

Blocking Fake Accounts in Online Social Networks

Mrs. M. Jasmine Sagaya Jonita¹, Ms. M. Deepa², Ms. R. Vainavi³

Assistant Professor, Department of Information Technology¹

Final Year Student, Department of Information Technology^{2,3}

Nirmala College for Women, Red Fields, Coimbatore, Tamil Nadu, India

Abstract: *The "BLOCKING FAKE ACCOUNTS IN SOCIAL NETWORKS" project is to anonymizing networks such as Tor allow users to access Internet services privately by using a series of routers to hide the client's IP address from the server. These fake social media accounts exist and it is important to identify them so that their activity is ignored or even reported. The purpose of these profiles is they can be created to give voice to a product of a brand, it does not inflict serious damage to the network.*

Keywords: Fake account

REFERANCES

- [1]. G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A Practical and Provably Secure Coalition-Resistant Group Signature, Scheme," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 255-270, 2000.
- [2]. M. Bellare, R. Canetti, and H. Krawczyk, "Keying Hash Functions for Message Authentication," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 1-15, 1996.
- [3]. M. Bellare and P. Rogaway, "Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols," Proc. First ACM Conf. Computer and Comm. Security, pp. 62-73, 1993.
- [4]. D. Boneh and H. Shacham, "Group Signatures with Verifier-Local Revocation," Proc. ACM Conf. Computer and Comm. Security, pp. 168-177, 2004.
- [5]. S. Brands, "Untraceable Off-Line Cash in Wallets with Observers (Extended Abstract)," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 302-318, 1993.