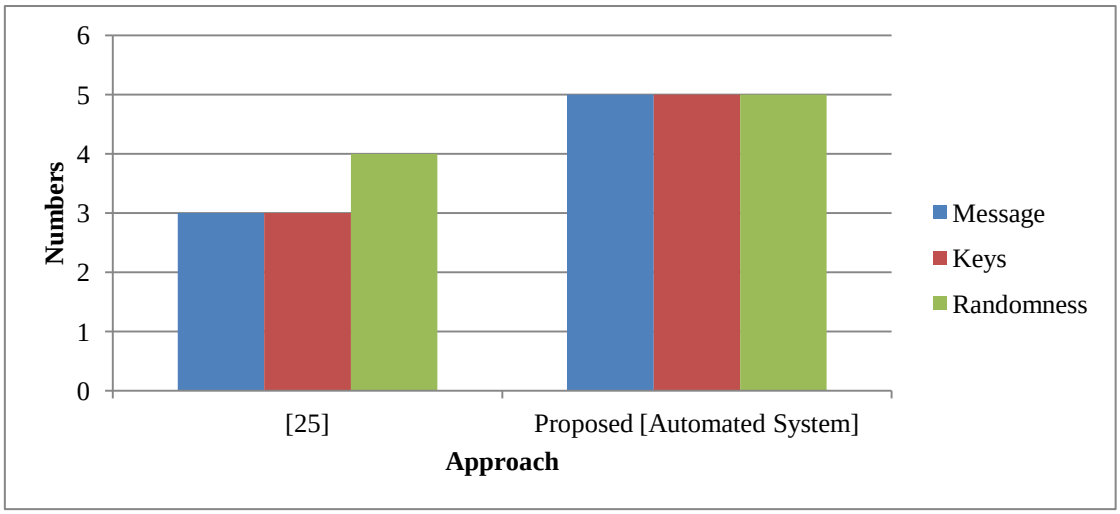

Figure 7 Comparative study based on parameters

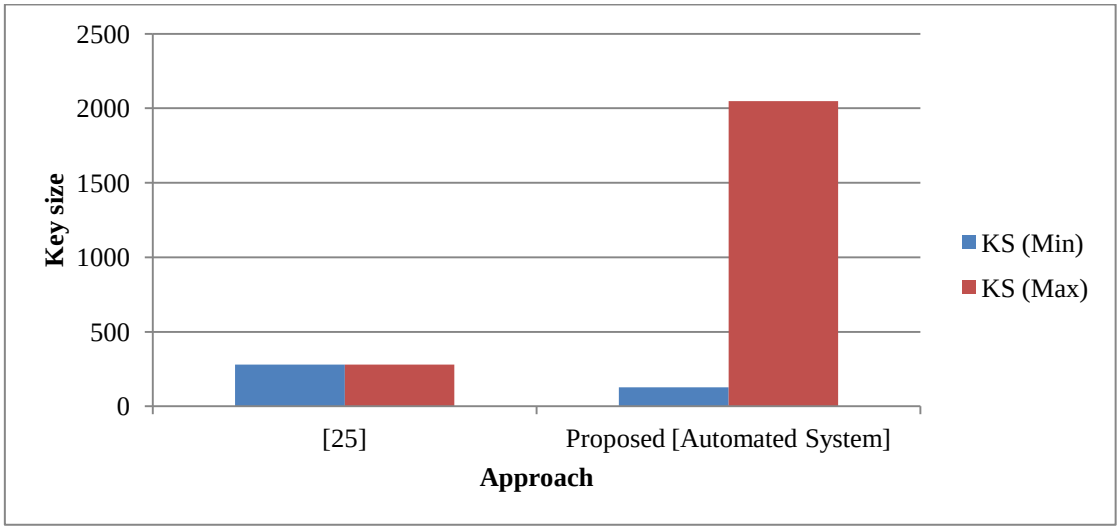

Figure 8 Comparative study based on key size

REFERENCES

1. Patra GK, Chakraborty N. Securing cloud infrastructure for high performance scientific computations using cryptographic techniques. International Journal of Advanced Computer Research. 2014 Mar 1;4(1):66.
2. 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. InSoftware Engineering (CONSEG), 2012 CSI Sixth International Conference on 2012 Sep 5 (pp. 1-8). IEEE.
3. Juels A, Kaliski Jr BS. PORs: Proofs of retrievability for large files. InProceedings of the 14th ACM conference on Computer and communications security 2007 Oct 28 (pp. 584-597). ACM.
4. 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.
5. Bowers KD, Juels A, Oprea A. Proofs of retrievability: Theory and implementation. InProceedings of the 2009 ACM workshop on Cloud computing security 2009 Nov 13 (pp. 43-54). ACM.
6. Manimaran A, Durairaj M. The conjectural framework for detecting DDoS attack using enhanced entropy based threshold technique (EEB-TT) in cloud environment. International Journal of Advanced Computer Research. 2016 Nov 1;6(27):230.
7. Soni A, Hasan M. Pricing schemes in cloud computing: a review. International Journal of Advanced Computer Research. 2017 Mar 1;7(29):60.
8. Annane B, Ghazali O, Alti A. A new secure proxy-based distributed virtual machines management in mobile cloud computing. International Journal of Advanced Computer Research. 2019; 9:43.
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 Jun 1;5(43):140-50.
10. Dalin G, Radhamani V. IRIAL-an improved approach for VM migrations in cloud computing. International Journal of Advanced Technology and Engineering Exploration. 2018 Jul 1;5(44):165-71.
11. Surbiryala J, Rong C. Data Recovery and Security in Cloud. In International Conference on Information, Intelligence, Systems and Applications (IISA) 2018 Jul 23 (pp. 1-5). IEEE.
12. Bharadwaj DR, Bhattacharya A, Chakkaravarthy M. Cloud Threat Defense–A Threat Protection and Security Compliance Solution. In IEEE International Conference on Cloud Computing in Emerging Markets (CCEM) 2018 Nov 23 (pp. 95-99). IEEE.
13. Chandel S, Ni TY, Yang G. Enterprise Cloud: Its Growth & Security Challenges in China. In IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom) 2018 Jun 22 (pp. 144-152). IEEE.
14. Koo J, Kim YG, Lee SH. Security Requirements for Cloud-based C4I Security Architecture. In International Conference on Platform Technology and Service (PlatCon) 2019 Jan 28 (pp. 1-4). IEEE.
15. Abdullah S, Bakar KA. Security and Privacy Challenges in Cloud Computing. In 2018 Cyber Resilience Conference (CRC) 2018 Nov 13 (pp. 1-3). IEEE.
16. Seo J, Nam J, Shin S. Towards a security-enhanced cloud platform. In IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC) 2018 Dec 4 (pp. 229-230). IEEE.
17. Cordova RS, Maata RL, Halibas AS, Al-Azawi R. Comparative analysis on the performance of selected security algorithms in cloud computing. In International Conference on Electrical and Computing Technologies and Applications (ICECTA) 2017 Nov 21 (pp. 1-4). IEEE.
18. Alshammari A, Alhaidari S, Alharbi A, Zohdy M. Security threats and challenges in cloud computing. In 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud) 2017 Jun 26 (pp. 46-51). IEEE.
19. Agarkhed J, Ashalatha R. An efficient auditing scheme for data storage security in cloud. In2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT) 2017 Apr 20 (pp. 1-5). IEEE.
20. Gayatri P, Venunath M, Subhashini V, Umar S. Securities and threats of cloud computing and solutions. In 2nd International Conference on Inventive Systems and Control (ICISC) 2018 Jan 19 (pp. 1162-1166). IEEE.
21. Arora A, Khanna A, Rastogi A, Agarwal A. Cloud security ecosystem for data security and privacy. In International Conference on Cloud Computing, Data Science & Engineering-Confluence 2017 Jan 12 (pp. 288-292). IEEE.
22. Halgaonkar PS, Kathole AB, Nadaf JS, Tambe KP. Providing Security in Vehicular Adhoc Network using Cloud Computing by secure key Method. In International Conference on Information, Communication, Engineering and Technology (ICICET) 2018 Aug 29 (pp. 1-3). IEEE.
23. Dubey AK, Gupta U, Jain S. Analysis of k-means clustering approach on the breast cancer Wisconsin dataset. International journal of computer assisted radiology and surgery. 2016 Nov 1;11(11):2033-47.
24. Dubey AK, Gupta U, Jain S. Comparative study of K-means and fuzzy C-means algorithms on the breast cancer data. International Journal on Advanced Science, Engineering and Information Technology. 2018 Feb 26;8(1):18-29.
25. Nugraha B, Khondoker R, Marx R, Bayarou K. A mutual key agreement protocol to mitigate replaying attack in expressive internet architecture (XIA). InProceedings of the 2014 ITU kaleidoscope academic conference: Living in a converged world-Impossible without standards? 2014 Jun 3 (pp. 233-240). IEEE.