International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Pseudonym-Based Privacy Preserving Framework for Facilitating Cloud Data Security

Premila Rosy

Abstract: ***The advent of cloud computing has revolutionized the option of sharing cloud resources among the cloud users for minimizing the cost overhead. But, the cloud data security is considered as the predominant issue that need to be addressed through the implementation of privacy preserving approaches that sustains and prevents the cloud resources and users from being compromised by the malicious intruders. In this paper, a Pseudonym-based Privacy Preservation Framework (PBPRF) is proposed for understanding its potential towards the accuracy and privacy preservation of cloud data based on the concept of P-Gene. This proposed PBPRF incorporates the benefits of the P-Gene which is responsible in the cloud space for providing security for the stored and utilized private data in the cloud that are periodically exchanged with the clients of the cloud environment. This proposed PBPRF scheme ensures secure sharing of data by relying on a trustworthy data aggregation scheme which is fully dependent on erasable data hiding technique. The simulation experiments and results of the proposed PBPRF mechanism is compared with the baseline PRIAS and TPAAAS techniques in terms of pseudonym generation cost, pseudonym verification, execution time and pseudonym verification time under batched and separated environment.***

Keywords: ***PRIAS and TPAAAS Techniques in terms of Pseudonym Generation Cost,***

I. INTRODUCTION

The advent of cloud computing has brought a dramatic change in the utilization of resources by considering them as a service such that the cloud user can access them from any place and any point of time [1-2]. In cloud computing, the end users utilize the benefits of cloud resources without realizing its exact location such that optimal storage and access of data can be predominantly achieved [3-5]. This cloud environment also wide open the feasibility of deploying and managing the cloud resources in order to prevent additional investment of capital with the focus for necessitating high potent network connectivity [6]. The cloud computing environment also enforces the periodic exchange of data that is independent of the location of data stored in the cloud infrastructure [7].

The majority of the contributed work in the literature propounded for ensuring security proved that pseudonym as the remarkable approach that can ensure security and eliminate the predominant overhead in cloud data dissemination [8-9].

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
Premila Rosy*, Research Scholar, Bharathiyar University, Coimbatore,Tamilnadu, India.

In addition, the pseudonym generation cost and pseudonym verification cost was determined to be enhanced during the deployment of the pseudonym process of security enforcement.

In this paper, Pseudonym-based Privacy Preservation Framework (PBPRF) is proposed using the benefits of P-Gene for quantifying its significance during the process of securing enforcement in the cloud data. The concept of P-Gene used in the proposed PBPRF is potent in ensuring maximum privacy preservation by periodic sharing of private data in the clouds. This proposed PBPRF approach is also determined to be significant since it completely uses the merits of trust-based data aggregation process that focuses on remarkable security. The simulation experiments of the proposed PBPRF mechanism are also conducted using the benchmarked PRIAS and TPAAAS techniques based on pseudonym generation cost, pseudonym verification, execution time and pseudonym verification time under batched and separated environment.

II. RELATED WORK

In this section, the recent works contributed to securing cloud data storage over the past decades are presented with the merits and limitations.

Initially, Ciphertext Policy-based Encryption scheme was proposed securing the data stored in the cloud infrastructure [11]. This Ciphertext Policy-based Encryption scheme utilized a reliable trust manager that handles the keys and its attributes for ensuring potential security in the system. This Ciphertext Policy-based Encryption scheme also incorporated multiple numbers of authorities for facilitating effective revocation and encryption. The complexity of this cipher text policy was determined to be phenomenal in ensuring accurate privacy preservation in the data storage clouds. Then, a privacy preservation approach-based on data integrity protection is proposed for utilizing the inherent features of traffic repairing and fault tolerance [12]. This data integrity protection Scheme was determined to be fine-tuned towards the elimination of deviation that exists between the securities under the implementation of thin cloud storage parameters. A Revocable Multi authority-based Ciphertext policy approach was contributed to implementing maximum security in the cloud data storage [13]. This Revocable Multi authority-based Ciphertext policy approach is potent in facilitating both the backward and forward security processes with the view to ensure significant access control. This Ciphertext policy approach was estimated to incur the low computational complexity and ensured maximum degree of availability and reliability of data cloud resources.

Further, Ciphertext policy-based attribute encryption system using Quantum features for ensuring potential security in the cloud storage [14]. This Quantum-based Ciphertext policy-based attribute encryption system utilized key distribution and generation based on the merits of Quantum key cryptography for facilitating predominant security enforcement process. The computational complexity of this Quantum-based Ciphertext policy-based attribute encryption system was also significant in permitting backward and forward security processes such that the cost of overhead is considerably reduced. A secure mechanism inspired using cipher text policy was also proposed for enforcing superior encryption standards during the process of securing cloud data storage [15]. The security of this contributed Ciphertext policy was estimated to be maximized such that the cost of implementation is maximized to the greatest extent. Then, a method of ensuring data access control of cloud storage was facilitated through the incorporation of the Revocable Multi-authority Cloud Storage [16]. This contributed approach was concluded to improve the rate of anonymity to the maximum level in order to focus on the investigation of data availability. The success rate and optimality rate of this Revocable approach was determined to be maximized with least overhead incurred during the process of enforcing data security.

Furthermore, the Pseudonym Reliable Improved Authenticaion Scheme (PRIAS) was proposed for enhancing the security of the cloud storage through the estimation of honest information [17]. This PRIAS improved the degree of cloud security under the dimension of scalability based on the method of accessing the cloud resources using the incorporation of the pseudonyms in the cloud environment. Finally, a Trusted Pseudonym-based Authority, Availability and Authentication Scheme (TPAAAS) was proposed for better enforcement of security in the cloud storage [18]. This TPAAAS inferred better security and confidentiality in terms of imposing a maximum degree of reliability of the cloud users in the network. The success rate and optimality rate of TPAAAS was also estimated to be maximized with least overhead incurred during the process of enforcing data security.

III. PROPOSED-PSEUDONYM-BASED PRIVACY AND RELIABILITY FRAMEWORK (PBPRF)

The proposed PBPRF is the reliable data hiding scheme that depends on the P-Gene generation for confirming contextual privacy in addition to the included additive data aggregation process that completely concentrates on private cloud data security using erasable data hiding technique. The Figure 1 highlights the architectural diagram of the steps involved in the P-Gene generation and verification process that depend on data encryption process that in turn depends on erasable data hiding. In PBPRF, the accuracy and privacy of each private data cloud is perturb rated to their private data using the creation of P-Gene that eliminates an extra level of data sharing and further the aggregated result are feasible to be recovered from the hidden data through them. This P-Gene oriented erasable data hiding technique is capable of hiding each and every data cloud and its private data based on their newly generated P-Gene characteristics and finally, it sends the hidden data to the other possible communication data private clouds for further interaction. This PBPRF scheme consists of two major phases that includes i) Pseudonym Generation and Maintenance in the primitive initialization phase and ii) Data recovering process in each cloud member in the final phase.

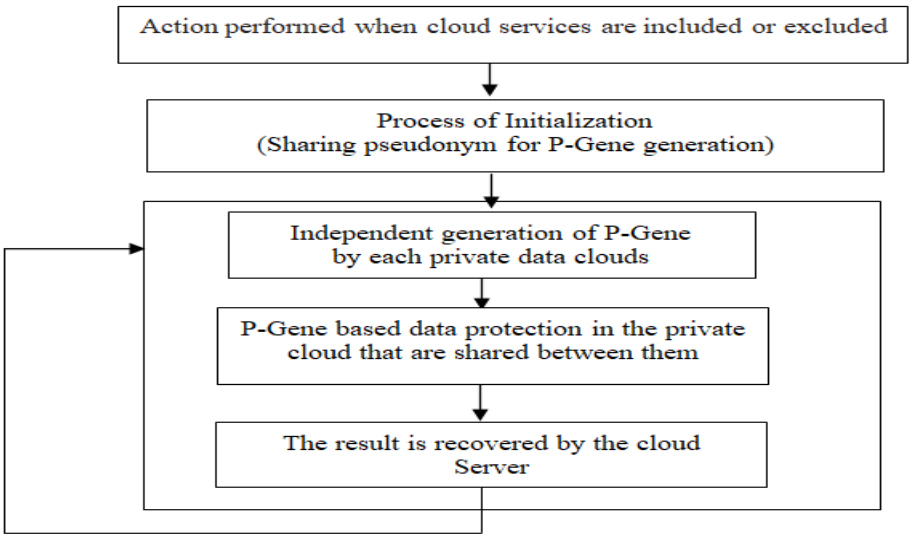

Figure 1-PRIAS-Generation of Pseudonym using P-Gene

Phase 1: PBPRF-Pseudonym Generation and Maintenance

In this phase of Pseudonym Generation and Maintenance in PBPRF, the privacy of private data clouds is investigated using three scenarios viz., i) Private data cloud members under interaction, ii) Failure of cloud interaction and iii) Addition of new private data clouds.

Scenario 1: Private data cloud members under interaction

In this scenario, the interacting private data clouds ' P ' and ' Q ' is responsible for randomly generating ' $k-1$ 'data as the new pseudonym through PS_Q^P. Then each encrypted PS_Q^P **is** forwarded to the interacting neighborhood private cloud ' Q ' based on the scheme of shared pair key $SPK_{(P,Q)}$. Similarly, the interacting private data cloud ' Q 'in turn receives the pseudonym PS_p^Q and shared pair key $SPK_{(Q,p)}$ from the private data cloud ' P '. In the second step, the interacting private data cloud' Q 'initializes the pseudonym table and stores the value of pseudonym PS_Q^P when the pseudonyms generated by the private data cloud ' P ' and ' Q 'are exchanged and it also updates the pseudonym received from other interacting private data clouds as shown in Table 1.

$SPK_{(Q,p)}$	1	2	….	k-1	k
PS_Q^P	PS_1^P	PS_2^P	·····	PS_{k-1}^P	PS_k^P
PS_p^Q	PS_1^Q	PS_2^Q	·····	PS_{k-1}^Q	PS_k^Q

Table 1: Pseudonym Table of PBPRF for private data cloud 'Q'

Scenario 2: Failure of cloud interaction

If the private data cloud ' P 'is notified about the failure of the interacting private data cloud ' Q ', then the cloud ' P removes the entry of cloud ' Q ', from its pseudonym table and similarly, If the private data cloud ' Q 'is notified about the failure of the interacting private data cloud ' P ', then the cloud ' Q removes the entry of cloud ' P ' from its pseudonym table

Scenario 3: Addition of new private data clouds

If the private data cloud ' P 'and ' Q 'is notified about the addition of an new interacting private data cloud ' R ', then the cloud ' P 'and ' Q ' updates the entry for cloud 'R' in their generated pseudonym tables and a pair of valid private cloud members (P, Q) generates and exchanges secret pseudonym . PS_Q^R and PS_P^R

Phase 2: PBPRF- Data recovering process

In this data recovery process of PBPRF, each of the private cloud member first checks whether all the participating cloud members have interacted and shared the data. If checking is confirmed, each of the cloud member computes $D=(\sum D_b)$ mod U 9 which is equivalent to the value of $\sum d_b$ and then it is utilized for sending {D,m} to the neighborhood interacting private data cloud. In contrast, if the confirmation of interaction is not delivered, for instance, if the cloud ' S ' is not reporting, then the private data cloud ' P ' asks the private data cloud ' Q ' to report regarding its interaction. If the private data cloud ' Q ' responds then the private data cloud ' P ' continues with the process of checking and P-Gene generation. Otherwise, the private data cloud ' Q ' is confirmed to be under failure and thus the interacting private data cloud ' P ' sends the P-Gene information to the other possible cluster cloud members for iterating phase -1 of Pseudonym Generation and Maintenance phase.

IV. SIMULATION RESULTS AND INFERENCES

The potential of PBPRF is compared with PRIAS and TPAAAS techniques using two libraries which are related to Pairing-Based Cryptography and GNU Multiple Precision Arithmetic. The experimental analysis of PBPRF is implemented using C coding, which is further investigated using Intel Pentium 2.70GHz processor with memory capacity of 4GB with the operating system Linux.

Initially, computation cost of the proposed PBPRF algorithm is compared with PRIAS and TPAAAS approaches and are presented in Figures 2, 3, 4, 5 and 6 for evaluating its effectiveness and efficiency. In this investigation, varying blocks of size from 100 to 10,000 are selected and the predominance of PBPRF, PRIAS and TPAAAS algorithms are compared. The execution phase and verification phase involved in computation is more potential in PBPRF algorithm in comparison to PRIAS and TPAAAS at the run time of PBPRF algorithm ranges from 0.0546s to 0.523s. The computation cost of PBPRF algorithm is very low for the time incurred in the generation and verification is very less.

The computation cost of PBPRF analyzed using integrity parameter of 0.2 is proving to be predominant by 35% and 38%, Further, the computation cost of PBPRF investigated under integrity parameters of 0.4 is confirmed to be predominant by 28% and 32% respectively.

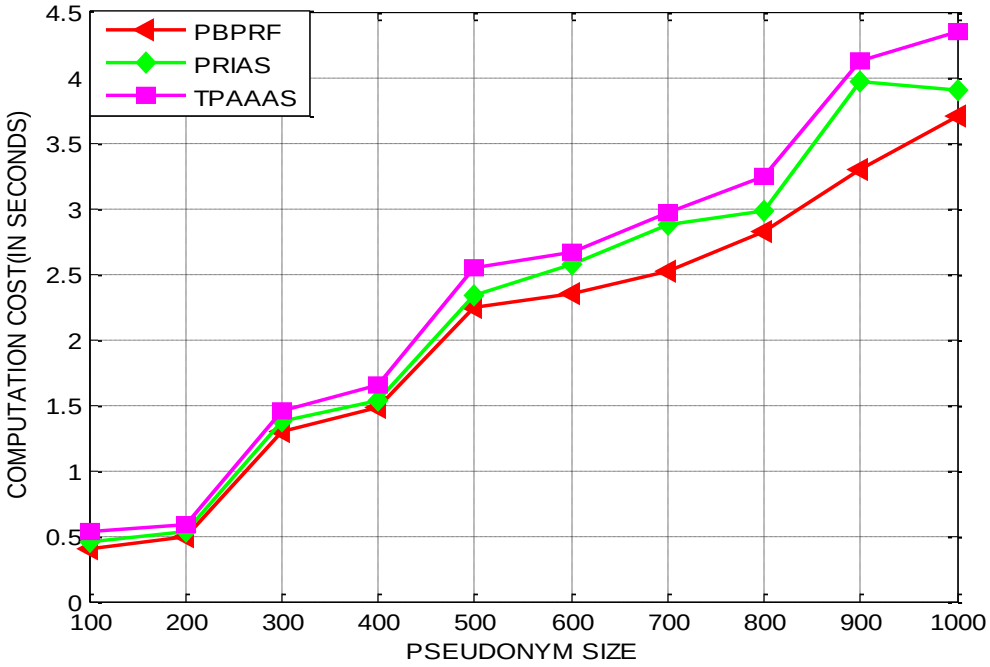

Figure 2 –PBPRF-computation cost-integrity parameter-0.2

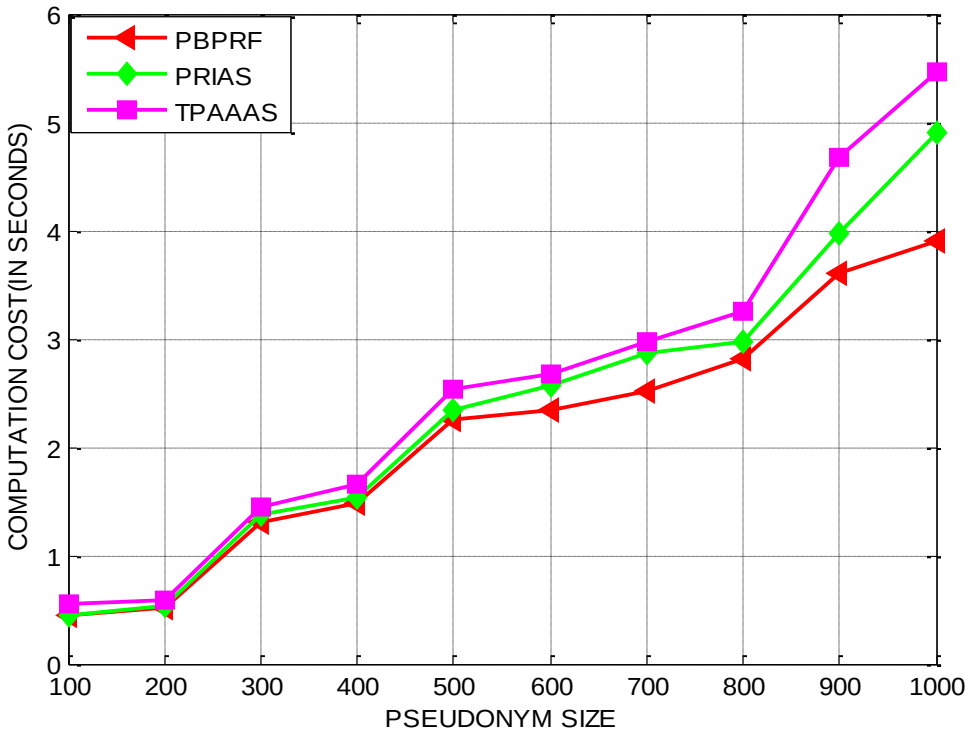

Figure 3 –PBPRF-computation cost-integrity parameter-0.4

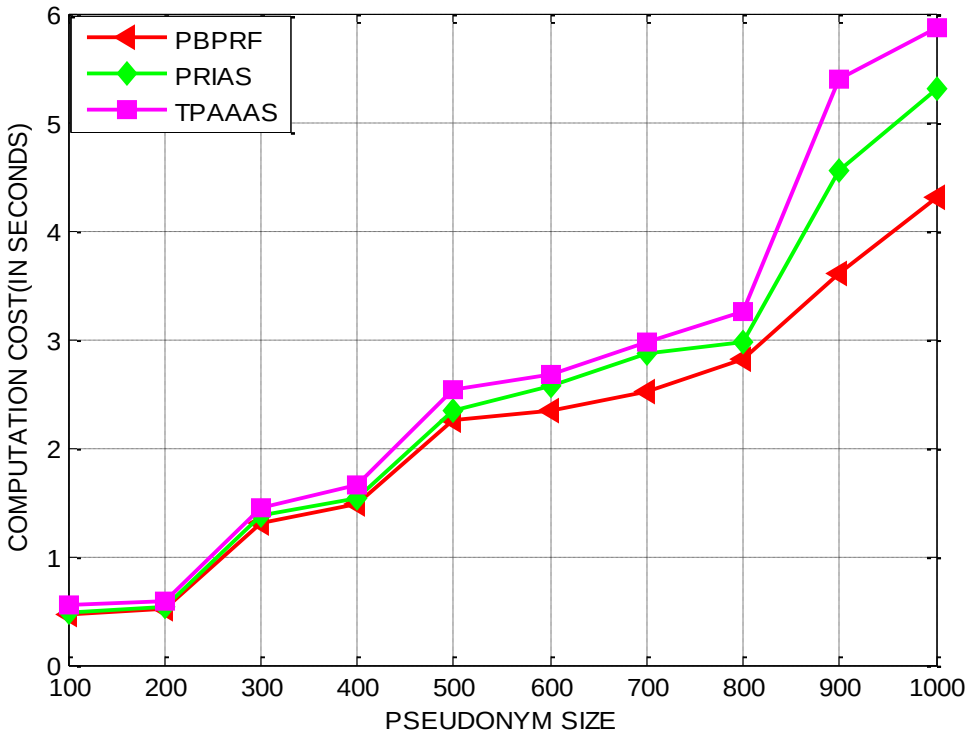

Figure 4 –PBPRF-computation cost-integrity parameter-0.6

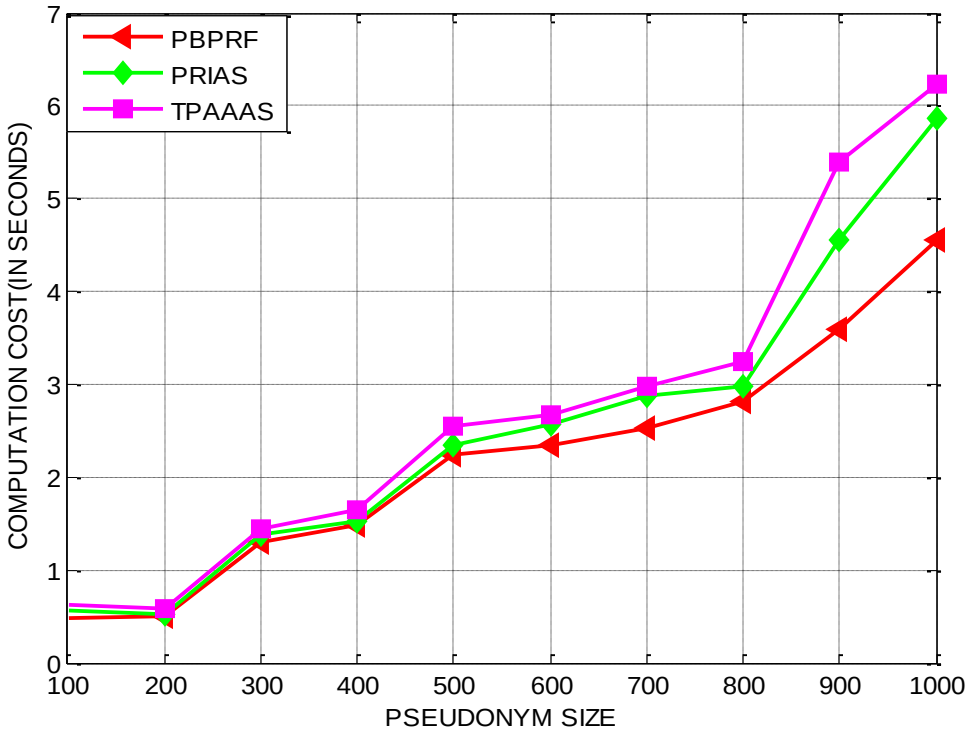

Figure 5 –PBPRF-computation cost-integrity parameter-0.8

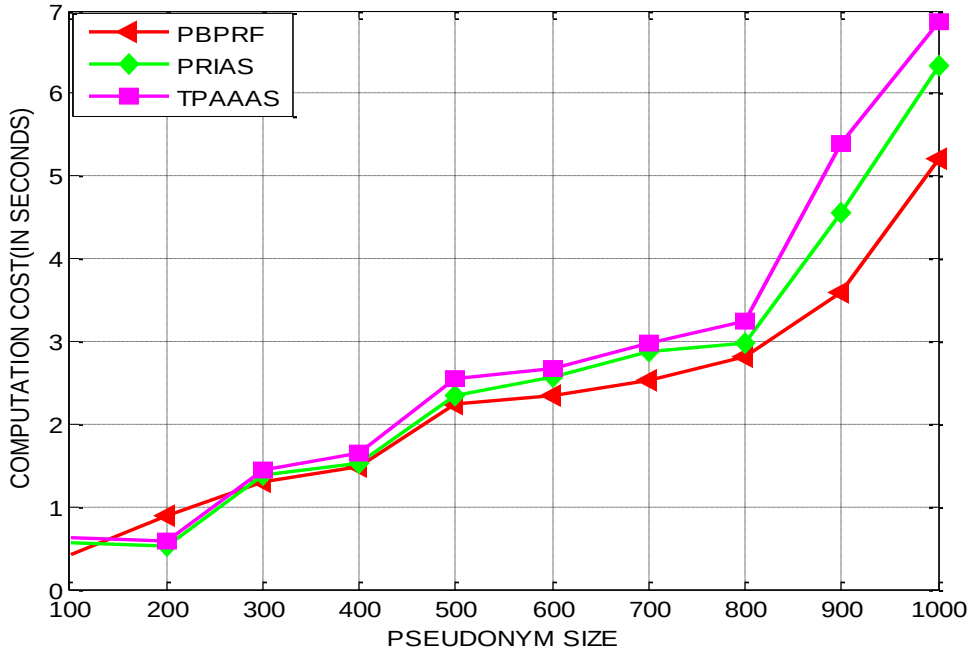

Figure 6–PBPRF-computation cost-integrity parameter-1.0

Furthermore, the computation cost of PBPRF investigated under integrity parameters of 0.6 is found to improve in an average by 25% and 28%. Likewise, the computation cost of PBPRF investigated under integrity parameters of 0.8 is proving to be better in an average by 16% and 19%. In addition, the computation cost of PBPRF investigated under integrity parameters of 1.0 is proving to be exceptional in an average by 12% and 15% than PRIAS and PAAAS schemes.

In the second level of experimental investigation, Figures 7, 8, 9, 10 and 11 presents the performance of PBPRF in terms of Pseudonym generation cost analyzed by varying the integrity parameter with increments of 0.2 from 0.2 to 1.0. The pseudonym generation cost of PBPRF is predominant to PRIAS and TPAAAS schemes as the pseudonym generation time used by PBPRF is comparatively less than the time incurred by PRIAS and TPAAAS techniques. The pseudonym generation cost of PBPRF analyzed using integrity parameter of 0.2 is proving to be predominant by 21% and 28% better to PRIAS and TPAAAS techniques.

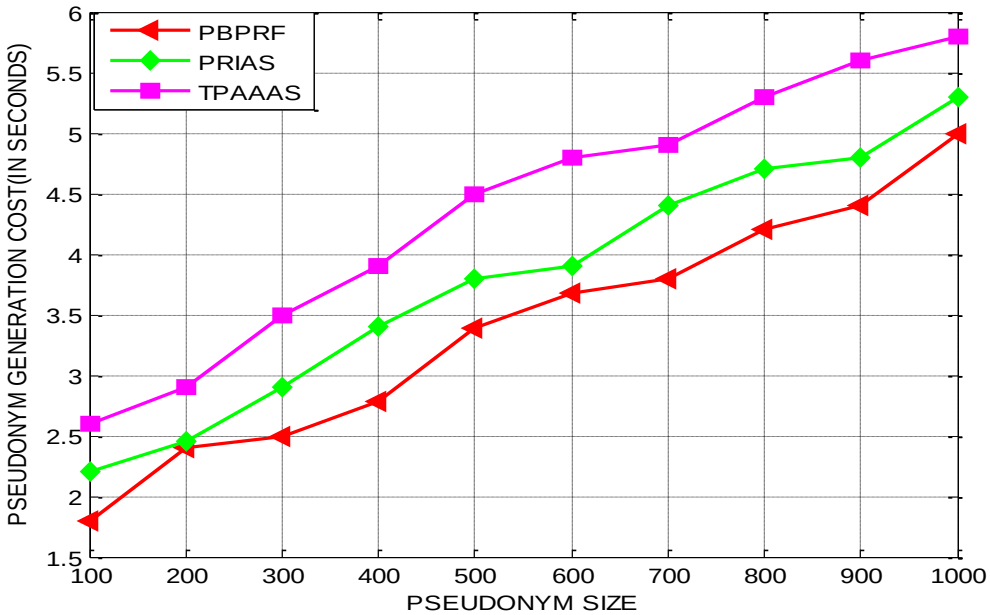

Figure 7 –PBPRF- Pseudonym Generation Cost-integrity parameter-0.2

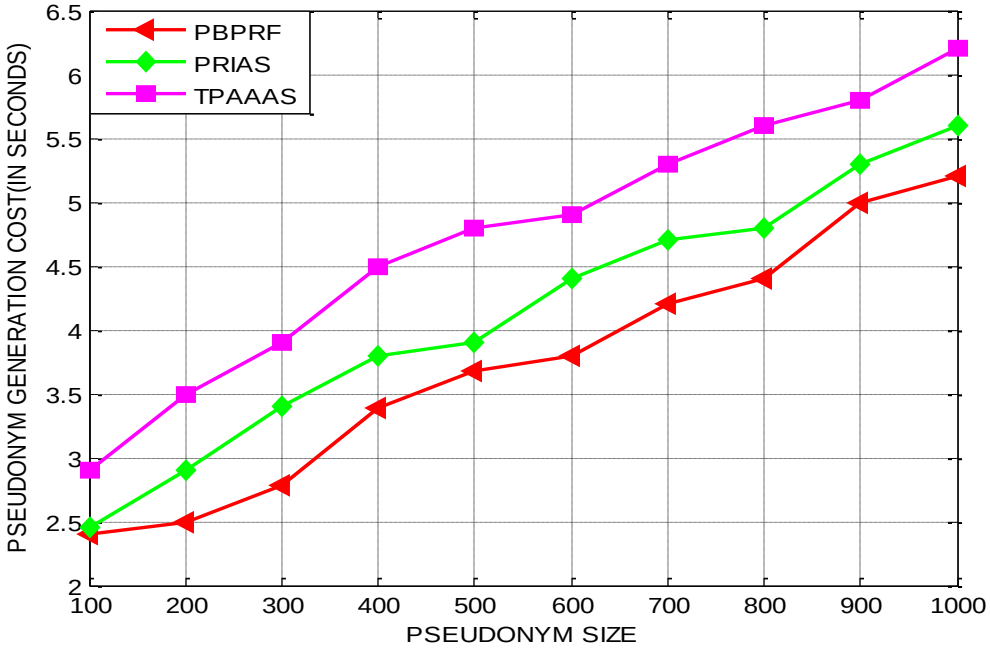

Figure 8 –PBPRF- Pseudonym Generation Cost-integrity parameter-0.4

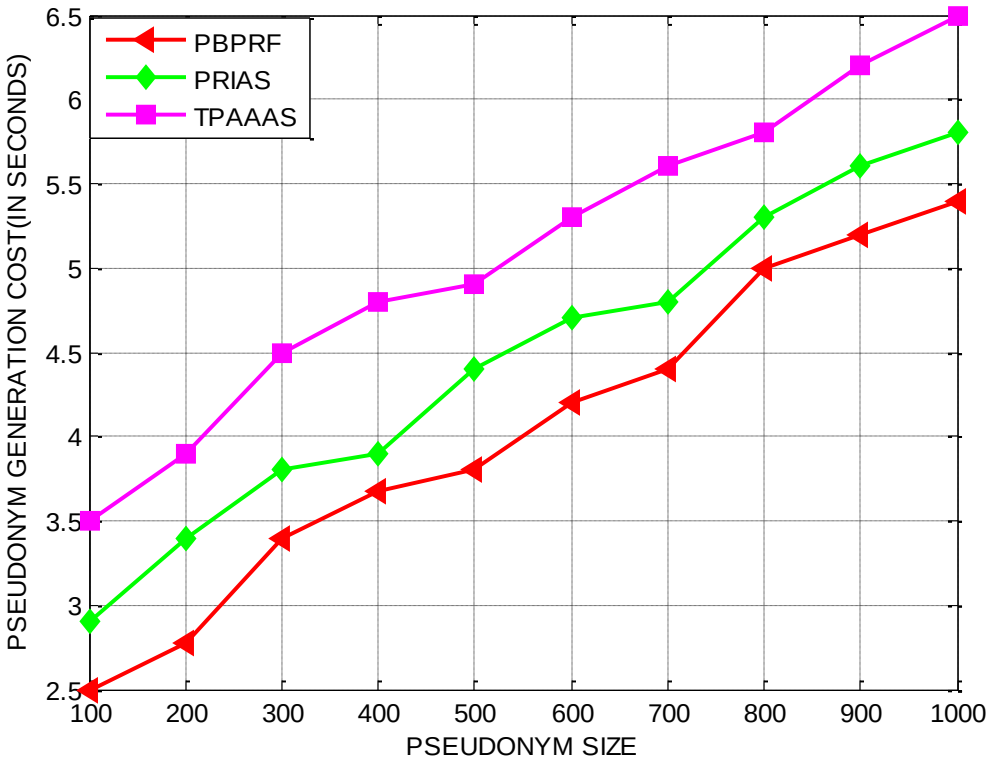

Figure 9 –PBPRF- Pseudonym Generation Cost-integrity parameter-0.6

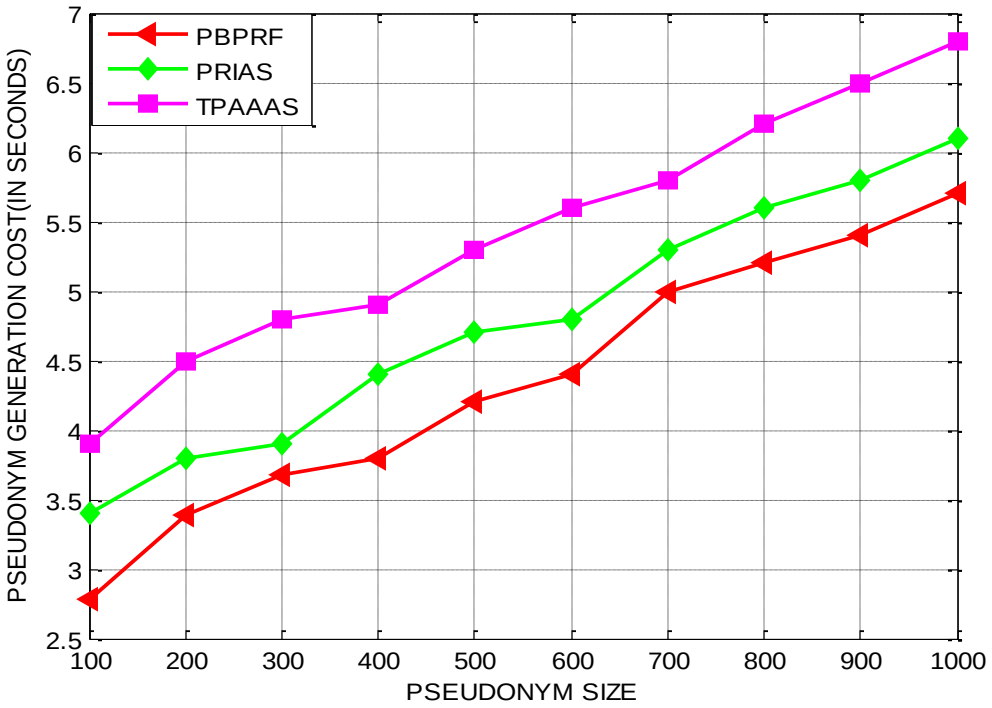

Figure 10 –PBPRF- Pseudonym Generation Cost-integrity parameter-0.8

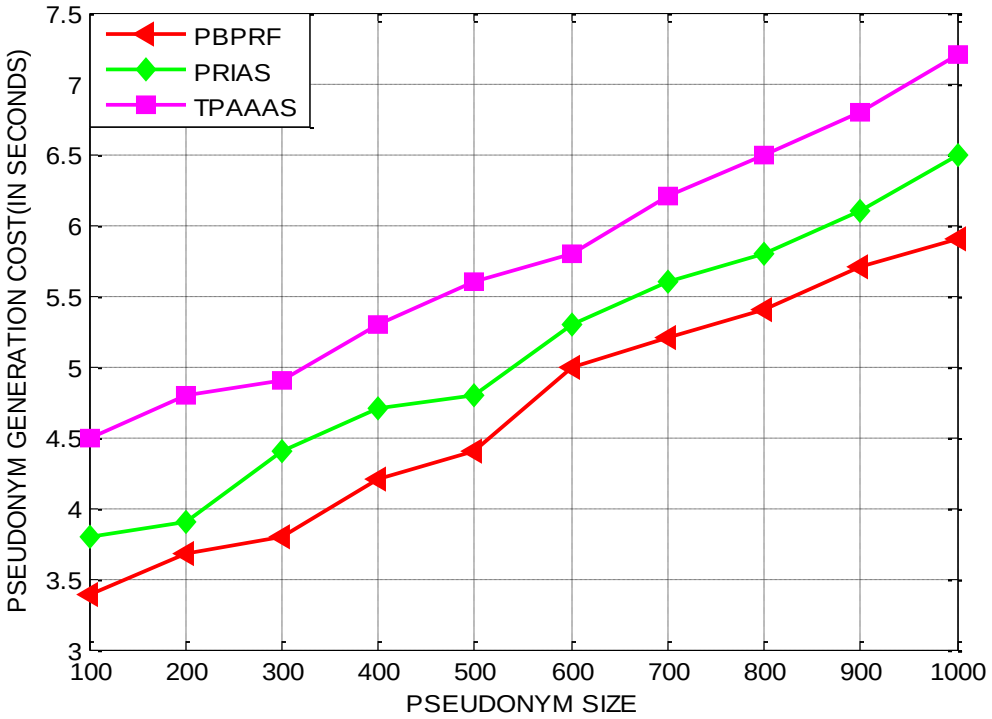

Figure 11 –PBPRF-Pseudonym Generation Cost-integrity parameter-1.0

Further, the pseudonym generation cost of PBPRF investigated under integrity parameters of 0.4 is confirmed to be predominant by 22% and 27% respectively. Furthermore, the pseudonym generation cost of PBPRF investigated under integrity parameters of 0.6 is found to improve in an average by 16% and 19%. Likewise, the pseudonym generation cost of PBPRF investigated under integrity parameters of 0.8 is proving to be better in an average by 10% and 12%. In addition, the pseudonym generation cost of PBPRF investigated under integrity parameters of 1.0 is proving to be exceptional in an average by 7% and 9% than PRIAS and TPAAAS schemes.

In addition, the significance of PBPRF in data privacy is investigated by comparison PRIAS and TPAAAS quantified using enhancement in accuracy and improvement in privacy preservation. Figure 12 and 13 portrays the predominant potential of PBPRF compared to PRIAS and TPAAAS based on accuracy as it uses the method of P-Gene for ensuring data accuracy. The improvement in accuracy of PBPRF is phenomenal and influential in both the case of separated and batched computation.

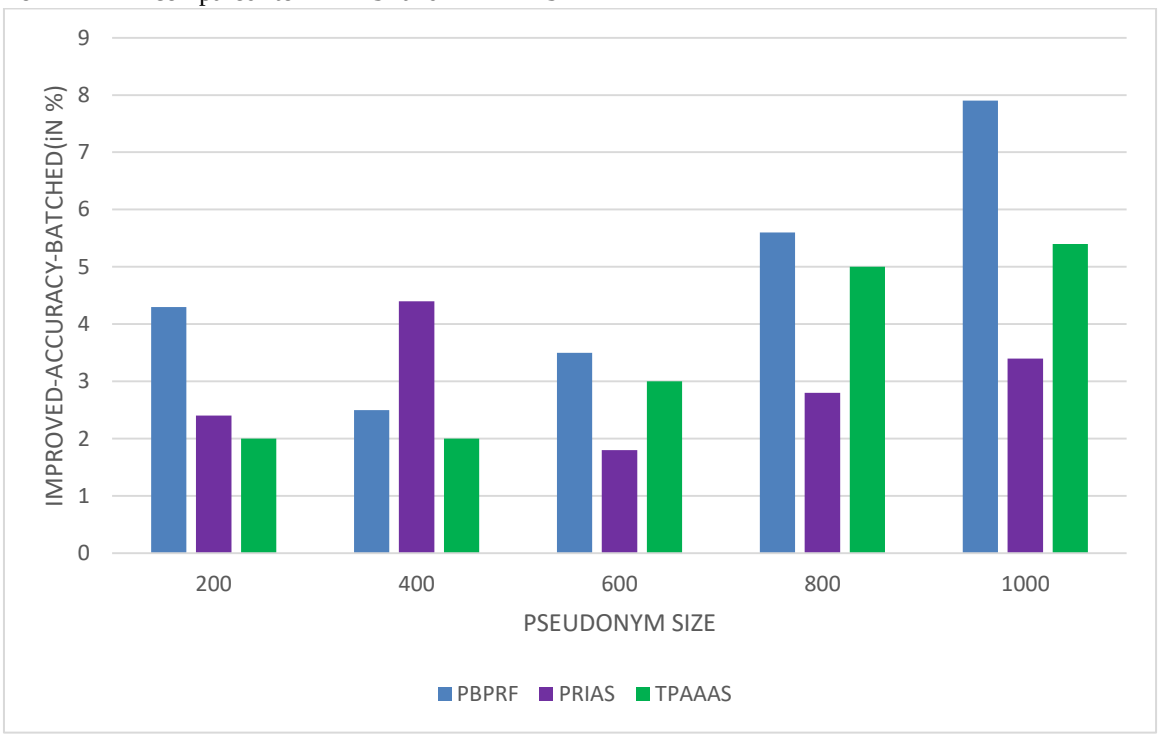

Figure 12 –PBPRF- Improved Accuracy-Batched

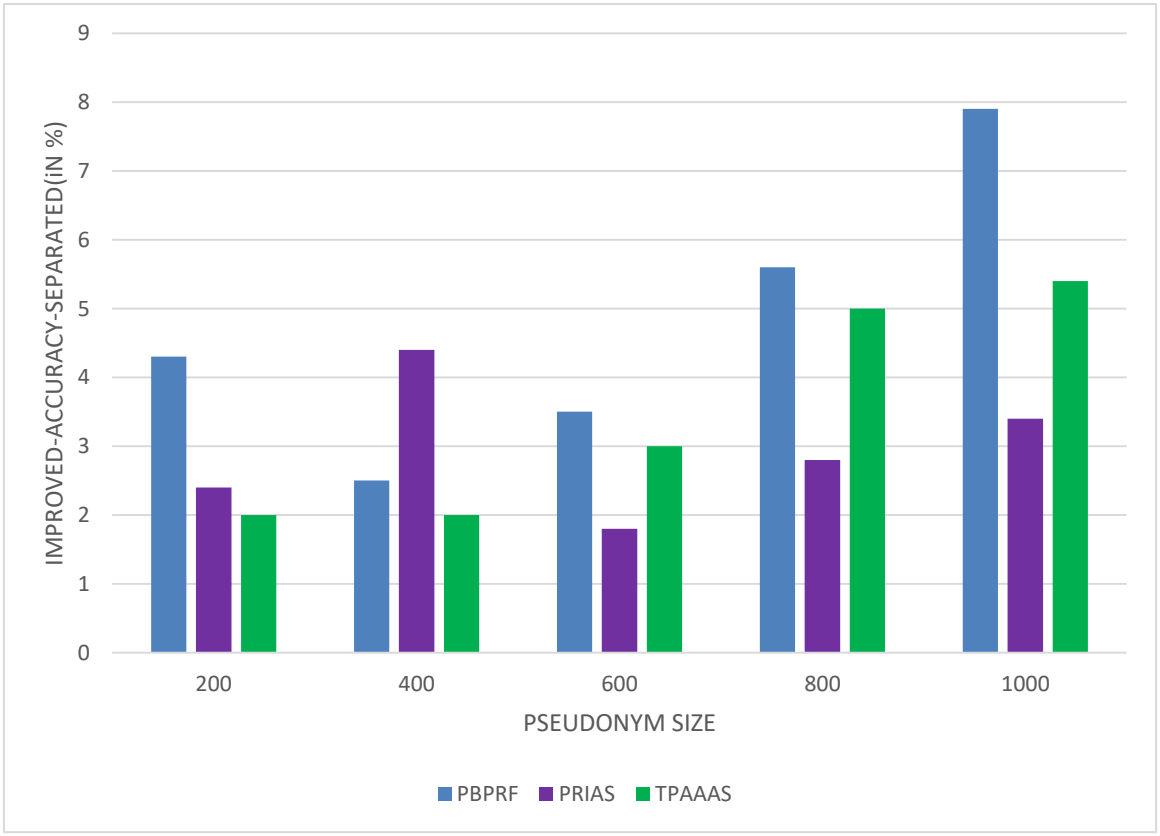

Figure 13 –PBPRF- Improved Accuracy-Separated

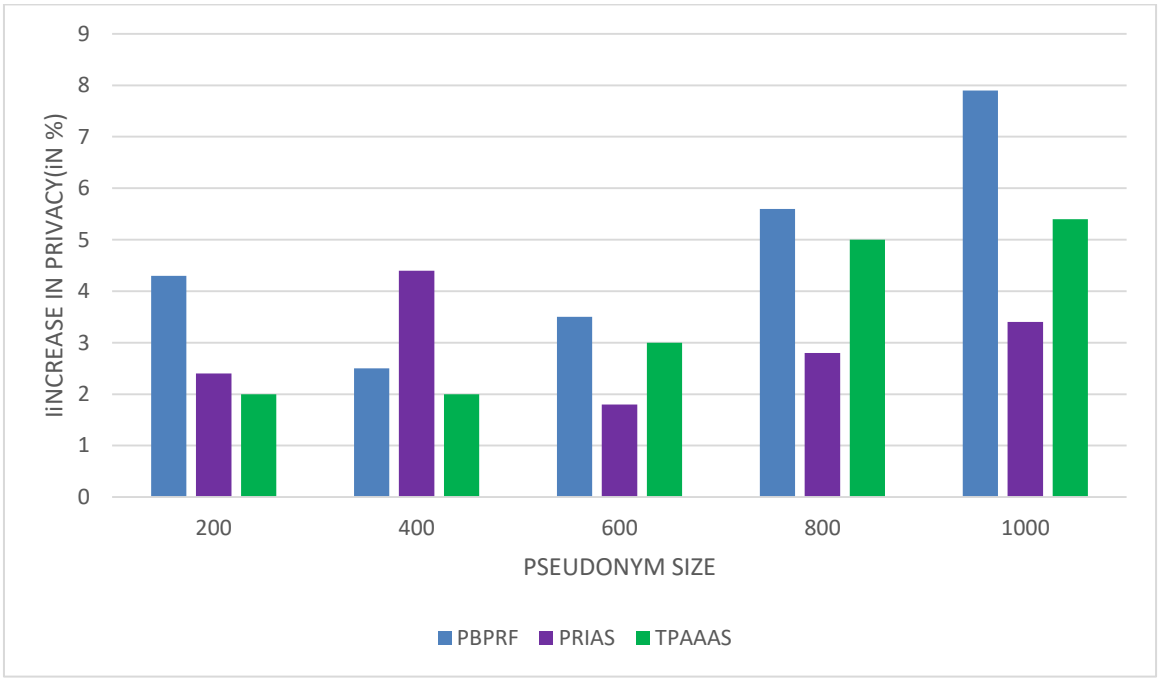

Figure 14 –PBPRF- Improved privacy-Batched

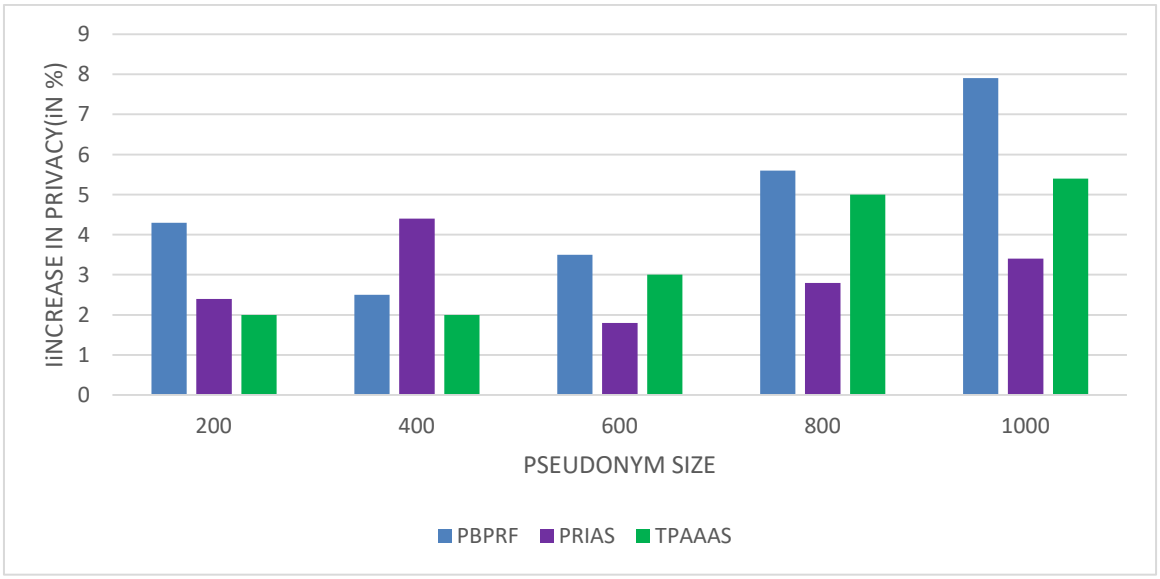

Figure 15 –PBPRF- Improved privacy-Separated

The proposed PBPRF is found to enhance the rate of accuracy under batched computation in an average by 8.95% and 9.45%. Similarly, PBPRF is also found to enhance the rate of accuracy under separated computation in an average by 8.97% and 9.35% compared to PRIAS and TPAAAS schemes. Figure 14 and 15 highlights the role of PBPRF compared to PRIAS and TPAAAS in preserving privacy under separated and batched computation. The improvement in privacy preservation of PBPRF seems to be phenomenal in both the case of separated and batched computation since it incorporates the scheme of P-Gene for enforcing data privacy preservation. PBPRF is found to enhance the rate of privacy under batched computation in an average by 6.55% and 6.98%. Similarly, PBPRF is also found to enhance the rate of privacy under separated computation in an average by 6.95% and 7.68% compared to PRIAS and TPAAAS schemes.

V. CONCLUSIONS

The proposed Pseudonym-Based Privacy and Reliability Framework (PBPRF) was propounded for securing and exchanging data by trusting upon P-Gene erasable data hiding approach. In PBPRF, the use of P-Gene in data security was responsible for reducing overhead under data sharing for ensuring reliable security of data through the hidden data technique made available to the user. The experimental investigation of PBPRF confirms its excellence over PRIAS and TPAAAS in preserving privacy under separated and batched computation.

The performance of PBPRF is found to enhance the rate of privacy under batched computation in an average by 6.55% and 6.98% and the improvement in accuracy of PBPRF is phenomenal and influential in both the case of separated and batched computation. PBPRF is found to enhance the rate of accuracy under batched computation in an average by 8.95% and 9.45% correspondingly

REFERENCES

1. Sarhan, A. Y., & Carr, S. (2017). A Highly-Secure Self-Protection Data Scheme in Clouds Using Active Data Bundles and Agent-Based Secure Multi-party Computation. *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*. *2*(1), 59-83.
2. Waters, B. (2011). Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization. *Public Key Cryptography – PKC 2011*, *1*(1), 53-70.
3. Balu, A., & Kuppusamy, K. (2014). An expressive and provably secure Ciphertext-Policy Attribute-Based Encryption. *Information Sciences*, *276*(2), 354-362.
4. Liang, X., Cao, Z., Lin, H., & Xing, D. (2009). Provably secure and efficient bounded ciphertext policy attribute based encryption. *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security - ASIACCS '09*, *1*(1), 56-87.
5. Yang, K., Jia, X., & Ren, K. (2013). Attribute-based fine-grained access control with efficient revocation in cloud storage systems. *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security - ASIA CCS '13*, *1*(2), 34-47.
6. Moataz, T., & Shikfa, A. (2013). Boolean symmetric searchable encryption. *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security - ASIA CCS '13*, *1*(2), 12-23.
7. Zhu, X., Liu, Q., & Wang, G. (2016). A Novel Verifiable and Dynamic Fuzzy Keyword Search Scheme over Encrypted Data in Cloud Computing. *2016 IEEE Trustcom/BigDataSE/ISPA*, *2*(1), 45-59.
8. Pei, X., Wang, Y., Yao, W., Lin, J., & Peng, R. (2016). Security Enhanced Attribute Based Signcryption for Private Data Sharing in Cloud. *2016 IEEE Trustcom/BigDataSE/ISPA*, *2*(1), 45-58.
9. Wang, S., Liang, K., Liu, J. K., Chen, J., Yu, J., & Xie, W. (2016). Attribute-Based Data Sharing Scheme Revisited in Cloud Computing. *IEEE Transactions on Information Forensics and Security*, *11*(8), 1661-1673.
10. Sundari S, & Ananthi M. (2015). Secure multi-party computation in differential private data with Data Integrity Protection. *2015 International Conference on Computing and Communications Technologies (ICCCT)*, *2*(1), 67-79.
11. Yang, K., & Jia, X. (2013). DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems. *Security for Cloud Storage Systems*, *2*(1), 59-83.
12. Chen, H. C., & Lee, P. P. (2014). Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage: Theory and Implementation. *IEEE Transactions on Parallel and Distributed Systems*, *25*(2), 407-416.
13. Yang, K., & Jia, X. (2014). Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage. *IEEE Transactions on Parallel and Distributed Systems*, *25*(7), 1735-1744.
14. Vidya, K., & Abinaya, A. (2015). Secure data access control for multi-authority Quantum based cloud storage. *2015 International Conference on Computing and Communications Technologies (ICCCT)*, *2*(1), 56-67.
15. Jianan Hong, Kaiping Xue, & Wei Li. (2015). Comments on "DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems"/Security Analysis of Attribute Revocation in Multiauthority Data Access Control for Cloud Storage Systems. *IEEE Transactions on Information Forensics and Security*, *10*(6), 1315-1317.
16. Srilakshmi, P. (2017). Data Access Control with Revocable Multi-authority Cloud Storage. *International Journal Of Engineering And Computer Science*, *2*(1), 67-78.
17. Krishna, M. B., & Krishna, M. S. (2017). Hierarchical Attribute Based Revocable Data Access Control For Multi Authority Cloud Storage. *IOSR Journal of Computer Engineering*, *19*(04), 91-97.
18. Patil, C. (2018). Securing Data and Providing Integrity over Cloud Storage. *International Journal for Research in Applied Science and Engineering Technology*, *6*(3), 938-940.