AICSA - AN ARTIFICIAL INTELLIGENCE CYBER SECURITY ALGORITHM FOR COOPERATIVE P2P FILE SHARING IN SOCIAL NETWORKS

J. Logeshwaran
Department of Electronics and Communication Engineering, Sri Eshwar College of Engineering, India

Abstract

The Network security is believed to be a subset or sub domain of cyber security. They differ significantly in the implementation of network security to protect internal information by examining the activities of employees and network access. In contrast, cyber security focuses on external threats, such as security breaches created by hackers. An Artificial Intelligence cyber security algorithm is proposed in this paper. Its special feature is that it works in Artificial Intelligence mode and detects cyber-attacks taking place on the network. It will also take appropriate precautionary measures and fix those cyber problems. Its performance has been compared with some of the algorithms currently in practice and its results are given. The currently proposed algorithm will be optimized for financial institutions as it exhibits better performance.

Keywords:

Network Security, Artificial Intelligence, Cyber-Attacks, Security Problems

1. INTRODUCTION

The Internet and social media affect the humanity as a whole. This is according to the Greek playwright Sophocles. Today we can consider a person who does not use any of the services from Google, Gmail to Twitter, Facebook, Instagram, WhatsApp, YouTube, Pinterest. We believe that all of these services are provided to us mostly for free. Most of us have never wondered why these services, which are available 24 hours a day, from communication and money transfer to personal relationships, are available for free. The social dilemma answers that at the outset. Tristan Harris, known as the Conscience of Silicon Valley, says in the film, "If you get anything for free, you're the seller!"

During our daily activities, many of us interact with social media. This is the situation not only in our country, but in many countries of the world. Did you know that with a world population of 7.3 billion, 3.41 billion people connect to the Internet every day? It is estimated that 2.30 billion of these Internet users are directly connected to social media. This is how people around the world use social media. We hope that all of you reading this article will be a member of any one social media or multiple social media. How to use social media so cleverly? Yes, that's what we are discussing about here. By the time you post your comments and photos, most people may not be online. Or, your comments and photos may not have been seen by others yet. Or, due to some other technical glitch, no one may have noticed them yet. There can be many reasons for this.

2. LITERATURE SURVEY

Chen et al. [1] analyzed a Social Network Integrated Reputation System. In that, there have a lot of friends on your social media accounts. Just as there are pros and cons to having a large number of online friends, there are also disadvantages. Are all the people we add to our Friend List our friends? We should always think about.

Boldrini et al. [2] provided a social-aware data dissemination in opportunistic networks. In that, there has many people posting many opinions without understanding the nature of the internet. By publishing these comments, he may have sought some benefit for the community. Yet, they evolve into clowns in the community. This is a very unfortunate situation, but this is how the world works. Therefore, our recommendation is to share only what is necessary with the world.

Conti et al. [6] identified the issues in Social-aware Content Sharing in Opportunistic Networks. The profile picture, cover photo, cover photo and all the comments you post to enhance your image. Today social media is another criterion for evaluating one's personality.

Lloyd et al. [12] implement a system for cohesive and secure community management. In that, there has some adjust the security settings to suit your profile. In particular, by restricting you from 'tagging' other people's posts and photos, adjusting your timeline so that no one else can record anything, and arranging iconic messages into 'spam messages', you too can avoid bulky interference online.

Wasserman et al. [15] analyze the social networks. They must remember that others like us have personal matters and that we must respect that privacy. There is no doubt that some of the ideologies that are published on social media are the best. We can also see that social media is being used to create conflicts between communities, culturally or otherwise, for other gains. We must be very careful about this.

3. PROPOSED SYSTEM

The user information entered first (Fig.1). The information is then matched with other information in the database. This test prevents the same user from logging in twice.

3.1 PROPOSED ALGORITHM

Step 1: Start
Step 2: Enter the input attributes details
Step 3: Check the attributes
Step 4: If (attributes = matching)
Step 5: Then verify the user details
Step 6: If (user details = not available)
Step 7: Then register the user
Step 8: Then enter the missing attributes
Step 9: Else (approve the profile)

Step 10: Else (lock the profile)

Step 11: Stop

The information so entered is verified and then recorded. Pre-inputs that user can edit his records. That information that was new will be recorded. All of his information will be locked and protected after the registration is completed.

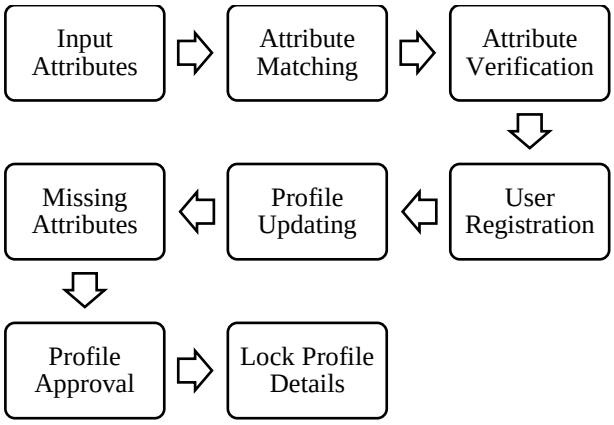

Fig.1. Proposed block diagram

4. RESULTS AND DISCUSSION

Accuracy: Accuracy is the parameter which describes the ratio between perfectly predicted profiles from the given profiles to the total number of entered profiles.

Accuracy = (Positive True Profile+Negative True Profiles)/(Total Profiles) (1)

Precision: Precision measurement is the ratio between the positive true profiles and total true profiles. The total true profiles are calculated by the sum of positive true profiles and false positive profiles.

Precision Measurement = (Positive True Profiles)/(Positive Profiles) (2)

Recall: Recall measurement is the ratio between the positive true profiles and the sum of positive true profiles and false negative true profiles.

Recall Measurement = (Positive True Profiles)/(Positive True Profiles + Negative false profiles) (3)

F1-Score: It is measured by the average sample values of precision and recall of the samples.

F1-Score Measurement=(2*(Recall*Precision))/ ((Recall+Precision)) (4)

Table.1. Simulation environment (Nano sensor observation)

Sensors	PT	NT	PF	NF
15	13	1	0	1
25	22	1	1	1
35	30	1	2	2
45	39	2	2	2
55	50	2	2	1

Table.2. Simulation environment (Nano sensor calculation)

Sensors	Accuracy	Precision	Recall	F1-Score
15	92.86	100.00	92.86	96.30
25	95.83	95.65	95.65	95.65
35	96.97	93.75	93.75	93.75
45	95.35	95.12	95.12	95.12
55	96.30	96.15	98.04	97.09

5. CONCLUSION

Social media is designed so that our friends can see and react to everything we share. So, when posting important events of life, photos, and occasional appearing comments on social media, we need to keep in mind that everyone we know, who we do not know, can see it in our friends list. So, if you are adding someone to the friendship list, you should only connect after careful thought. Also, even if you already have a good friend, do not hesitate to block them if someone is causing you trouble or emotional distress. The proposed system effectively performed to protect our profiles and achieves high accuracy rates while increasing the number of users.

REFERENCES

[1] K. Chen, H. Shen, K. Sapra and G. Liu, "A Social Network Integrated Reputation System for Cooperative P2P File Sharing", *Proceedings of 22nd International Conference on Computer Communication and Networks*, pp. 1-7, 2013.

[2] C. Boldrini, M. Conti and A. Passarella, "Contentplace: Social-Aware Data Dissemination in Opportunistic Networks", *Proceedings of International Conference on Computer Communication*, pp. 203-210, 2008.

[3] N.V. Kousik, M. Sivaram and R. Mahaveerakannan, "Improved Density-Based Learning to Cluster for User Web Log in Data Mining", *Proceedings of International Conference on Inventive Computation and Information Technologies*, pp. 813-830, 2021.

[4] K. Chen, H. Shen, K. Sapra and G. Liu, "A Social Network Based Reputation System for Cooperative P2P File Sharing", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 26, No. 8, pp. 2140-2153, 2015.

[5] K. Praghash and T. Karthikeyan, "Data Privacy Preservation and Trade-off Balance Between Privacy and Utility using Deep Adaptive Clustering and Elliptic Curve Digital Signature Algorithm", *Wireless Personal Communications*, Vol. 78, 1-16, 2021.

[6] M. Conti, F. Delmastro and A. Passarella, "Social-aware Content Sharing in Opportunistic Networks", *Proceedings of International Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, pp. 1-3, 2009.

[7] G. Dhiman, A.V. Kumar, R. Nirmalan and S. Sujitha, "Multi-Modal Active Learning with Deep Reinforcement Learning for Target Feature Extraction in Multi-Media Image Processing Applications",

Multimedia Tools and Applications, Vol. 23, pp. 1-25, 2022.

[8] C. Boldrini, M. Conti and A. Passarella, "Exploiting Users Social Relations to Forward Data in Opportunistic Networks: The Hibop Solution", *Pervasive and Mobile Computing*, Vol. 4, No. 5, pp. 633-657, 2008.

[9] S. Wasserman and K. Faust, "*Social Network Analysis: Methods and Applications*", Cambridge University Press, 1994.

[10] Y. Peng, M. Yang and Y. Dai, "Analyze the Impact of User Search Behavior on DHT-based P2P File Sharing System", *Proceedings of International Conference on Grid and Cooperative Computing*, pp. 137-142, 2006.

[11] J. Lloyd and R. Anane, "Implementation of A System for Cohesive and Secure Community Management", *Proceedings of International Conference on Computer Supported Cooperative Work in Design*, pp. 133-138, 2021, pp. 133-138.

[12] J. Logeshwaran and R.N. Shanmugasundaram, "Enhancements of Resource Management for Device to Device (D2D) Communication: A Review", *Proceedings of International Conference on* IoT in Social, Mobile, Analytics and Cloud, pp. 51-55, 2019.