SPY-BOT: Machine learning-enabled post filtering for social network-integrated industrial internet of things

Md Arafatur Rahman[a], Nafees Zaman[b], A. Taufiq Asyhari[c], S. M. Nazmus Sadat[b], Prashant Pillai[a], Ruzaini Abdullah Arshah[b]

[a] University of Wolverhampton, School of Mathematics and Computer Science, Wulfruna Street, Wolverhampton, WV1 1LY, United Kingdom

[b] Faculty of Computing, University Malaysia Pahang, Tun Abdul Razak Highway, 26300 Gambang, Kuantan, Pahang, Malaysia

[c] School of Computing and Digital Technology, Birmingham City University, Millenium Point, Birmingham, B4 7XG, United Kingdom

ABSTRACT

A far-reaching expansion of advanced information technology enables ease and seamless communications over online social networks, which have been a *de facto* premium correspondents in the current cyber world. The ever-growing social network data has gained attention in recent years and can be handy for industrial revolution 4.0. With the integration of social networks with the Internet of Things being noticed in different industries to enhance human involvement and increase their productivity, security in such networks is increasingly alarming. Vulnerabilities can be characterized in the form of privacy invasion, leading to hazardous contents, which can be detrimental to social media actors and in turn impact the processes of the overall Social Network-Integrated Industrial Internet of Things (SN-IIoT) ecosystem. Despite this prevalence, the current platforms do not have any significant level of functionality to capture, process, and reveal unhealthy content among the social media actors. To address those challenges by detecting hazardous contents and create a stable social internet environment within IIoT, a statistical learning-enabled trustworthy analytic tool for human behaviors has been developed in this paper. More specifically, this paper proposes a machine learning (ML)-enabled scheme SPY-BOT, which incorporates a hybrid data extraction algorithm to perform post-filtering that arbitrates the users' behavior polarity. The scheme creates class labels based on the featured keywords from the decision user and classifies suspicious contacts through the aid of ML. The results suggest the potential of the proposed approach to classify the users' behavior in SN-IIoT.

KEYWORDS

Behavioral analysis; Computational method; Machine learning; Natural language processing; Social Network; IIoT; Post-filtering

ACKNOWLEDGMENT

This paper is partially supported by UMP Internal Grant (RDU192704) and PGRS Grant (PGRS1903105) Malaysia.