

Accountable Proxy Re-Encryption for Secure Data Sharing

Girish T L¹ and Neha Singhal²

Student, Department of Master of Computer Applications¹
Associate Professor, Department of Information Science and Engineering²
Rajarajeshwari College of Engineering, Bangalore, Karnataka, India

Abstract: *The COVID 19 pandemic is a humanitarian emergency that poses an enormous threat to society and has impacted various social media platforms and journalism. News and social media has become an immensely popular platform for consumption of information. The wide spread of fake news could inflict damages on social media platform. And hence, the need of Fake News Detection in the present scenario is inevitable. In this paper, we survey the recent literature about different approaches to detect fake news over the Internet. In particular, firstly I have discussed about fake news and the various terms related to it that have been considered in the literature. Further I have highlighted various publicly available datasets and various online tools that are available and can debunk Fake News in real time. Hence, I have described fake news detection methods based on two broader areas i.e., its content and the social context. Finally, I have curated a comparison of various techniques that are used to detect fake news.*

Keywords: Fake news detection, Internet, content context, social context

REFERENCES

- [1]. "Amazon S3," as in "Amazon S3." <http://aws.amazon.com/s3/> <http://aws.amazon.com/s3/> "What's the best cloud choice?" "What's the best cloud choice?" "Google Drive, iCloud, Dropbox, and more are analysed."
- [2]. A. Secretive, "What's the greatest cloud choice? Google Drive, iCloud, Dropbox, and more" [Online]. A website where you may learn more about it is <http://gizmodo.com/5904739>.
- [3]. "Divertible conventions and nuclear intermediary cryptography," Springer, New York, NY, USA, 1998, pp. 127-144 in Advances in Cryptology-EUROCRYPT'98, M. Blast, G. Bleumer, and M. Strauss.
- [4]. In Proc. ninth ACM Symp. Inf. Comput. Commun. Secur., 2012, pp. 1-10, "A certificateless intermediary re-encryption scheme for safe information sending to public cloud."
- [5]. O. Blazy, X. Bultel, and P. Lafourcade, "Two safe strange intermediary based information storage," in Proc. SECURE, 2016, pp. 251-258.
- [6]. P. Xu, J. Xu, W. Wang, H. Jin, W. Susilo, and D. Zou, "For the most part half breed intermediary re-encryption: a secure information separation over cryptographic mists," ACM Asia Conf. Comput. Commun. Secur., 2016, pp. 913-918.
- [7]. C. Zuo, J. Shao, J. K. Liu, G. Wei, and J. Shao, J. Shao, J. Shao, J. Shao, J. Shao, J. Shao, J. Sha
- [8]. S. Myers and A. Shull, "Functional denial and key revolution," in Proc. Cryptographers Track RSA Conf., 2018, pp. 157-178.
- [9]. "Secure intermediary re-encryption with picked ciphertext," in Proc. fifteenth ACM Conf. Comput. Commun. Secur., 2007, pp. 185-194.
- [10]. G. Ateniese, K. Fu, M. Green, and S. Hohenberger present "Further enhanced intermediary re-encryption techniques with applications to achieve scattered capacity" in Proc. Netw. Distrib. Syst. Secur. Symp., 2005.