









in a large-scale, failure-prone environment because the central load balancer is put under considerable workload that is linearly scaled with the system size, and possibly it will become the performance bottleneck and the single point of failure.

## 8. Future Scope

In future for the database servers we can use cloud or Hadoop servers for more security, as well as the data can be distributed in different chunks with HDFS (Hadoop Distributed File System).

## References

- [1] Efficient Two-Server Password-Only Authenticated Key Exchange Xun Yi, San Ling, and Huaxiong Wang IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 9, SEPTEMBER 2013
- [2] L. Barolli and F. Xhafa, JXTA-OVERLAY: A P2P platform for distributed, collaborative and ubiquitous computing, IEEE Trans. Ind. Electron., vol. 58, no. 6, pp. 21632172, Oct. 2010.
- [3] Sonal C. Pansare and Prof. Vaishali Nandedkar, "An Efficient Two-Server Password Only Authenticated Key Exchange Secure Against Dictionary Attacks", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 11, November 2014.
- [4] X. Li, W. Qiu, D. Zheng, K. Chen, and J. Li, Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards, IEEE Trans. Ind. Electron., vol. 57, no. 2, pp. 793800, Feb. 2010.
- [5] M. Cheminod, A. Pironti, and R. Sisto, Formal vulnerability analysis of a security system for remote fieldbus access, IEEE Trans. Ind. Inf., vol. 7, no. 1, pp. 3040, Feb. 2011.
- [6] X. Li, W. Qiu, D. Zheng, K. Chen, and J. Li, Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards, IEEE Trans. Ind. Electron., vol. 57, no. 2, pp. 793800, Feb. 2010.
- [7] W. Juang, S. Chen, and H. Liaw, Robust and efficient password authenticated key agreement using smart cards, IEEE Trans. Ind. Electron., vol. 15, no. 6, pp. 25512556, Jun. 2008.
- [8] J. Katz, P. MacKenzie, G. Taban, and V. Gligor, "Two-Server Password-Only Authenticated Key Exchange," Proc. Applied Cryptography and Network Security (ACNS '05), pp. 1-16, 2005.
- [9] Y. Yang, R.H. Deng, and F. Bao, "A Practical Password-Based Two-Server Authentication and Key Exchange System," IEEE Trans. Dependable and Secure Computing, vol. 3, no. 2, pp. 105-114, Apr.-June 2006.
- [10] J. Brainard, A. Jueles, B.S. Kaliski, and M. Szydlo, "A New Two-Server Approach for Authentication with Short Secret," Proc. 12th Conf. USENIX Security Symp., pp. 201-214, 2003.

- [11] H. Jin, D.S. Wong, and Y. Xu, "An Efficient Password-Only Two-Server Authenticated Key Exchange System," Proc. Ninth Int'l Conf. Information and Comm. Security (ICICS '07), pp. 44-56, 2007.
- [12] Y. Yang, R.H. Deng, and F. Bao, "Fortifying Password Authentication in Integrated Healthcare Delivery Systems," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS '06), pp. 255-265, 2006.
- [13] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. Information Theory, vol. IT-31, no. 4, pp. 469-472, July 1985.
- [14] Wei-Kuo Chiang and Jian-Hao Chen, "TW-KEAP: An Efficient Four-Party Key Exchange Protocol for End-to-End Communications", Proceedings of the 4th international conference on Security of information and networks, pp. 167-174, 2011.
- [15] Miss. Sonal Chandrakant Pansare and Prof. Vaishali Nandedkar (Assistant Professor), "PAKETS: Password Authenticate Key Exchange using Two-Servers", 2012. cPGCON 2015, MET's Institute of Engineering.

## Author Profile

**Miss. Sonal Chandrakant Pansare** is a student of Masters in Engineering, Computer Department, PVPIT, Pune University. She received Bachelors of Engineering in 2010 from Mumbai University. Her research interests are Computer Networks (Wireless Networks), Web 2.0, Network Security, Database Systems etc.

**Prof. V. S. Nandedkar** is working as Assistant Professor and Head of Department of Information Technology in PVPIT, Pune University. She completed her master in engineering (CSE) with specialisation Signal Processing and now she is perusing her Ph.D.