Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/13S123

An Effective Pseudonym-based Privacy Preservation Mechanism for Securing Services in Cloud Computing Environment

S. Bhaggiaraj[1,*] *and V. Sumathy*[2]

[1] Department of Information Technology,Sri Ramakrishna Engineering College, Coimbatore, India.
[2] Electronics and Communication Engineering , Government College of Technology, Coimbatore, India.

Received: 23 Jun. 2019, Revised: 13 Jul 2019, Accepted: 17 Jul. 2019
Published online: 1 Aug. 2019

Abstract: The cloud computing environment facilitates diversified number of potential services to its users such as the utilization-based pricing that is, every cloud provider has its own pricing scheme, on-demand service utilization and risk transference during the process of resource sharing. However, the security to cloud services during the event of data sharing is considered as the crucial task. In this paper, an Effective Pseudonym-based Privacy Preservation Mechanism (EP-PPM) is proposed for facilitating significant data sharing using the method of erasable data hiding. This EP-PPM approach utilizes the benefits of the P-Gene for hiding the data in order to prevent the overhead occuring during the process of data exchange provisioned between the cloud servers and its users. This EP-PPM scheme ensures secureness to the cloud services by periodic updating of pseudonym based on bilinear maps, that is shared between the interacting entities of the cloud environment. The simulation experiments and investigations of the proposed EP-PPM scheme evaluated, using the pseudonym generation and verification cost occuring in the process of securing cloud services, confirm a predominant improvement over the benchmarked security approaches of the literature. The percentage of privacy-preservation is calculated based on number of cloud service. As compared to the proposed EP-PPM scheme with existing IPN-PPM, P2E-CDSS and RDIC-PPM methods, the proposed method achieves the best results.

Keywords: Cloud computing, privacy preservation mechanism, cloud services

1 Introduction

Computing is the process of performing operations with the help of a machine called a computer. There are different types of computing theorems such as cloud computing [1,2,3,4], quantum computing [5,6,7,8], neural computing [9,10] and DNA computing [11,12]. Cloud Computing (CC) is a new service delivery and computational paradigm which provides virtualized and highly scalable resources through the internet. The virtualized service platform of the cloud has a large number of occupants by influencing various other environments like distributed computing paradigm, grid computing information systems infrastructures and service-oriented computing. All the aforementioned paradigms comprise of a wide-ranging collection of computers, mobile terminals, networking system, applications and storage resources [13]. This is referred to as Cloud Service Providers (CSP). The CSPs not only allows the client to acquire the services, but also facilitates the client to get the shared resources for lease. Some of the service providers are Microsoft, CloudSafe, IBM, Amazon, Google, Salesforce.com, GoGrid, Box.net, etc. The functionalities of CSP also include implementation of the economic scale for clients, balancing of work load for clients, and limited resource consumption to clients [14]. This infrastructure also permits the clients to contract out their own data to cloud data center for efficient handling of resources. In addition, cloud infrastructure also has lots of advantages which could be able to provide dynamic, flexible, effective and reliable services to its clients on-demand basis from anywhere and at any time. Even though, the cloud infrastructure possesses more advantages stipulation of these services with authentication, confidentiality, privacy, integrity and other security issues. The architecture of distributed-access control scheme for

* Corresponding author e-mail: baggiaraj.s@gmail.com

cloud computing is given in [28]. In cloud storage data integrity model is described [31]. The maximum probability of evolving to the most challenging issues is given in [15,16].

The very important challenge in the cloud infrastructure is the issues related to the Identity Access Management (IAM). The IAM refers to the concept of identifying the identity of the client with their credentials and management of data related to client credentials. IAM also refers to the issues related to the credentials of the cloud service authentication. The various problems related to data integrity, verification and privacy are also coming under the IAM. The main modules of IAM consist of identification and access control which are considered as premium concepts among the seven cloud securities. This identity authentication defines the basis for the access control and offers guaranteed services to the elements of the systems which also include clients and services in terms of integrity and privacy. In a similar way, the access control is defined as the service which decides whether to provide the service to the entity or not.The decision of providing and not providing service is based on the diversified cloud services and multiple clients [17]. Thus, it is clear that context privacy in the cloud remains indispensable and even though a number of privacy-preserving schemes is proposed for ensuring privacy. Third party auditing in multiple cloud storage scheme is given in [18]. The encryption and decryption based method for authentication that is given in [19]. Most of the proposed context privacy schemes cause more overhead in key management. Secured data access with privacy scheme is given in [23] and [24].

In this paper, EP-PPM is proposed for encouraging huge information sharing utilizing the technique of erasable data hiding. This proposed EP-PPM approach encourages the setting security in the additive data aggregation process depending on incorporation of the erasable data hiding technique. This proposed EP-PPM approach is additionally investigated depending on three logical measurements, for example, Number of private clouds and its services are interacting as a cluster, the failure of the private cloud and new private cloud with their services are included. RPPFSDS is also investigated based on computation cost of pseudonym generation and verification, improvement in data privacy and percentage improvement in privacy preservation (P2E-PPM)[30]. Security and privacy of cloud computing is given in [37]. RDIC-PPM is given in [39].

The rest of the segments are sorted out as, Section 2 describes potential contextual privacy preserving approaches contributed in the writing in the ongoing past. Section 3 talks about the significances of the EP-PPM scheme dependent on three setting-based investigations. The exploratory outcomes that affirm the novelty and efficacy of the proposed work over the benchmarked contextual approaches are investigated point by point in Section 4. Section **??** depicts the convincing explanation related to the noteworthy commitment of RPPDSDS.

2 Related Work

Since a decade, the issue of keeping up identity secret and getting to the resources in the anchored way has turned out to be more well known among scientists, academicians, and industrialists.

At first, Lin et al.[18] delineated a proof-based token issuing approach for the members to deal with the character verification with no confided in incorporated expert. The proposed security engineering represents an effective co-ordinative verification scheme which can be connected for cloud service protection. This scheme introduced an effective and confidential-preserving cumulative scheme that is highly flexible, dynamic confidential preserving key-management scheme. This scheme also finds an application in a cloud environment client's privacy.

At that point, Zhu et al.[19] presented an anchored, secret saving, and recognizable identification plan in order to facilitate secured communications among the members and validate the members dependence on obscurity. The creators additionally found an application to convey this work in any system by taking care of client's protection. Further, Bertino et al. [20] exhibited an identity management system for achieving intensive authentication and privacy in cloud infrastructure. The test of sharing the "Master Key Secret" has been tended to in this paper. They utilized an entity-based personality administration framework which handles the overseeing of various entities for computerized characters in cloud.

Further, Chen et al. [21] has proposed another work which ensures individual identifiable data. This paper exhibited a novel structure which fuses information mining ideas to foresee data advantage from the client's individual distinguishing proof data. Yang et al. [22] pooled the bunch of confirmation process with the character check and administration. This idea prompts viable communication for the validation and checking the scheme. They used the data of the scrambled information and different gatherings processing with the end goal to display a methodology for a character administration framework without a centralized operator. Sanka et al.[23] introduced a strategy alluded as SPICE for identity management, which fulfills unlinkability, delegatable confirmation, and different properties in distributed computing. These ideas are upheld for both access control and protection of privacy. They additionally introduced hybrid methods for consolidating various security level alongside access control with the end goal to propose a productive access control scheme in the cloud environment. At that point Goyal[24], Mon and Naing[25] presented a hierarchy-based encryption scheme and the encryption depends on the characteristics of the data. This plan gives fine access control to the

cloud infrastructure. They likewise prescribed a weighted parameter-based encryption scheme with cipher policy arrangement all together to keep the protection and honesty in the change of information. This hierarchy-based encryption scheme is one of the ABE-based access control plan in which the arrangement of encoded data are in the cloud. The customer set the weighted parameter for coordinating to the decode the mutual data. The strategies displayed so far guarantee security regarding information and it is not far as cloud infrastructure, cloud services such as resources, platforms, or interfaces.

Besides, Almutairi et al.[26] displayed a reliable distributed design for giving access control in the appropriate frameworks. These techniques consolidate the approaches of the software engineering and security to deal with the issues identified with security in cloud framework. They used blind signature in order to authenticate the outside of the confirmed conditions. This strategy offers confirmation and access control in a distributed domain which guarantees identification, authentication, accountability and differentiated access control technique. The Ruj et al.[27] used parameter-based signature to implement authentication and identity confidentiality and they introduced a novel protection privacy preserving authenticated access control scheme in which the decentralization and robustness prevent replay attacks and denial of service attacks.

Then, an Improved PetriNetwork-based Privacy Preserving Mechanism (IPN-PPM) was contributed for mitigating the trust of the cloud providers from the user perspective[28]. This IPN-PPM scheme interacts and cooperates with the privacy enforcing cohesion approach for deploying, promoting, and adapting the possibility of increasing the degree of data privacy. This IPN-PPM scheme also concentrates on the process of verifying and clinching the intrusion of confidential information in order to facilitate predominant performance in the cloud storage-based services. This IPN-PPM acts as the protecting guard that maintains high-level secrecy during the process of initiating cloud data services. In addition, Remote Data Integrity Checking-based Privacy Preserving Mechanism (RDIC-PPM) was propounded with the benefits of Pedersen Commitment Approach for resolving the problems of privacy [29]. This RDIC-PPM approach enables the users to receive the secret keys only when the significant attributes are determined by the interaction between the cloud users and services. The theoretical analysis of the RDIC-PPM approach confirmed the scalability, storage, computation, and scalability strength towards the security of the cloud services to a maximum degree. Finally, a Privacy Preserving and Effective Cloud Data Sharing Service (P2E-CDSS) was proposed for facilitating adaptive and efficient privacy preservation[30]. This P2E-CDSS incorporated an attribute-based encryption approach for facilitating superior ciphertext policy, such that data security is strengthened for succeeding privacy to a maximum level. This P2E-CDSS approach enforced full collision resistance and access control for better security in the interaction with the cloud services. The access policy of this P2E-CDSS approach was determined to be maximized in term of data privacy and privacy preservation rate.

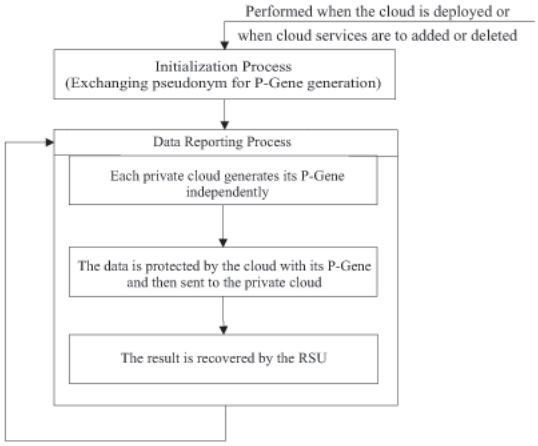

Fig. 1: P-Gene based Pseudonym

3 Reliable Privacy Preserving Framework for Securing Data Services (RPPFSDS)

RPPFSDS is the distributive scheme that ensures context privacy in the additive data aggregation process based on the erasable data hiding technique. Figure 1 describes the process of P-Gene generation and data encryption process. In this scheme, each private cloud perturbs its private data via its P-Gene without additional data exchange, and the aggregation result can be recovered from the hidden data in the P-Gene.

This erasable data hiding technique is incorporated in each cloud in order to hide its private data using a constructed P-Gene, and then sends the hidden data to the other interacting cloud. In this way, privacy can be ensured during the communication process.

3.1 Initialization Process for Pseudonym Generation and Maintenance:

The process of pseudonym generation and maintenance is analyzed through three cases:

Case 1: Number of private clouds is interacting as a cluster

1.Step 1: Initially each private cloud node b randomly generates $(n-1)$ data as pseudonym based on P_c^b.

Table 1: Pseudonym Table T_b of private cloud b

C	1	2	$\cdots$	$n-1$	N
P_c^b	P_1^b	P_2^b	$\cdots$	P_{n-1}^b	P_n^b
P_b^c	P_b^1	P_b^2	$\cdots$	P_b^{n-1}	P_b^n

Now each encrypted P_c^b is sent to the corresponding neighboring private cloud c through the use of shared pair wise key $S_{k(b,c)}$: $\{P_c^b\}_{S_{k(b,c)}}$. Likewise, the neighboring private cloud b receives pseudonym P_b^c from private cloud c.

2.Step 2: Once the pseudonym is exchanged, The private cloud b sets the pseudonym table that contains all of its generated pseudonym P_c^b and those that are received from the other private cloud members. The pseudonym Tb of private cloud 'b' is given in table 1.

Case 2: Cloud interaction fails When private cloud b is notified that its private cloud c fails, already interacting private cloud b deletes P_c^b and P_b^c from Table 1.

Case 3: New private clouds with its services are added When private cloud b is notified that new private cloud members have been added, assumed to be d. The private cloud b generates pseudonym P_d^b, which is then added to table T_b and sent to d : $P_d^b{}_{S_{k(b,c)}}$. Similar to **??**, each added private cloud member generates pseudonym for all other interacting private cloud members and then sends these pseudonym to the corresponding cloud cluster members. Each added private cloud member d also maintains its pseudonym table for P-Gene generation. After this process, each pair of valid private cloud members (b,c) only shares the two secret pseudonym, namely, $\{P_c^b, P_b^c\}$.

3.2 Data Verification Process:

The private cloud b collects data, hides its data through its P-Gene, and sends the hidden data to its interacting private cloud c. The cloud member b recovers the data after receiving all reports.

1.**Original data perturbation** According to pseudonym $\{P_c^b\}$, the private cloud b obtains all the P-pseudonym$(P-P_c^b)$, where each one is the lowest l bits of $T(P_c^b)$. Afterwards, node b calculates the P-Pseudonym is given by,

$$P - P_b^b = U - (\sum P_c^b) \mod U \tag{1}$$

According to the corresponding pseudonym $\{P_b^c\}$, private cloud b obtains all the P-pseudonym, $\{P_b^c\}$ which has the lowest l bits of $T(P_b^c)$. Thereafter, cloud member b calculates its P-Gene P_b according to $\{P_b^c\}$ is given by,

$$P - P^b = (\sum P_b^c) \mod U \tag{2}$$

Then the cloud member b hides its data with d^b and with P^b as $D^b = (d^b + P^b) \mod U$ and then it sends $\{D^b, b\}$ to its interacting clouds.

2.**Data recovering process in each cloud member** For each cloud member, the data recovering process checks if all the cloud members have sent their data.

(a)If so, each cloud member calculates $D = (\sum D_b) \mod U$, which is equivalent to $\sum d_b$ and then it sends $\{D, m\}$ to the next interacting cloud member.

(b)Otherwise, by assuming that the other interacting cloud c does not report, cloud member b asks c to report. If cloud c responds, cloud member b continues checking and calculating as (1). Otherwise, c is considered a failure and the cloud member b sends this information to the cluster members and this happens for each cloud member b, otherwise, this needs to execute 1.

4 Experimental Results

In this section, the significance of the proposed EP-PPM approach is investigated by conducting experiments using the Cloudsim simulator. The test bed used in the Cloudsim simulator must be modified with different number of pseudonyms, cloud services, and cloud users. The performance metrics considered for the investigation of the proposed EP-PPM approach are pseudonym generation cost, pseudonym verification cost, and percentage in data privacy in order to quantify its predominant role in securing cloud services in a predominant manner.

Initially, the predominance of the proposed EP-PPM approach is investigated using pseudonym generation cost, pseudonym verification cost and data privacy under a varying number of pseudonyms. Figure 2 depicts that the pseudonym generation cost of the proposed EP-PPM approach under an increasing number of pseudonyms is nearly 12%, 15%, and 17% minimized relative to the benchmarked IPN-PPM, P2E-CDSS and RDIC-PPM approaches. Similarly, Figure 3 proves that the pseudonym verification cost of the proposed EP-PPM approach under monotonically increasing pseudonyms is nearly 11%, 15%, and 18% reduced compared to the benchmarked IPN-PPM, P2E-CDSS and RDIC-PPM approaches. In addition, Figure 4 highlights that the percentage in data privacy of the proposed EP-PPM approach under the systematic increase of pseudonym count is approximately increased by 16%, 19%, and 22% superior to the benchmarked IPN-PPM, P2E-CDSS and RDIC-PPM approaches.

Further, the predominance of the proposed EP-PPM approach is investigated using pseudonym generation cost, pseudonym verification cost and data privacy under a varying number of cloud services. Figure 5 illustrates that the pseudonym generation cost of the proposed EP-PPM approach under an increasing number of cloud

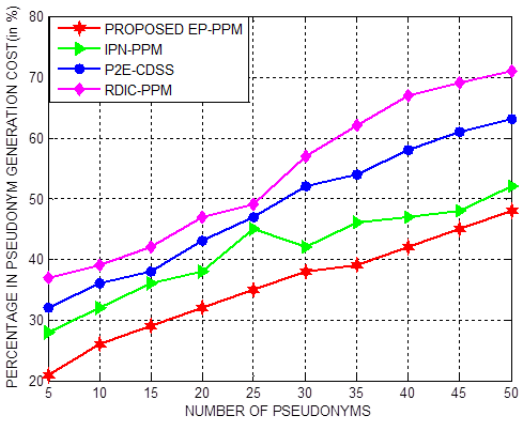

Fig. 2: Proposed EP-PPM-pseudonym generation cost versus number of pseudonyms

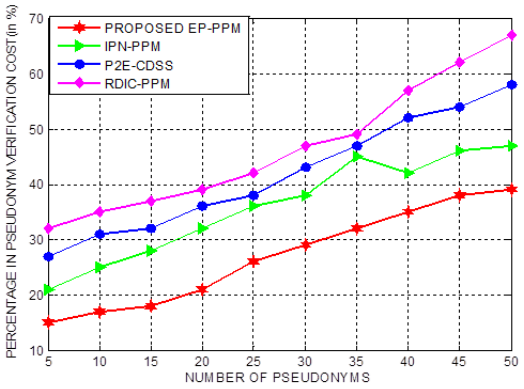

Fig. 3: Proposed EP-PPM-pseudonym verification cost versus number of pseudonyms

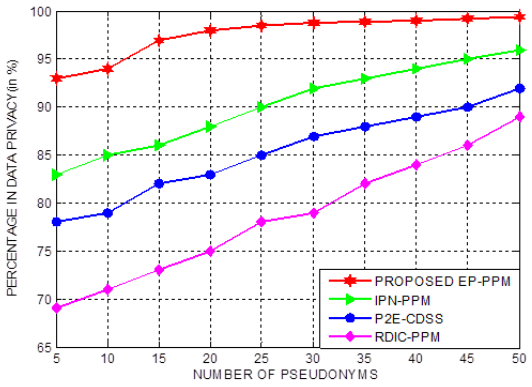

Fig. 4: Proposed EP-PPM-Percentage in data privacy and pseudonym count

services is nearly 10%, 13%, and 15% minimized relative to the benchmarked IPN-PPM, P2E-CDSS and RDIC-PPM approaches. Similarly, Figure 6 confirms that the pseudonym verification cost of the proposed EP-PPM approach under monotonically increasing cloud services is nearly 8%, 10%, and 13% reduced compared to the benchmarked IPN-PPM, P2E-CDSS and RDIC-PPM approaches. In addition, Figure 7 highlights that the percentage in data privacy of the proposed EP-PPM approach under the systematic increase of cloud services is approximately increased by 14%, 17%, and 19% superior to the benchmarked IPN-PPM, P2E-CDSS and RDIC-PPM approaches.

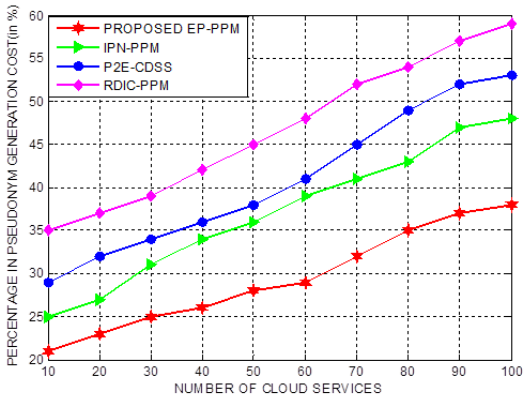

Fig. 5: Proposed EP-PPM-pseudonym generation cost versus number of cloud services

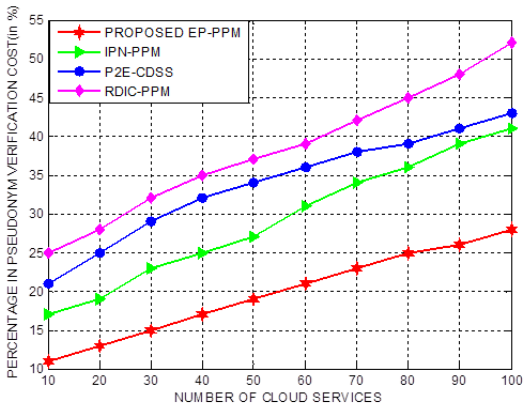

Fig. 6: Proposed EP-PPM-pseudonym verification cost versus number of cloud services

Furthermore, the potential of the proposed EP-PPM approach is investigated using pseudonym generation

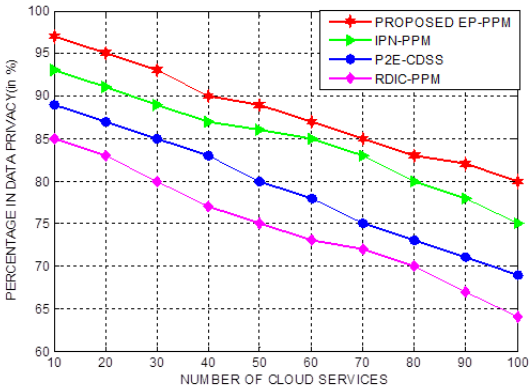

Fig. 7: Proposed EP-PPM-Percentage in data privacy versus number of cloud services

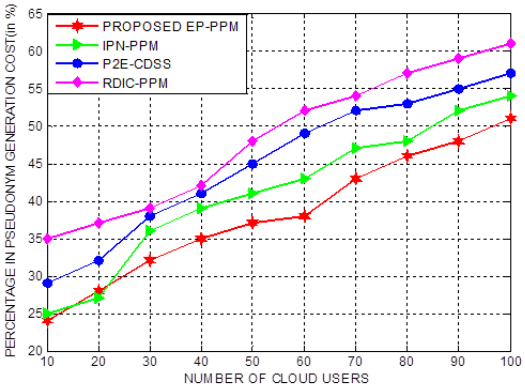

Fig. 8: Proposed EP-PPM-pseudonym generation cost versus number of cloud users

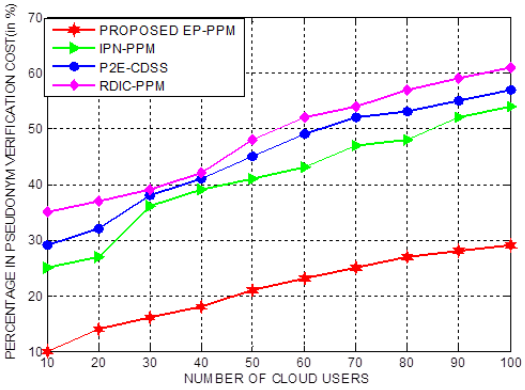

Fig. 9: Proposed EP-PPM-pseudonym verification cost versus number of cloud users

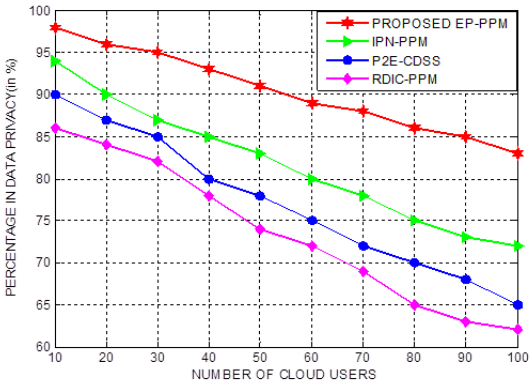

Fig. 10: Proposed EP-PPM- Percentage in data privacy versus number of cloud users

cost, pseudonym verification cost and data privacy under a varying number of cloud users. Figure 8 depicts that the pseudonym generation cost of the proposed EP-PPM approach is nearly 15%, 18%, and 21% minimized relative to the benchmarked IPN-PPM, P2E-CDSS, and RDIC-PPM approaches. Similarly, Figure 9 indicates that the pseudonym verification cost of the proposed EP-PPM approach is nearly 10%, 13%, and 16% reduced compared to the benchmarked IPN-PPM, P2E-CDSS and RDIC-PPM approaches. In addition, Figure 10 highlights that the percentage in data privacy of the proposed EP-PPM approach is nearly 13%, 16%, and 18% superior to the benchmarked IPN-PPM, P2E-CDSS and RDIC-PPM approaches.

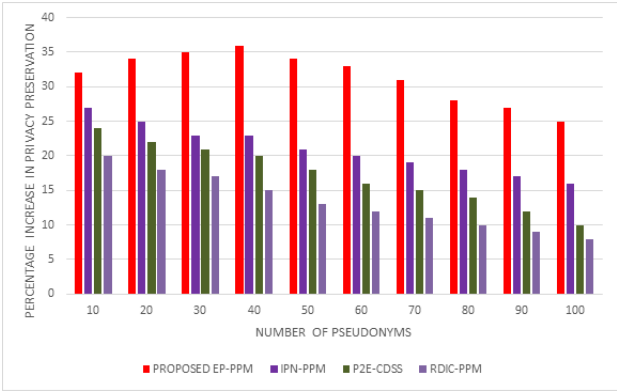

Fig. 11: Proposed EP-PPM - Percentage Improvement in privacy preservation (number of pseudonyms)

Finally, Figures 11 and 12 highlight the predominance of the proposed EP-PPM which is evaluated under the percentage improvement in privacy preservation under a number of pseudonyms and number of cloud services.

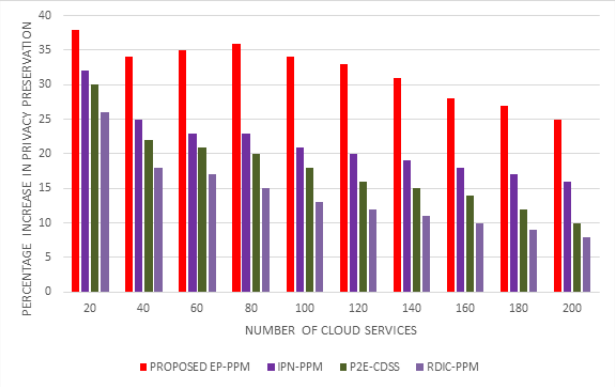

Fig. 12: Proposed EP-PPM- Percentage Improvement in privacy preservation (number of cloud services)

The mean percentage improvement in privacy preservation of the proposed EP-PPM approach under varying cloud users is determined to be 8%, 10%, and 13% superior over the compared IPN-PPM, P2E-CDSS, and RDIC-PPM approaches under its implementation under the varying number of pseudonyms. Likewise, the mean percentage improvement in privacy preservation of the proposed EP-PPM approach under varying cloud users is determined to be 6%, 9% and, 23% superior over the compared IPN-PPM, P2E-CDSS, and RDIC-PPM approaches under its implementation under the varying number of cloud services. This significant improvement in the mean privacy preservation rate under different number of pseudonyms and cloud services is mainly due to the utilization of p-Gene erasure technique incorporated in the proposed EP-PPM scheme.

5 Perspective

In this paper, EP-PPM has been presented for sharing and securing data that relies on erasable data hiding technique. In this proposed EP-PPM, private data in the cloud space is secured based on the benefits of P-Gene that reduces overhead in data exchange and ensures the possibility of sending the hidden data to the interacting users. The simulation results of the proposed EP-PPM prove that it is the predominant privacy-preserving technique in comparison with IPN-PPM, P2E-CDSS, and RDIC-PPM as it uses a reduced computational complexity which is approximately 18.5% greater than the baseline techniques. The pseudonym generation and pseudonym verification time handled by the proposed EP-PPM is also found to increase by 9.25% and 8.75% on being compared to the benchmark privacy-preserving schemes considered for comparison. The percentage of improvement in privacy preservation is calculated based on number of cloud services used in proposed EP-PPM. The proposed method achieves the best result as compared to the recent related literatures.

References

[1] Y.Duan, G. Fu, N. Zhou, X. Sun, N. Narendra, B. Hu, Everything as a Service (XaaS) on the Cloud: Origins, Current and Future Trends, 2015 IEEE 8th International Conference on Cloud Computing. IEEE, ISBN 978-1-4673-7287-9, pp. 621628, 2015 doi:10.1109/CLOUD.2015.88.

[2] G. von Laszewski, J. Diaz, F. Wang and G. C. Fox, Comparison of Multiple Cloud Frameworks, 2012 IEEE Fifth International Conference on Cloud Computing, Honolulu, HI, pp. 734-741, 2012, doi: 10.1109/CLOUD.2012.104

[3] S.He, L. Guo, Y. Guo, M. Ghanem, Improving Resource Utilisation in the Cloud Environment Using Multivariate Probabilistic Models, 2012 2012 IEEE 5th International Conference on Cloud Computing (CLOUD). pp. 574581, 2012

[4] M. Mao, M. Humphrey, A Performance Study on the VM Startup Time in the Cloud, Proceedings of 2012 IEEE 5th International Conference on Cloud Computing (Cloud2012), pp. 423, ISBN 978-1-4673-2892-0, 2012, doi:10.1109/CLOUD.2012.103.

[5] M. Abdel-Aty, Quantum information entropy and multi-qubit entanglement, Progress in Quantum Electronics, 31(1), pp. 1-49, 2007

[6] M. Abdel-Aty, An investigation of entanglement and quasiprobability distribution in a generalized JaynesCummings model, Journal of Mathematical Physics 44(4), pp. 1457-1471, 2003

[7] N. Metwally, M. Abdelaty, A.-S.F Obada, Entangled states and information induced by the atom-field interaction, Optics Communications 250(1-3), pp. 148-156, 2005

[8] M. Zidan, A.-H. Abdel-Aty, M. El-shafei, M. Feraig, Y. El-Abou, H. Eleuch and M. Abdel-Aty, Quantum Classification Algorithm Based on Competitive Learning Neural Network and Entanglement Measure, Appl. Sci., 9, 1277, 2019.

[9] A. Sagheer, M. Zidan and M. M. Abdelsamea, A Novel Autonomous Perceptron Model for Pattern Classification Applications, Entropy, 21(8), 763, 2019.

[10] M. Zidan, A. Sagheer and N. Metwally, An Autonomous Competitive Learning Algorithm using Quantum Hamming Neural Networks, In Proceedings of the 2015 International Joint Conference on Neural Networks (IJCNN), Killarney, Ireland, pp. 1–7, 2015.

[11] M. Ogihara and A. Ray, Simulating Boolean circuits on a DNA computer, Algorithmica 25:239250, 1999.

[12] Y. Benenson, B. Gil, U. Ben-Dor, R. Adar, E. Shapiro, An autonomous molecular computer for logical control of gene expression, Nature. 429 (6990): 423429, 2004.

[13] N. Lee and Y. Chang, Hybrid Provable Data Possession at Untrusted Stores in Cloud Computing. 2011 IEEE 17th International Conference on Parallel and Distributed Systems, **1(2)**, 23-35 (2011).

[14] Boyang Wang, Baochun Li and Hui Li, Oruta: privacy-preserving public auditing for shared data in the cloud. IEEE Transactions on Cloud Computing, **2(1)**, 43-56 (2014).

[15] B. Wang, H. Li and M. Li, Privacy-preserving public auditing for shared cloud data supporting group dynamics, 2013 IEEE International Conference on Communications (ICC), **2(2)**, 11-18 (2013).

[16] Y. Yu, J. Ni, M. H. Au, Y. Mu, B. Wang and H. Li, Comments on a Public Auditing Mechanism for Shared Cloud Data Service, IEEE Transactions on Services Computing, **8(6)**, 998-999 (2015).

[17] T. E. Trueman and P. Narayanasamy, Ensuring Privacy and Data Freshness for Public Auditing of Shared Data in Cloud, 2015 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), **1(2)**, 23-31 (2015).

[18] M. Shashidhara and C.P. Jain, Privacy Preserving Third Party Auditing in Multi Cloud Storage Environment, 2014 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), **1(1)**, 34-42 (2014).

[19] Y. Zhang, X. Chen, J. Li, D. S. Wong and H. Li, Anonymous attribute-based encryption supporting efficient decryption test, Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security - ASIA CCS '13, **2(2)**, 13-21 (2013).

[20] E. Bertino, P. A. Bonatti and E. Ferrari, TRBAC: A Temporal Role-based Access Control Model, ACM Transactions on Information and System Security, **4(3)**, 191-233 (August 2001).

[21] K. Y. Chen, C. Y. Lin and T. W. Hou, The Low-Cost Secure Sessions of Access Control Model for Distributed Applications by Public Personal Smart Cards, Proceedings of the 17th IEEE International Conference on Parallel and Distributed Systems, 894-899 (December 2011).

[22] K. Yang and X. Jia, Attribute-based Access Control for Multi-Authority Systems in Cloud Storage, Proceedings of the 32nd IEEE International Conference on Distributed Computing Systems, 536- 545, (2012).

[23] S. Sanka, C. Hota and M. Rajarajan, Secure Data Access in Cloud Computing, Proceedings of the 4th IEEE International Conference on Internet Multimedia Services, (December 2010).

[24] E. E. Mon and T. T. Naing, The Privacy-aware Access Control System using Attributed-and Role based Access Control in Private Cloud, Proceedings of the 4th IEEE International Conference on Broadband Network and Multimedia Technology, 447-451 (October 2011).

[25] V. Goyal, O. Pandey, A. Sahai and B. Waters, Attribute-based Encryption for Fine-Grained Access Control of Encrypted Data, Proceedings of the 13th ACM Conference on Computer and Communications Security, 89-98 (2006).

[26] A. Almutairi, Abdul Rahaman and Muhammad I. Sarfraz, Saleh Basalamah, Walid G. Aref Ghafoor, A distributed access control architecture for cloud computing, IEEE, 36-44 (2012).

[27] S. Ruj, A. Nayak and I. Stojmenovic, DACC: Distributed Access Control in Clouds, Proceedings of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 91-98 (2011).

[28] D. Chandramohan, T. Vengattaraman, D. Rajaguru and P. Dhavachelvan, A new privacy preserving technique for cloud service user endorsement using multi-agents, Journal of King Saud University - Computer and Information Sciences, **28(1)**, 37-54 (2016).

[29] J. Chen and H. Ma, Privacy-Preserving Decentralized Access Control for Cloud Storage Systems, 2014 IEEE 7th International Conference on Cloud Computing, **1(2)**, 45-56 (2014).

[30] Xin Dong, Yu Jiadi, Yuan Luo, Yingying Chen, Guangtao Xue and Minglu Li, P2E: Privacy-preserving and effective cloud data sharing service, 2013 IEEE Global Communications Conference (GLOBECOM), **1(1)**, 45-59 (2013).

[31] B Priyadharshini and P Parvathi. Data Integrity in cloud storage. 2012 IEEE Inter, conf. on Advances in Engineering, Science and Management. **June 2012**.

[32] Jian Shen, Tianqi Zhou, Debiao He, Yuexin Zhang, Xingming Sun, and Yang Xiang. Block Design-based key agreement for Group Data Sharing in Cloud Computing. IEEE Transaction on Dependable and Secure Computing. **July 2017**; 1-15.

[33] David S. Linthicum. Emerging Cloud Patterns. IEEE Cloud Computing. 2016; **3(1)**: 88-91.

[34] Kan Yang, Xiaohua Jia and Kui Ren. Secure and Verifiable Policy update outsourcing for Big Data Access control in cloud. IEEE Transactions on Parallel and Distributed Systems. 2015; **26(12)**: 3461-3470.

[35] Luo Yuchuan, Fu Shaojing, Xu Ming, and Wang Dongsheng. Enable data dynamics for algebraic signatures based remote data possession checking in the cloud storage. China Communications. 2014; **11(11)**: 114-124.

[36] Henry Chang. Privacy Regulatory Model for the Cloud: A Case Study. IEEE Cloud Computing. 2015; **2(3)**: 67-72.

[37] Zahir Tari. Security and Privacy in Cloud Computing. IEEE Cloud Computing. 2014; **1(1)**: 54-57.

[38] Hongli Zhang Zhigang Zhou, Lin Ye, and Xiaojiang Du. Towards Privacy Preserving publishing of Set-Valued Data on Hybrid Cloud. IEEE Transactions on Cloud Computing. 2018; **6(2)**: 316-329.

[39] Jining Zhao, Chunxiang Xu, Fagen Li, and Wenzheng Zhang. Identity-based public verification with privacy-preserving for data storage securing in cloud computing. IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences. 2013; **96(12)**: 2709-2716.

[40] Bin Liu, Yurong Jiang, Fei Sha, Ramesh Govindan. Cloud-Enabled Privacy-Preserving Collaborative Learning for Mobile Sensing. Proceedings of the 10th ACM conference on Embedded Network Sensor systems. **November 2012**. 57-70.

S. Bhaggiaraj obtained his Bachelor of Technology Degree in Information Technology from Vellore Institute of Technology, Vellore (formerly called as Vellore Engineering College, Vellore) in the year 2004. He obtained his Master of Engineering Degree in VLSI Design from Government College of Technology, Coimbatore in the year 2009. He is currently working as Assistant Professor in Information Technology department, Sri Ramakrishna Engineering College, Coimbatore and doing research in Cloud Security under the erstwhile Anna University of Technology Coimbatore, currently Anna University, Chennai. He is specialized in the area of Cloud computing, Network security, VLSI Design, Service Oriented Architecture, Sensor network and Embedded System. He has 11 years of academic experience. He has participated in various seminars, workshop, and national conferences and attended Faculty Development Programme and published six papers in International Journals. He is an active member in various Professional bodies like ISTE, ISSE, IACSIT and IAENG.

V. Sumathy obtained her Bachelor of Engineering Degree in Electronics and Communication Engineering in the year 1988, and Master Degree in Computer Science and Engineering from Government College of Technology, Coimbatore in the year 2000. She received Doctoral Degree from Anna University, Chennai in the year 2007. She is currently working as Professor and Head in Electronics and Communication Engineering department, Government College of Engineering, Bodinayakannur. She is specialized in the area of Adhoc Network, Sensor Network, Embedded Systems and Cloud computing. She has 25 years of academic experience. She has Guided 6 Research scholars and 5 ongoing research scholars. She has received Rs15 Lakhs from DST for the project proposal and also mentor for the project. She has visited Michigan State University, USA for Collaborative Research work in the area of Sensor Networks during the year 2014.She has published 32 papers in national and international journals.