Received: September 9, 2021. Revised: January 4, 2022.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Real Time Profile Analysis and Fake Detection Model for Improved Profile Security in Online Social Networks

M. Senthil Raja[1] L. Arun Raj[2]* P. M. Ashok Kumar[3] R. Nandha Kumar[4]

[1]*Department of Computer Science Engineering,*
SRM Institute of Science and Technology, Tamilnadu, India
[2]*Department of Computer Science Engineering,*
B.S.A. Crescent Institute of Science and Technology, Tamilnadu, India
[3]*Department of Computer Science Engineering, KL University, Vijayawada, India*
[4]*Department of Computer Science Engineering, VIT, Andhra Pradesh*
* Corresponding author's Email: arunraj@crescent.education

Abstract: The problem of social network security has been well studied. Numbers of approaches are identified towards securing the profile of social network users and identifying the fake profiles. Still the methods suffer to produce efficient results on detecting fake profiles. To improve the performance, an efficient profile analysis and fake detection model is presented in this article. The proposed Real Time Profile Analysis and Fake Detection Model (RTPAFDM) works on three phases: first the Post Level Trust Analysis (PLTA) is performed, which monitors the post updated on every day and share the posts internally with other users to claim the trustworthy of the post which computes the value of User Post Trust Weight (UPTW); second the method performs Profile Level Trust Analysis (PrLTA) which extracts the profile information like user name, personal details, contact details and friends list. According to the information extracted, the method searches on the entire social network to measure the Profile Match Similarity (PSM). Based on the PSM value, the method would identify the originality of the profile; finally, the method performs Profile Historic Trust Analysis (PHTA) which works on the earlier posts made and their truth values. It computes the value of Historical Trusted Post Weight (HTPW). Using the result of all these trust analysis values, the profile security and fake detection is performed. The method is evaluated with Twitter data set and achieved fake detection accuracy up to 97% and supports the improvement profile security efficiently.

Keywords: OSN, Profile security, RTPAFDM, PLTA, PrLTA, PHTA, PSM, Fake detection, Social networks.

1. Introduction

The modern society spends the most time in social networks. The Online Social Network (OSN) is the platform where the modern human society floats every day at every second. They use the OSN platform to share variety of information. They post variety of information according to their profession, personal and public interest. For example, the user who is an engineer would post on political issue. Also, he can share his own details to their friends and public. All these has been viewed and accessed by variety of users. As like any other network, the OSN has its own security issues. The profile of any user can be hacked by malicious users and the malicious user would post on anonymous users account. Similarly, the malicious user would generate fake accounts with the information of genuine user and they can clone their details to make it visibly true and post on their profile. The problem is whatever the information post on the specific user account is considered as posted by his own and they are responsible for the information being posted on his/her account. For example, if the account of United States of America is hacked and posted with the tweet as "India is the sole manufacture of terror groups" then Mr. Donald Trump is responsible for the tweet and he is answerable for the issues comes after that. All these

encourage the need of profile security and detecting the malicious accounts in online social networks.

The profile security has been increased according to different factors like: by enforcing different access restrictions, enforcing different access management schemes. Also, the security of profile can be improved by adapting different security measures in restricting the user access on various information. More than this, the security of the profile can be improved by enforcing strategic approach on detecting malicious profiles. Towards this, a real time profile analysis and fake detection model is presented in this paper. It works by analyzing the different features and analyze the profile in different diagonals.

The PrLTA is the process of analyzing the trust of any profile according to the profile details. The details of profile user like name, age, mobile, email, location, address and etc. can be used in analyzing the trustworthy of any profile considered. By analyzing the profile according to the profile details, the trustworthy of the profile can be measured to support fake detection and to improve the security. Similarly, the post level trust analysis (PLTA) can be performed to measure the trustworthy of the profile and post which can be measured according to the post made and the feedback obtained from other users. Similarly, the trust of the profile can be measured by analyzing the historical post made and their truth. By analyzing the trust of profile in different way supports the detection of fake profiles and supports improving the performance of social networks. By combining both results of PLTA and result of profile trust, the security performance and fake detection can be improved. The detailed approach is presented in the next sections. The Section 1, presents the detailed introduction of fake profile detection and discusses various methods and measures. Also, Section 1 discusses the need of developing novel approach. Section 2 presents the detailed review on existing schemes of detecting fake accounts. Section 3, presents implementation of proposed method and Section 4 details the experimental results and discussion. Finally, Section 5 details the conclusion or summary of the article.

2. Related works

There are number of approaches recommended by researchers towards fake detection and profile security in online social networks. Such approaches are discussed in this section.

The problem of fake profile detection is well briefed and the author presented a detailed review on the problem. Towards improving the performance in detecting fake profiles different normalization approaches like Min-Max and Z score has been presented. The method is evaluated with the twitter data set [1, 2]. A machine learning model is presented towards securing the social media accounts which calculate followers and friends of any account to measure the trust of any user [3].

The author presented different approaches and survey on the methods of identifying fake accounts where the method uses unstructured data belongs to the social networks [4]. A neural network based fake account detection scheme is presented in [5] which designed a pooling layer to optimize the training process to make it capable to identify fake accounts.

The author focusses on combined the both content analysis and profile feature evaluation approaches to find the fake accounts. It considered the characteristics and nature of spam profile towards detecting the fake accounts. The performance of the approach is evaluated using different classification algorithms. The detection of social bot and fake accounts are reviewed in, which also discusses how machine learning algorithm can be used in profile creation and analysis [6-8].

A support vector machine based neural network approach towards fake account detection in twitter has been discussed in detail in [9], which also discusses different feature reduction and selection techniques. In [10], the author presents a graph based approach to mitigate fake account in social networks. Similarly, set of methods are validated for their performance. The performances of Decision tree and naïve Bayes algorithms are validated for their performance in identifying fake profiles [11-12].

In [13], a graph based approach is presented which extracts anomaly features from different accounts to generate a graph using which the method identifies the densely connected user to find the fake profiles. Similarly, in [14], a deep neural network based approach is presented which uses text and user features to identify the fake profiles with the region features.

The method [15] considers the similarity of friends in different profiles to detect the fake one and a two layer approach is presented which classify the profile according to meta data and the topology information. Similarly, the presence of social bots and chat box is identified using algorithmically driven entities on genuine users and political partisanship [16-18]. The author presents a detailed review on security issues on OSN and discusses various approaches in identifying the fake profiles [19].

In [20], the author focusses on the detailed analysis on exposed user information used in fake profile attacks and other facebook applications. The

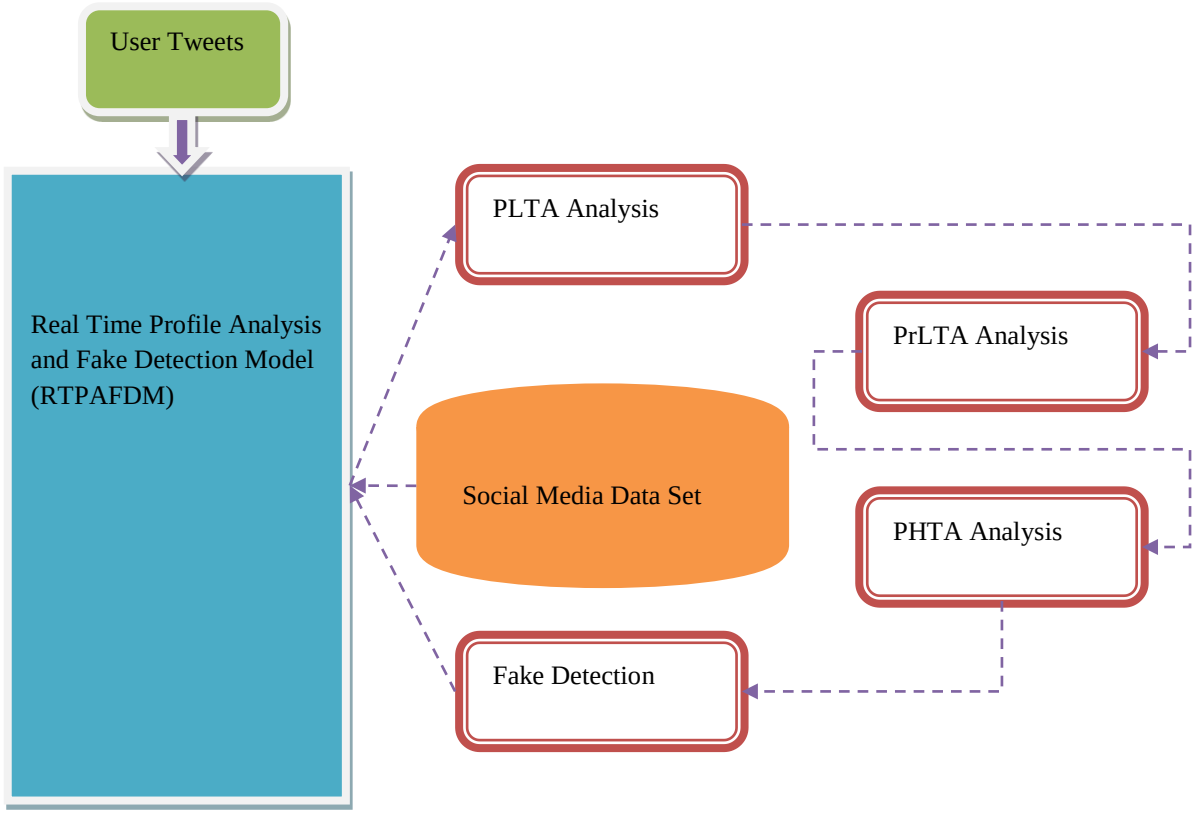

Figure. 1 Architecture of proposed RTPAFDM model

detection of fake news is identified using FakeNewsTracker [21] which collects the data and news pieces and verifies their truthness towards producing quality results. All the methods suffer to achieve higher performance in detecting fake accounts and profiles towards improving the security in online social networks.

2.1 Problem definition

The problem of fake account detection in social network is analyzed deeply. There exist several methods discussed in literature, each have their own merits and demerits. However, they suffer to achieve higher performance. In this way, from the literature survey, the problem of fake account detection can be improved by adapting, profile level trust, historical data level trust, and profile level trust. By enforcing the trust measurement with various levels, the performance of fake detection and access restriction can be improved.

3. Proposed work

3.1 Real time profile analysis and fake detection model (RTPAFDM):

The proposed real time profile analysis and fake detection model reads the post made by different social network users. According to the posts made, the method performs analysis on post level, profile level and historical data level information. The post level trust analysis (PLTA) is performed according to the posts made by the user and the profile level trust analysis (PrLTA) is performed according to the profile information. Similarly, using the historical post made by the same profile, the trust analysis is performed as Profile Historic Trust Analysis (PHTA). Each trust analysis stage estimates different trust weight based on which the fake profile is detected and supports improving the security of online social networks. The detailed approach is presented in this section.

The functional architecture of proposed real time profile analysis and fake detection model is presented in the Fig. 1, where the functional components of the model are detailed in this section.

3.2 Post level trust analysis (PLTA)

The post level trust analysis scheme reads the post made by the user at specific time. From the post generated, the method extracts the text content and image features. Such features extracted are shared with different other users. Each user has been asked for the feedback about the post and from the feedback obtained, the method computes the user post trust weight (UPTW). The users would generate positive

and negative feedback for any post. According to the feedback obtained, the method computes the value of UPTW. Estimated value of UPTW is used in the detection of malicious profiles in social networks.

3.2.1. PLTA algorithm

Input: User Tweet UT
Output: UPTW
Start
Step 1: Read user tweet UT.
Step 2: Identify list of friends in the profile.

$$Fl = \sum_{i=1}^{size(Friends)} Friends \in Profile(UT)$$

Step 3: Select random users Ru = $Random(Rl, N)_{i=1}^{Size(Fl)}$
//where N is the number less than the size of FL.
Step 4: For each user u from Ru
Send the post to the user u.
Obtain feedback Fb=$\sum$ Fb ∪ Fb(u).
End
Step 5: Compute No of positive feedback Npf = $\sum_{i=1}^{Size(Fb)} Fb(i).Type == Positive$
Step 6: Compute UPTW = $Npf / Size(Fb)$
Stop

The post level trust analysis algorithm measures the trust value of the user according to the post the user performed earlier. As the system maintains the traces of post made by the user, the traces are used in measuring the trust value. The post level trust analysis algorithm identifies the users on the profile and their friends. From the friends list, it selects set of users in a random passion and post them the tweet. Also, it obtains set of feedback from the users and based on that the method computes the value of user post trust weight. Estimated value of UPTW has been used towards fake detection in online social networks.

3.3 Profile level trust analysis

The profile level trust analysis is performed by measuring the similarity among different profiles. To perform this, the method extracts different profile information like name, age, sex, location, profession, interest, friends list, and so on. Using these features being extracted, the method computes the value of Profile match similarity (PMS). According to the value of PMS, the method performs fake profile detection.

3.3.1. PrLTA algorithm

Input: User Post UP
Output: PMS
Start
Step 1: Read UP.
Step 2: Extract User Name Un = $UserName \in Profile(Up)$
Step 3: Extract User Age Uage = User Age ∈ Profile(Up)
Step 4: Extract User Profession Upo = $Profession \in Profile(Up)$
Step 5: Extract location Ul = $User\ Location \in Profile(Up)$
Step 6: Extract User sex Usex = $User\ Sex \in Profile(Up)$
Step 7: Extract User interest Uint = $User\ Interest \in Profile(Up)$
Step 8: Extract friends list Fl = $Friends\ List \in Profile(Up)$
Step 9: For each user profile upr in the network according to the region
Initialize count=0
If Un equals upr(Un) then
Count = count+1
If Un equals upr(Un) && uage equals Upr(uage) then
Count = count+1
If Un equals upr(Un) && uage equals Upr(uage) && Used equals upr(Usex) then
Count = count+1
If Upo equals upr(Upo) then
Count = count+1
If Ul equals upr(ul) then
Count = count+1
If Uint equals upr(uint) then
Count = count+1
If fl equals upr(fl) then
Count = count+1
end
Compute profile match similarity PSM.
PSM = if (Un==Upr(un)?0.7:0.2)× (Fl==Upr(fl)?0.9:0.3)× $\frac{count}{7}$
End
Step 10: Choose the maximum value of PSM.
Stop

The environment would have number of profile users. The trust of any user can be measured based on the profile itself. In this part, the method considers

variety of profile information in measuring the trust of any user. The profile level trust analysis algorithm estimates the value of profile similarity measure PSM towards various profiles. According to the value of PSM, a higher valued PSM is selected and based on that the fake profile has been detected.

3.4 Profile historic trust analysis

The trust of any user profile has been analyzed according to the historical behavior of the user. The model maintains set of fake tweets or information posted by different users in different period of time. According to this, the method collects set of tweets or posts generated by the user considered. From the list of posts identified, the method identifies number of posts identified as fake and number of posts identified as genuine. According to that, the method computes the value of Historical Trusted Post Weight (HTPW). The estimated value of HTPW has been used to perform fake profile detection and security improvement.

3.4.1. PHTA algorithm

Input: User Post Upost, Post History PH
Output: HTPW.
Start
Step 1: Read Post History PH, User Post Upost
Step 2: Identify user name Uname = UserName∈Upost
Step 3: Identify set of post made by user Uname as Pl.

Post list Pl = $\sum_{i=1}^{Size(Upost)} Upost(i).Username == Uname$

Step 4: Compute No of genuine posts Gp = $\sum_{i=1}^{Size(Pl)} Pl(i).Post.type == genuine$

Step 5: Compute No of fake post Fp = $\sum_{i=1}^{Size(Pl)} Pl(i).Post.type == Fake$

Step 6: Compute HTPW = $Gp/_{size(Pl)}$
Stop

The trust of user can be measured according to the historic behaviors of any user. The profile historic trust analysis algorithm reads the historic posts generated by the user at different time stamp. According to the historic post of user, the method computes the value of genuine post and fake posts made by the user to compute the value of HTPW. Estimated value of HTPW has been used to perform fake profile detection.

3.5 Fake profile detection

The proposed fake profile detection algorithm reads the user profile and the posts made by them. Using this information, the method performs Post Level Trust analysis (PLTA), User Profile Level Trust Analysis (PrLTA) and Historic Trust Analysis (PHTA). The post level trust analysis algorithm estimates the value of User Post Trust weight (UPTW) and the profile trust analysis algorithm measures the value of PSM (Profile Similarity Measure) and the Profile historic trust analysis algorithm estimates the value of HTPW. Using all these values, the method computes the value of Fake Profile Weight (FPW). According to the value of FPW, the method performs fake profile detection.

3.5.1. Algorithm

Input: User Post Upost
Output: Boolean
Start
Step 1: Read User post Upost
Step 2: UPTW = Perform Post Level Trust Analysis.
Step 3: PSM = perform Profile level trust analysis.
Step 4: HTPW = perform Profile historic trust analysis.
Step 5: Compute FPW = $\frac{PSM}{HTPW} \times UPTW$
Step 6: If FPW<Th then
Return fake
Else
Return genuine.
End
Stop

The fake detection algorithm uses the result of trust measured by various algorithms like post level trust analysis, profile level trust analysis and historic trust analysis. According to the result of trust analysis algorithms. The above algorithm shows how the fake profile are detected by measuring different trust weights. According to that, the method computes the value of FPW, the method performs fake profile detection.

4. Results and discussion

The proposed Real Time Profile Analysis and Fake Detection Model (RTPAFDM) has been implemented and evaluated for its performance using twitter data set. The method has been evaluated for its performance under various constraints. The performance is measured on various parameters.

Obtained results have been presented in detail in this section.

The details of data set being used to evaluate the performance of proposed algorithm have been presented in Table 1.

The performance in detecting the fake profile has been measured under varying number of users in the environment. In each case, the proposed RTPAFDM algorithm has produced higher performance than other approaches. The inclusion of proposed algorithm in fake detection support the performance development in fake account detection by measuring the trust values in post level, profile level and historic level. Finally, by combining all the trust values in measuring trust weight, the performance in fake detection has been improved.

The performance in detecting the fake profile by the different approaches are measured and presented in Fig. 2. The proposed RTPAFDM approach has produced higher performance than other approaches in all the cases.

The ratio of false classification in fake profile detection has been measured under varying number of users in the environment. In each case, the proposed RTPAFDM algorithm has produced less false ratio than other approaches. The inclusion of proposed algorithm in fake detection support the performance development in reduction of false ratio in the fake account detection by measuring the trust values in post level, profile level and historic level. Finally, by combining all the trust values in measuring trust weight, the false ratio in fake detection has been reduced.

The ratio of false detection introduced by the method in detecting fake profiles are measured and presented in Fig. 3. The proposed RTPAFDM

Table 1. Details of evaluation

Parameter	**Value**
Data Set	Twitter
Number of tweets	1 million
Number of users	500
Tool Used	Advanced Java

Table 2. Performance on fake profile detection

Fake Profile Detection Performance			
	100 Users	300 Users	500 Users
Multi Agent	67	72	76
SVM-NN	69	76	79
Medium Gaussian SVM	72	79	83
RTPAFDM	87	93	97

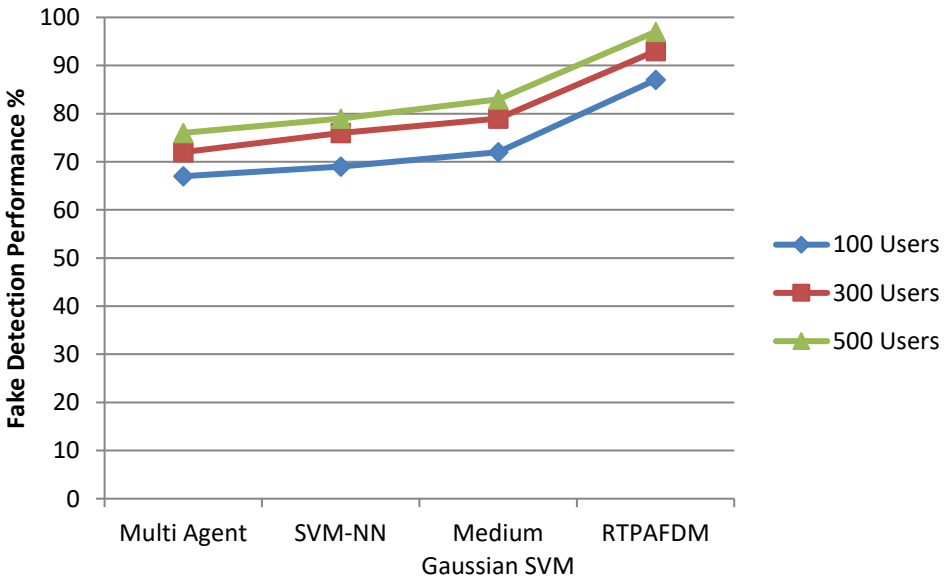

Figure. 2 Performance in fake profile detection

Table 3. Performance on false ratio in fake profile detection

False Ratio in Fake Profile Detection			
	100 Users	300 Users	500 Users
Multi Agent	33	28	24
SVM-NN	31	24	21
Medium Gaussian SVM	28	21	17
RTPAFDM	13	7	3

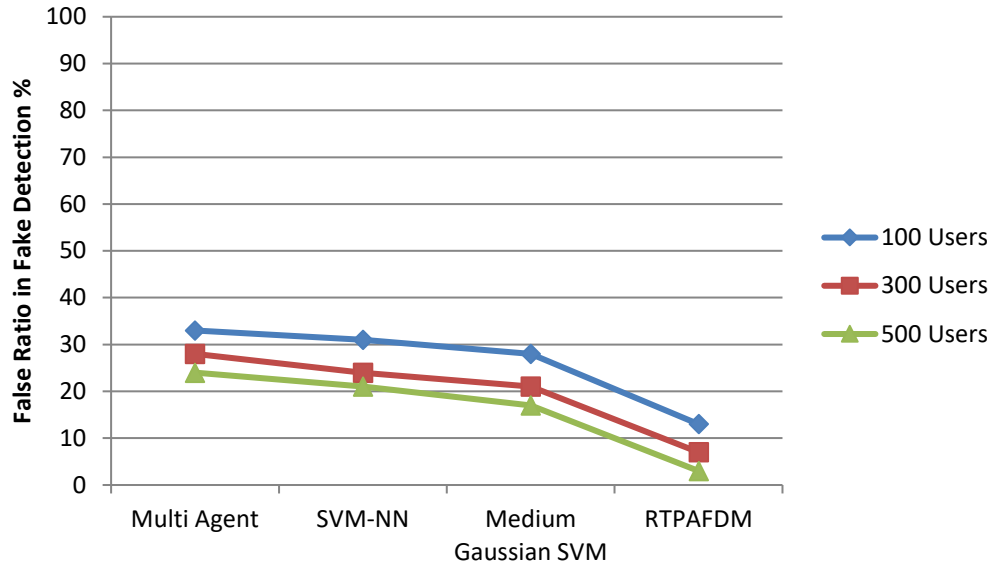

Figure. 3 False ratio in performance in fake profile detection

Table 4. Performance on time complexity in fake profile detection

Time Complexity Fake Profile Detection			
	100 Users	300 Users	500 Users
Multi Agent	63	68	74
SVM-NN	57	64	69
Medium Gaussian SVM	48	56	62
RTPAFDM	23	27	33

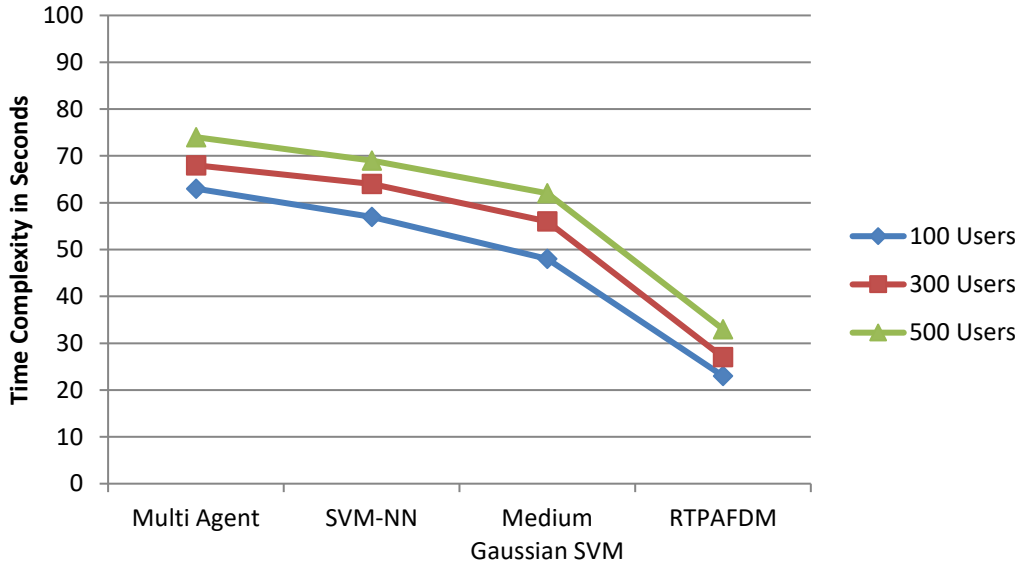

Figure. 4 Time complexity in fake profile detection

approach has produced less value than other approaches in all the cases.

The time complexity introduced by different methods in fake profile detection has been measured under varying number of users in the environment. In each case, the proposed RTPAFDM algorithm has produced less time complexity than other approaches. The adaption of proposed approach support the reduction of false ratio as the method verifies the trust in profile, historic and post level. However, the method reduces the time complexity.

The time complexity introduced by the method in detecting fake profiles are measured and presented in Fig. 4. The proposed RTPAFDM approach has produced less value than other approaches in all the cases.

5. Conclusion

This article presented a novel real time profile analysis and fake detection model (RTPAFDM) towards the detection of fake profiles in social networks. The method performs post level trust analysis (PLTA), which monitors the post updated on every day and share the posts internally with other users to claim the trustworthy of the post which computes the value of User Post Trust Weight (UPTW) and performs Profile Level Further, in future the performance of fake account detection can be improved by adapting group level reputation and feedback approaches which verifies the trust according to reputation obtained from user groups in social network and feedback obtained from various user groups.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

M.Senthil Raja developed the concept, performed the computation simulation, and prepared initial manuscript.L.Arun Raj, P.M.Ashok Kumar, R.Nandha Kumar verified the method, supervised the findings of this works, evaluated and edited the manuscript draft. All authors discussed the results and contributed to the final manuscript.

References

[1] S. Joshi, H. G. Nagariya, N. Dhanotiya, and S. Jain, "Identifying fake profile in online social network: An Overview and Survey", *Communications in Computer and Information Science*, Vol. 1240, pp. 17-28, 2020.

[2] P. Kondeti, L. P. Yerramreddy, A. Pradhan, and G. Swain, "Fake account detection using machine learning", In: *Proc. of Evolutionary Computing and Mobile Sustainable Networks*, Vol. 53, pp. 791-802, 2020.

[3] N. Singh, T. Choudhury, A. Thakral, and T. Sharma, "Detection of fake profile in online social networks using machine learning", In: *Proc. of International Conference on Advances in Computing and Communication Engineering*, pp. 231-234, 2018.

[4] D. Ramalingam and V. Chinnaiah, "Fake profile detection techniques in large-scale online social networks: A comprehensive review", *Computers & Electrical Engineering*, Vol. 65, pp. 165-177, 2018.

[5] P. Wanda and H. J. Jie, "Deepprofile: finding fake profile in online social network using dynamic CNN", *Journal of Information Security and Applications*, Vol. 52, 2020.

[6] N. Kadam and H. Patidar, "Social media fake profile detection technique based on attribute estimation and content analysis method", *International Journal of Recent Technology and Engineering*, Vol. 8, 2020.

[7] A. M. Alzoubi, J. Alqatawna, H. Faris, and M. A. Hassonah, "Spam profiles detection on social networks using computational intelligence methods: The effect of the lingual context", *Journal of Information Science*, Vol. 47, No. 1, pp. 58-81, 2021.

[8] V. Tiwari, "Analysis and detection of fake profile over social network", In: *Proc. of International Conference on Computing, Communication and Automation*, pp. 175-179, 2017.

[9] S. Khaled, N. El-azi, and H. M. Mokhtar, "Detecting fake accounts on social media", In*: Proc. of IEEE International Conference on Big Data*, pp. 3672-3681, 2018.

[10] M. Conti, R. Poovendran, and M. Secchiero, "Facebook: detecting fake profiles in online social networks", In: *Proc. of the 2012 International Conference on Advances in Social Networks Analysis and Mining*, pp. 1071-1078, 2012.

[11] P. Krishnan, D. J. Aravindhar, and P. B. P. Reddy, "Finite automata for fake profile identification in online social networks", In: *Proc. of 4th International Conference on Intelligent Computing and Control Systems*, pp. 1301-1305, 2020.

[12] Y. Elyusufi, Z. Elyusufi, and M. H. Kbir, "Social networks fake profiles detection based on account setting and activity", In: *Proc. of*

International Conference on Smart City Applications, pp. 1-5, 2019.
[13] D. Yuan, Y. Miao, N. Z. Gong, Z. Yang, Q. Li, D. Song, Q. Wang, and X. Liang, "Detecting fake accounts in online social networks at the time of registrations", In: *Proc. of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1423-1438, 2019.
[14] Y. Liu and Y. F. B. Wu, "Fned: a deep network for fake news early detection on social media", *ACM Transactions on Information Systems*, Vol. 38, pp. 1-33, 2020.
[15] M. Mohammadrezaei, M. E. Shiri, and A. M. Rahmani, "Identifying fake accounts on social networks based on graph analysis and classification algorithms", *Security and Communication Networks*, 2018.
[16] P. M. A. Kumar, "Implementation of Facial Expression in Chat Box", *International Journal of Pure and Applied Mathematics*, Vol. 119, No. 14, pp. 221-228, 2018.
[17] A. Bessi and E. Ferrara, "Social bots distort the 2016 US Presidential election online discussion", *First Monday*, Vol. 21, pp. 7-11, 2016.
[18] M. Fire, R. Goldschmidt, and Y. Elovici, "Online social networks: threats and solutions", *IEEE Communications Surveys & Tutorials*, Vol. 16, No. 4, pp. 2019-2036, 2014.
[19] M. Fire, D. Kagan, A. Elyashar, and Y. Elovici, "Friends or foe? Fake profile identification in online social networks", *Social Network Analysis and Mining*, Vol. 4, No.1, 2014.
[20] R. V. Kotawadekar, A. S. Kamble, and S. A. Surve, "Automatic detection of fake profiles in online social networks", *International Journal of Computer Sciences and Engineering*, Vol. 7, No.7, pp. 40-45, 2019.
[21] K. Shu, D. Mahudeswaran, and H. Liu, "FakeNewsTracker: a tool for fake news collection, detection, and visualization", *Computational and Mathematical Organization Theory*, Vol. 25, pp. 60-71, 2019.