Step2: If items appear at least K times in generalized tree (DC) then (C,SD) is a valid solution.
Step3: If items does not appear at least K times in generalized tree (DC) then (C,SD) is not a valid solution.
Step4: If solution is invalid then cannot prepare projected Synopsis tree.
Step5: If solution is Valid then prepare projected Synopsis tree which is used in structure Check.

6.3 FixStructure Check

Step1: Collect all id's from sidelink list of projected synopsis tree.
Step 2: Check all possible combinations of size m and all sets of relation between them up to size n.
Step 3: If node satisfy these m size combination and n size relation between them, then solution guarantees k(m,n) anonymity for D.

7. Performance Evaluation

Performance is evaluated by comparing domain model and contextualized generalization cut.

Figure 3: Execution time

Execution time of old domain model and new contextualized generalization model is calculated and as shown in fig 3 less time is required to run by using contextualized generalization.

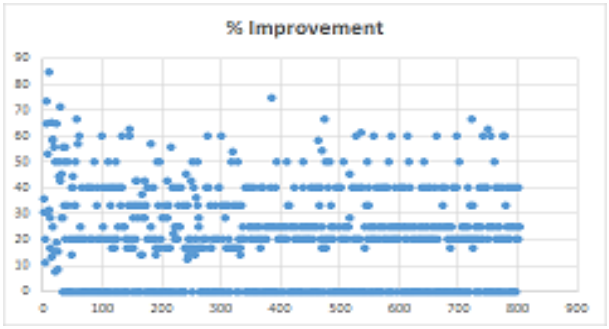

Figure 4: % improvement in contextualized generalization model

8. Conclusion

Generalization cut is reduced so performance of proposed system is increased. Maximum Complexity Reduction due to Contextualized Generalization Hierarchy for Anonymization Algorithm. For tree structure data an anonymization algorithm is developed which gives K(m,n) anonymous data set.

References

[1] M. Nergiz, C. Clifton, and A. Nergiz, Multirelational k-anonymity, IEEETrans. Knowl. Data Eng., vol. 21, no. 8, pp. 11041117, Aug. 2009.
[2] R. Chaytor and K. Wang, Small-domain randomization: Same privacy more utility, Proc. VLDB Endowment, vol. 3, pp. 608618, 2010.
[3] G. Ghinita, P. Kalnis, and Y. Tao, Anonymous publication of sensitive transactional data, IEEE Trans. Knowl. Data Eng., vol. 23, no. 2, pp. 161174, Feb.2011.
[4] J. Cao and P. Karras, Publishing microdata with a robust privacy guarantee,Proc. VLDB Endowment, vol. 5, no. 11, pp. 13881399, 2012.
[5] A. Gkoulalas-Divanis and G. Loukides, Utility-guided clustering- based transaction data anonymization, Trans. Data Privacy, vol. 5, no. 1, pp. 223251, 2012.
[6] G. Cormode, Personal privacy vs population privacy: Learning to attack anonymization, in Proc. 7th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2011, pp. 12531261.
[7] R. Chen, N. Mohammed, B. C. M. Fung, B. C. Desai, and L. Xiong, Publishing set-valued data via dierential privacy, Proc. VLDB Endowment, vol. 4, no. 11,pp. 10871098, 2011.
[8] D. Kifer and A. Machanavajjhala, “No free lunch in data privacy”in Proc. ACM SIGMOD Int. Conf. Manage. Data, 2011, pp. 193–204.
[9] D. Kifer, Attacks on privacy and deFinettis theorem, in Proc. ACM SIGMODInt. Conf. Manage. Data, 2009, pp. 127138.
[10] G. Aggarwal, T. Feder, K. Kenthapadi, S. Khuller, R. Panigrahy, D. Thomas,and A. Zhu, Achieving anonymity via clustering, in Proc. 25th ACM SIGMOD- SIGACT-SIGART Symp. Principles Database Syst., 2006, pp. 153162.
[11] Olga Gkountouna and ManolisTerrovitis,”Anonimizing collections of tree structured data”, IEEE Transactions on Knowledge and Data Engineering Vol 27, No. 8, August 2015 pp.2034-2048.
[12] https://en.wikipedia.org/wiki/K-anonymity
[13] https://en.wikipedia.org/wiki/Quasi-identifier