Proceedings of the 2nd Indian International Conference on Industrial Engineering and Operations Management
Warangal, Telangana, India, August 16-18, 2022

Using Deep Learning for Protecting Security on Online Social Network: A Comprehensive Study and New Perspectives

Tilottama Singh
Assistant Professor, Amity International Business School
Amity University Uttar Pradesh, India
tsingh6@amity.edu

Sukanta Kumar Baral
Professor, Department of Commerce, Faculty of Commerce & Management
Indra Gandhi National Tribal University, Madhya Pradesh, India
sukanta.baral@igntu.ac.in

Richa Goel
Assistant Professor, Amity International Business School
Amity University Uttar Pradesh, India
rgoel@amity.edu

Supriya Lamba Sahdev
Assistant Professor, Amity International Business School
Amity University Uttar Pradesh, India
lamba.supriya9@gmail.com

Yashika Garg
Graduate Student, Amity International Business School
Amity University Uttar Pradesh, India
yashika.garg@s.amity.edu

Abstract

Online social networks (OSNs) have gained a lot of popularity in the past few years. The capacity of OSNs to provide a way for users to interact with their peers is the driving force behind this phenomenon. Social media sites like Facebook, Twitter, and Instagram have recently become an inextricable part of our everyday lives. Information sharing raises many security and privacy problems, in cases where users upload personal material such as photographs, videos, and audio. An attacker can take advantage of shared data for malevolent purposes. In the case of children, the risks are much higher. This study examines numerous risks associated with OSN and also possible ways that can secure social network users to address these issues. The research will also prove that DL is a viable and scalable approach for OSN's state-of-the-art PPS by using a deep neural network for identifying potential threats. The framework proposed in the chapter helps identify features related to attacks on Online Social Networks, determine the relevant policies, scan networks, and create subnetwork anomaly nodes. It's a continuous process to perform retrospective analysis and help improve models by adjusting parameters. Using Deep Learning Algorithms, attributes are classified and stored in a secure database. This repository is used in detecting attacks on online social networks and taking the most appropriate actions. Finally, it identifies several unresolved concerns and obstacles that now impede real-world implementation and suggests future paths for achieving trustworthiness in online social networks along this dimension.

Keywords
Deep learning, OSN, Data Privacy, Data Security, Deep learning application, Deep neural network

1. Introduction
In today's digital age, one of the most pressing issues in social networking is optimization. The massive expansion of the social network creates several chances for companies and decision-makers to disseminate new goods and content in a very systematic and cost-effective manner (Hassanien, & Pan, 2017). Nowadays, people of all ages are glued to social networking sites for a variety of reasons. It is thought to be a simple way for users to send personal messages, photos, and videos to one another. While many individuals like social media, misleading practises such as fake news and rumours can cause users to believe erroneous information. Information spreads swiftly, almost instantaneously, on social media and in the news, making it enticing to hackers. Various points of view on OSN secrecy and assurance must be examined. Organizations and businesses also utilise social media to market their products and services based on consumer interest and attention. An opinion leader has a major effect on the decisions and conduct of others (Mafarja & Mirjalili, 2018). The identification of spam in social networking sites is a significant challenge now-a-day. Researchers are eager to do studies in these areas. Many academics have worked hard to develop effective ways of detecting spam. Benjamin Markines and colleagues proposed using supervised learning techniques to detect spam. TagSpam, TagBlur, DomFp, Numads, Plagiarism, and ValidLinks are the six unique criteria that these techniques are assessed on. Kyumin Lee et al. offer a spam detection strategy based on honeypots and the SVM machine learning algorithm. Xin Jin et al. (2011) discovered spammers in social networks using the GAD clustering technique. This method addresses the concerns of scalability and real-time spam detection. Using the ELM method, Xueying et al (2015) categorise social networking messages as spam.

Deep Learning Techniques have been adopted because of the ever-increasing development of deep learning in various domains, including vision, recommendation systems, natural language processing, OSN, and so on. These advancements are primarily due to the availability of massive datasets and significant processing power (Kaveh & Ghazaan, 2017). The datasets are often crowdsourced and may contain sensitive information. This poses significant privacy concerns because this information might be abused or leaked as a result of various faults, notably in OSN. Fake accounts, on the other hand, pose a significant security risk to OSN. Even if the cloud provider and communication channel are trusted, an attacker can employ inference attacks to predict aspects of the data used for training or uncover the underlying model architecture and parameters.

OSN has a vast number of members, and thousands of new people may join every day. Unfortunately, the attackers attempt to create bogus accounts on a large scale. As a result, the OSN system must provide a cluster-level, trustworthy detection model. However, major security problems in the OSN have recently been discovered, and several papers on the matter have been published. Deep learning (DL) is a sort of machine learning that is similar to the biological neural networks seen in the human brain (NNs). The success of deep learning models in dealing with computer vision issues such as picture classification, object identification, text classification, and speech recognition has piqued the interest of many researchers. The DL architecture advances in lockstep with the amount of data available. We can gain huge boosts in processing capability thanks to GPU computing. It is possible to do quick training and deployment of DL models using GPUs. It's an intriguing way for improving performance. Despite the fact that numerous research on both attacking and protecting users' privacy and security measures in OSN have been published, they are still dispersed. In practice, anomaly issues are made up of several forms of threats, such as vertical attacks on OSN providers or horizontal attacks on OSN members. Many studies propose traditional approaches to deal with the problems, such as statistical, rule-based, and clustering strategies. However, present approaches are incapable of detecting malicious actions quickly. In this survey, we look at the privacy risks raised by deep learning, as well as the mitigation approaches used to address them. We also show that there is a gap in the literature when it comes to test-time inference privacy, and we suggest some potential future study avenues. Many research communities have proposed security problems such as anomaly detection, malicious link prediction, and intrusion detection in OSN.

1.1 Objectives
This present study aims to ascertain the hurdles of OSN implementation by using a deep neural network for identifying potential threats model. Further, the study aims to present the use of DL for overcoming predominant challenges of OSN.

1.2 Research Gap
The development of deep learning techniques has attracted a lot of attention from the industry and scientific communities for a variety of reasons. DL-based detection methods have been a key source. For example, several

studies have investigated the influence of deep learning on OSN. As a result, both in academia and in business, the success of DL for OSN necessitates a complete assessment in order to better comprehend the current situation and provide solutions. Numerous researchers looked at experiments on rumour detection in which they discriminated between unverified and verified information, with the latter remaining unresolved or proving to be true or untrue. Kumar and Shah (2018) studied a broader range of incorrect information on the internet, bringing together previous research, current advancements, and future directions in one place. However, based on existing research, we can conclude that there is no clear definition of what constitutes misinformation. Although attempts have been made to evaluate and synthesise the literature on Deep Learning in a clear and concise manner, there are still enough gaps to review the literature on disinformation in a more comprehensive manner. Shu et al. (2017), for example, use data mining tools to illustrate an intriguing relationship between psychological concepts, fake news, and social networks in an existing survey. The research reviewed by researchers exhibits a related problem of rumour detection in which they distinguish between unverified and verified information, with the latter remaining unresolved or turning out to be true or untrue. Studies have also looked at a broader range of incorrect information on the internet, presenting existing work, current progress, and future directions all in one place.

2. Review of Literature

A large-scale OSN has millions of users and billions of transactions. People's popularity and social standing may rise as their OSN rises. Users of OSN, for example, may earn popularity by amassing a large number of likes, followers, and comments on their posts (Yokotani & Takano, 2021). It is, however, far too simple to set up phone accounts or buy them cheaply online. On the internet, it is much easier to purchase Twitter and Instagram followers and likes (Denley, 2019). Many malevolent reasons of private data leaking are currently the first step towards jeopardising present user privacy. The majority of OSN solutions for identifying suspicious accounts concentrate at activity changes. Users' actions often alter over time. The server can detect the suspect account by seeing sudden changes in access patterns for information and activity. Diverse communities, on the other side, advocate for a learning paradigm as a solution to the OSN security problem. The model can train the features data in a period with a large scale of the dataset by utilizing a learning technique. An analysis, for example, uncovered a method for detecting bogus nodes that combines SVM, RF, and AdaBoost (Mozafari et al., 2020).

In addition to OSN characteristics data, dynamic data such as behavioural analysis, graph theory, learning algorithms, and application design may be used in counterfeit detection research. They provide numerous methods for detecting and classifying abnormalities by calculating the characteristics. A study looks into how to counter the intruder's suspicious conduct by developing a community detection system. Several publications are now proposing deep learning solutions to the social network problem. Deep learning is used to analyse user behaviour, profile discovery, link prediction, and sentiment analysis. A Deep Belief Network (DBN) may be utilised to construct a signed OSN link prediction, according to one publication. Previous studies employed social network analysis to predict social phenomena (Stadtfeld et al., 2019).

Social interactions come in many different strengths and forms. In contrast, OSNs typically reduce complicated connections to simple binary ones. As a result, there is a mismatch between the offline social network model and the online social graph model, which contradicts our security concept of preserving consistency across online and offline social networks. We must enhance the connection model to incorporate numerous aspects of real-world social networks (or link model for an online social graph).

In a number of ways, a deep learning-based enriched social interaction model can increase OSN privacy and security. First and foremost, we communicate various bits of knowledge with our friends and coworkers. Because a misunderstanding might result in embarrassment, all social relationships should be expressly stated and treated as such when making privacy decisions. Second, all security measures are founded on trust connections. By definition, user trust relationships are not equal. Traditional privacy solutions based on binary trust relationships overlook and compensate for existing strength inequalities. As a result, they are incapable of providing fine-grained access control and may result in data breaches. Third and finally, when making privacy judgments, interaction intensity can be used as a proxy for relationship quality. In general, if two users do not contact frequently, they merely wish to send a modest quantity of information. Measuring interaction intensity provides up the capability of measuring network dynamics. However, while defining social ties, the trade-off between accuracy and complexity must be addressed. Inaccurate and unclear descriptions may disclose security flaws, while analysing and processing excessively complex descriptions will entail computing costs, rendering the OSN unworkable in reality (Table 1).

Table 1. Challenges of OSN

Notation	Challenges	Description	References
C1	Heterogeneity	The data available on web and varied data bases in abundant and heterogeneous. It is often grouped, unfiltered and incomplete. Several studies have attempted to work on filtration of data and possible absorption of valid and genuine data.	Tai et al, (2020)
C2	Scalability	OSN face a tremendous amount of scalability issues. In OSN scaling is an issue due to the rapid growth that they potentially experience. Postponement of scaling is dangerous.	Mitchell and Gayor, (2020)
C3	Missing information	A lot of missing data in OSN and the strategies to deal with replacement of missing data is one of the predominant challenges. Also, while retrieving the missing data, it is pertinent to note whether the data is systematically missing, and if it is then whether missing data is related to the values of observed variables.	Yazidi et al, (2020)
C4	Confidentially and Privacy	The privacy is of utmost importance and most challenging to manage due to large interface. Privacy concerns can be multidimensional, such as user identity anonymity, personal space, communication privacy, and so on. The element of data privacy pertains to data confidentiality as well as the owner's anonymity.	Pertegal et al, (2019)
C5	Authentication and Data Integrity	The authentication and data integrity means that consistency should be kept and any attempt on deviation should be monitored with an immediate correction plan.	Willis et al, (2017)
C6	Adversaries in OSN's	The internal and external attackers may prove to be malicious in OSN network. They might not be visible on user interface but may claim to be a big threat to data and privacy matters of the users.	Jakubowska, (2019)
C7	Design Conflict	As previously indicated, many security and privacy problems have intrinsic design conflicts with traditional design goals such as usability and sociability of OSNs.	Probst et al., (2013)
C8	Data Mining Challenge	Data collected by OSN providers or data aggregators is an excellent resource for social and marketing analysis since it reveals information about the evolution of a social group, collaborative problem solving, and other concerns. They might also be used to improve and customise OSN services based on user choices and interests. However, there may be inconsistencies between social data mining and OSN privacy rules. An attacker might compromise OSN users' privacy by leveraging publicly accessible OSN data and specific background information.	Jakubowska, (2019)
C9	Protecting Online Social Graphs	A significant feature of OSNs is the online social network that links users. It gathers the crucial data that underpins all of the sociable services provided by OSNs, thus it must be secured first and foremost.	Mitchell and Gayor, (2020)

Organizers should adopt laws and regulations to protect privacy during research, development, and operation, such as developing tools that allow users to monitor user privacy when contributing data to deep learning systems, as described

in the following article. Tensorflow, Torch, Caffe, and OpenCV are popular deep learning frameworks for developing deep learning systems. The flaws in these frameworks have an effect on the deep learning systems that are built on top of them. An attacker exploits weaknesses in a deep learning system by attacking a black or white box. Black box attacks rely on a high number of system queries to gather a huge amount of data from which alternative models may be developed. Deep learning systems, on the other hand, are increasingly restricting the amount of queries allowed into the system, thus Tramér's black box attacks need knowledge of the attack system's design. Moreover, deep learning systems have additional features to prevent undisclosed assaults, making it more difficult for attackers to execute. Furthermore, a thorough understanding of deep learning systems is required nowadays. Changing the input or function of a node in a neural network layer may result in erroneous output. To give effective protection strategies as well as approaches to uncover vulnerabilities in the system's assault, one must first grasp the operational model and how each node performs in each deep neural network.
Experts utilise the original dataset to develop various solutions depending on training models and privacy constraints. Algorithms, algorithm parameters, quasi-identifying features, and sensitive qualities are examples of these setups. Because anonymized data is utilised in a number of situations, the framework also allows data professionals to assess the process's outcome using multiple utility assessments. Furthermore, if customers are dissatisfied with the framework's offered solution, they can choose another from the solution space.

3. Deep Learning Application

The research uses deep learning techniques to detect malicious websites in online social network. Features representations are used to create training data for this task.

The general framework of Deep Learning is given below:

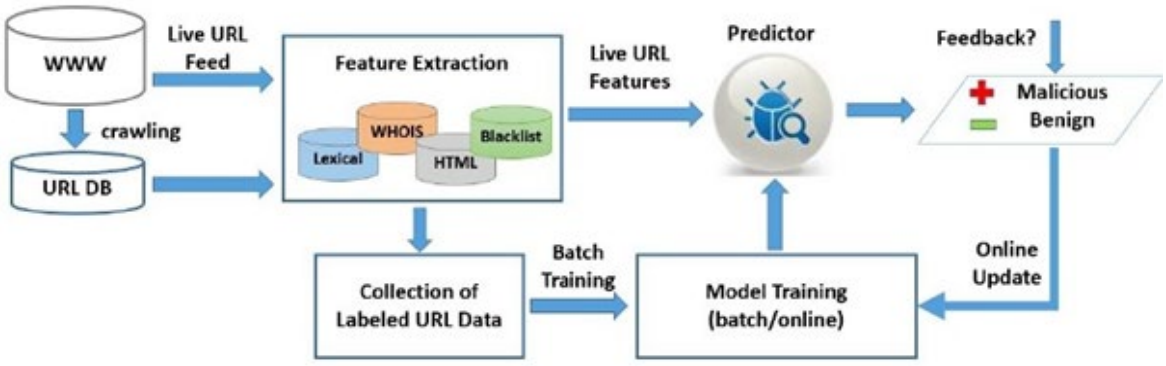

Figure 1. General framework of Deep Learning

Source: https://www.semanticscholar.org/paper/Malicious-URL-Detection-using-Machine-Learning%3A-A-Sahoo-Liu/51006f395255a3c5bed1f418a1b838b2f24b7b38

Malicious URLs host unsolicited material (spam, phishing, drive-by downloads, etc.) and deceive visitors into falling for scams (including financial loss, identity theft, and malware installation), resulting in billions of dollars in damages each year. It is crucial to quickly identify and respond to such dangers. Traditionally, blacklists have been the main tool used for this detection. Blacklists, however, are not thorough and are unable to catch freshly created malicious URLs. Machine learning approaches have recently drawn more interest as a way to increase the generality of malicious URL detectors. The diagram above Figure 1 demonstrates how machine learning is used to give a thorough analysis and a structural knowledge of malicious URL detection methods.

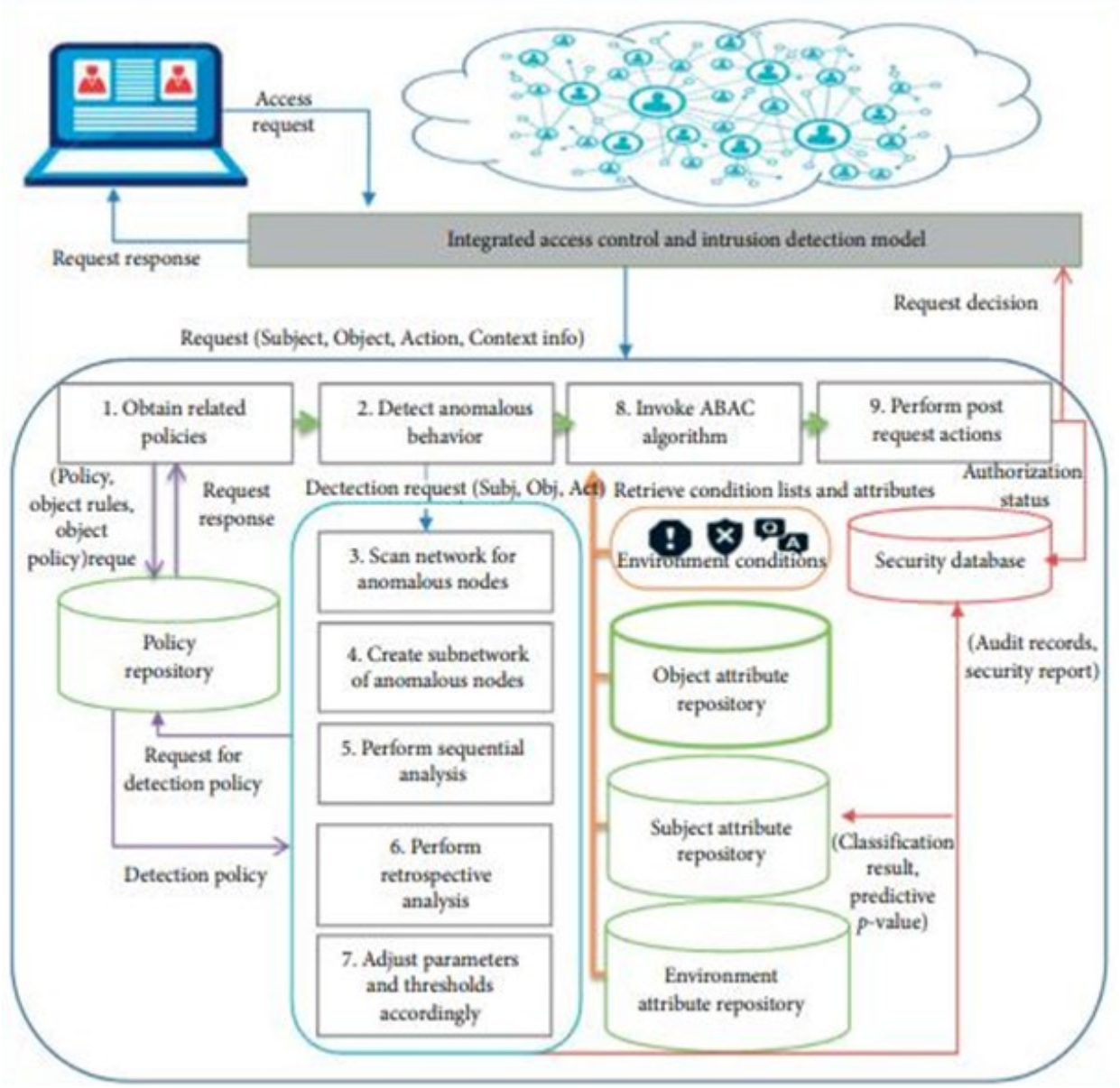

Figure 2. Integrated access control and intrusion detection Model
Adopted from: Aljably et. al. (Wiley Hindwai)

The integrated access control and intrusion detection model illustrated in the Figure 2 above that can also be deployed for the effective implementation of deep neural networks. The deep neural network can be used to detect anomalies as given in the steps: -

(i) Step 1: feature extraction from auditing
(ii) Step 2: normalization of features vectors
(iii) Step 3: leaning of normal behavior is used to predict the next vector
(iv) Step 4: the networks calculate the joint and conditional probability for each vector.
(v) Step 5: the model would determine anomaly scores. These scores would be used to rank.
(vi) Step 6: provides access, if the user proves to be anomalous, they are denied access and flagged, and the pattern of behavior is stored.

Protecting security on Online Social networks is gaining a lot of traction, both practitioners and academicians are doing significant research in this area. Deep learning techniques using artificial neural network algorithms can contribute to detecting anomalies, and malicious websites and help in predicting attacks on online social networks. Deep learning techniques extract the relevant features and utilize these features in the prediction of the outcome.
The framework proposed in the chapter helps identify features related to attacks on Online Social Networks, determine the relevant policies, scan networks, and create subnetwork anomaly nodes. It's a continuous process to perform retrospective analysis and help improve models by adjusting parameters. Using Deep Learning Algorithms, attributes are classified and stored in a secure database. This repository is used in detecting attacks on online social networks and taking the most appropriate actions.
Malicious URL attributes are divided into the following groups (Table 2):

a. Lexical features: the textual size of URL, its domain, size of the domain, path structure, token size
b. Features based on hosting of the site: Features extracted from the hosting domain- location of the server
c. Features based on the contents: features dictionary developed for content containing malicious tokens.

Table 2. Malicious URL attributes

S. No	Feature Group	Feature	Data Type	Description
1	Lexical Group	Number Dots	numeric	Number of characters '.' in URL
2		Subdomain Level	Numeric	Count of subdomain levels
3		Path Level	Numeric	The depth of URL
4		URL length	Numeric	The Length of URL
5		IP address	True/False	IP address is used or not
6		Number Dash	Numeric	Count of '-'
7		Path length	Numeric	Count of characters
8		Query length	Numeric	
	Host-based features	Pop-up window	True/False	Check if there is a pop-up window
		Insecure form	True/False	Check if there is an Insecure form
		Abnormal form	True/False	Check if there is an Abnormal form
		Extension Favicon	True/False	Check if there is Extension Favicon
		Right-click disabled	True/False	Check if Right-click disabled
		Image only form	True/False	Check if the image only form
		Submit information to an e-mail		Check if asking to submit information to e-mail
	Content related feature	Extracted tokens	matrix	

Experimental Set-Up:
First, input the features extracted from the input to a standard convolution layer. The convolution operation is as follows:

$Z_l = \sigma(W_1 \circ X_{l:\, l+k-1} + b)$
$Z^{(i)} = [Z_1, Z_2 \ldots\ldots Z_{L-k+1}]$
b= bias
$W_1 \in R^{Kxd}$ = convolutional filter
Next, convert to a group convolutional operation
$Pi = \vartheta\ (W^2 Z^i) \in R^V$
Z^i represents the i^{th} dimension
Vectorization

$$\vartheta(x) = squash\,(x) = \frac{\|x\|^2}{1+\|x\|^2} \times \frac{x}{\|x\|^2}$$

ϑ means the nonlinear squash function
Predict the output:
$U_{i=}\ W_3 P_i$
Calculate weighted sum of all prediction
$v_j = \vartheta\,(\sum_i c_i\, u_i)$

where c_i is the coupling coefficient.
Our model uses the Adam optimizer with a default learning rate of 0.001.

Evaluation Indicators:
The evaluation is calculated as follows:-

$$ACC = \frac{TP + TN}{TP + TN + FP + FN}$$

$$P = \frac{TP}{FP + TP}$$

$$R = 2\,x\,\frac{PxR}{P + R}$$

$$F = \frac{TP}{FN + TP}$$

TP= True Positive
TN= True Negative
ACC= Accuracy
FP=: False Positive
FN= False Negative
P= Precision
R= Recall
Evaluation Matrices:

Accuracy (ACC), precision (P), recall (R), and F score (F)

4. Case EDICOM

Each client request at EDICOM creates a technical task in our management system where various pieces of information are gathered, including the description of the work to be done, the customer making the request, traceability dates, the number of working days the client will be charged for the work, etc. The task's complexity is then manually rated by an experienced manager on a scale of one to five. A technical project manager with the necessary skills will be assigned for its execution based on this qualification. Additionally, this accreditation will let technicians more effectively modify their capacity based on the volume of projects they oversee and their level of complexity. The definition of this problem fits well within artificial intelligence algorithms, specifically in the machine learning branch and, in particular, in its most contemporary version: deep learning. It is possible to approach the problem from a traditional algorithmic point of view, but we see quite clearly that this is not the best approach.

5. Conclusion

This research looked at concerns of security and privacy in online social networks. Experts from the social science and network security sectors, as well as business, regulatory bodies, and other relevant organisations, will need to collaborate to establish secure procedures and standards. The research is intended to be a starting point for developing OSNs that are both safe and private. The outcome of the research will encourage the OSN scholars and developers to build more inventive OSN designs that do not compromise users' data security and privacy. Although attempts have been made to evaluate and synthesize the literature on OSN in a clear and concise manner, there are still enough gaps to review the literature on disinformation in a more comprehensive manner. For example, use data mining tools to illustrate an intriguing relationship between psychological concepts, fake news, and social networks in an existing survey. Protecting security on Online Social networks is gaining a lot of traction, both practitioners and academicians are doing significant research in this area. Deep learning techniques using artificial neural network algorithms can contribute to detecting anomalies, malicious websites and help in predicting attacks on online social networks. Deep learning techniques extract the relevant features and utilize these features in the prediction of the outcome.
However, based on existing research, we can conclude that there is no clear definition of what constitutes misinformation, there is no clear definition of what constitutes accurate information, and there is no clear description of what constitutes. Existing research projects have made substantial use of DL and have produced significant results for DL. Most of the present study has focused on the link of one user to another on SN, their prior activity, and other factors in propagating incorrect information. However, just a few research have combined the user's mental health concerns with their previous activities. Although we mentioned some future directions in the previous part, one of the most important future areas of our study is to extend modelling. As a result, we may first examine user relationships and prior activity on SN, where people may express their feelings about the spread of bogus news. Second, because the proclivity to spread false information is tied to the user's human mental state, we may combine the user's human mental state with prior data to better analyse the user's behaviours. Social networks are inherently dynamic in real-life settings. The total number of nodes, the underlying network topology, and attribute data may change over time. These features might, for example, correlate to users, relationships, and personal profiles in real-world social networks like Facebook. Because of this feature, existing static learning methodologies are made worthless. Although several ways to dealing with dynamic networks have been proposed, they typically rely on certain assumptions, such as assuming that the node set is stable and that only dynamics caused by edge deletion and addition are taken into account. Furthermore, present research seldom investigates changes in attribute information. As a result, the question of how to create efficient and effective network embedding techniques for dynamic networks remains unresolved.

5.1 Future Recommendation

To increase system security, notable OSN providers have created a number of solutions based on the benchmark dataset. Facebook, LinkedIn, and Twitter have begun to experiment with artificial intelligence technology in order to increase their deep learning capabilities. Facebook uses artificial intelligence to identify suicidal ideas in order to automatically report content. LinkedIn suggests the best possible match for the user's position. Their artificial intelligence technology can forecast the most comparable persons looking for new employment or relationships. Twitter uses a neural system to edit a photo based on face recognition or to build a thumbnail from a full image. Public OSN provides a large-scale sentiment dataset to aid the research community. Amazon, for example, has a vast dataset containing a large number of customer reviews and transactions. Several articles have described approaches for detecting tension spikes in OSN stress and assessing the degree of damage in the link between people or groups. Another experiment focused on forecasting the development and dissolution of network links in a dynamic situation. In OSN, the connection anomaly problem is commonly utilised as a security parameter. Future research might give a link anomaly model that blends Sequentially Discounting Normalized Maximum Likelihood (SDNM L) with Kleinberg's burst model for detecting emergent themes in social streams. Furthermore, OSN security and privacy paradigms should contain smart, trust, anonymity, detectable traceability, and link prediction assistance. A traditional statistical method cannot detect abnormalities like zero-day attacks or unexploited vulnerabilities. Other current research areas in this domain include recommendation services, network unsafe behaviour, and link categorization.
As a result, the learning approach can be used to carry out malicious predictions. By building a multistage and elastic detection framework, studies can give a DL strategy for identifying harmful mobile device behaviours. COMPA, a method reported in recent studies, presents a method for detecting hacked accounts based on behavioural profile and anomaly detection, and the research applies hybrid features to detect suspicious actions. The next step of OSN development will be to build OSN adaptive security using learning methods such as CNN and RNN instead of traditional rule-based or statistical analysis.
The use of representation learning algorithms for network analysis has increased dramatically in recent years. We offered an outline of current work on this topic in this paper. Existing approaches are divided into three categories depending on the main learning modules they employ; representation look-up tables, autoencoders, and graph

convolutional networks. Despite the fact that multiple solutions to various social network analysis challenges have been discovered in recent years, we feel there are still many possible chances worth researching further. Although numerous approaches to dealing with dynamic networks have been presented, they all rely on specific assumptions, such as assuming that the node set is stable and dealing primarily with dynamism induced by edge deletion and addition. Furthermore, past efforts seldom took changes in attribute information into account. As a result, the question of how to build effective and efficient network embedding solutions for really dynamic networks is still unresolved.

References

Altay EV, Alatas B., Detection of cyberbullying in social networks using machine learning methods. In: International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), pp 87–91, 2018.

Alwehaibi A, Roy K., Comparison of pre-trained word vectors for Arabic text classification using deep learning approach. In: 17th IEEE International Conference on Machine Learning and Applications (ICMLA), pp 1471–1474, 2018.

Bai N, Meng F, Rui X, Wang Z., Rumour detection based on graph convolutional neural net. IEEE Access vol. 9, pp. 21686–21693, 2022.

Chandra Y, Jana A., Sentiment analysis using machine learning and deep learning. In: 7th International Conference on Computing for Sustainable Global Development (INDIACom), pp 1–4, 2020.

Dubova M, Moskvichev A, Goldstone R., Reinforcement communication learning in different social network structures. In: Proceedings of 1st workshop on language in reinforcement learning in conjunction with International Conference on Machine Learning (ICML), 2020.

Dutta S, Masud S, Chakrabarti S, Chakraborty T., Deep exogenous and endogenous influence combination for social chatter intensity prediction. Association for Computing Machinery, New York, pp 1999–2008,2020.

Tai, K. Y., Dhaliwal, J., & Shariff, S. M, Online social networks and writing styles– a review of the multidisciplinary literature. IEEE Access, vol. 8, pp. 67024-67046, 2020.

Mitchell, D., & El-Gayar, O. F., The effect of privacy policies on information sharing behavior on social networks: A Systematic Literature Review, proceedings of the 53rd Hawaii International Conference on System Sciences, 2020.

Al-Yazidi, S., Berri, J., Al-Qurishi, M., & Al-Alrubaian, M., Measuring reputation and influence in online social networks: A systematic literature review. IEEE Access, vol. 8, pp. 105824-105851, 2020.

Pertegal-Vega, M. Á., Oliva-Delgado, A., & Rodriguez-Meirinhos, A., Systematic review of the current state of research on Online Social Networks: Taxonomy on experience of use. Comunicar. Media Education Research Journal, vol.27(2), 2019. DOI: https://doi.org/10.3916/C60-2019-08

Willis, E. A., Szabo-Reed, A. N., Ptomey, L. T., Steger, F. L., Honas, J. J., Washburn, R. A., & Donnelly, J. E., Do weight management interventions delivered by online social networks effectively improve body weight, body composition, and chronic disease risk factors? A systematic review. Journal of telemedicine and telecare, vol. 23(2),pp. 263-272, 2017.

Jakubowska, A., Kaselionyte, J., Priebe, S., & Giacco, D., Internet use for social interaction by people with psychosis: A systematic review. Cyberpsychology, Behavior, and Social Networking, vol.2(5),pp. 336-343, 2019.

Probst, F., Grosswiele, L., & Pfleger, R., Who will lead and who will follow: Identifying Influential Users in Online Social Networks. Business & Information Systems Engineering, vol. 5(3),pp. 179-193, 2013.

Biography

Dr Tilottama Singh is a certified HR analyst and trained academic, researcher, and trainer with 9 years of experience in the field of Human Resources and Work Dynamics. She is currently employed as an Assistant Professor in Amity University, Noida, UP. She works in the fields of sustainability, economics and strategy. She earned her doctorate specializing in emotional spiritual quotient in the year 2020. She has published several papers in reputed national and international journals.

Prof. (Dr.) Sukanta Kumar Baral is a Professor, Department of Commerce, Faculty of Commerce & Management, Indira Gandhi National Tribal University (A Central University of Government of India), Amarkantak, Madhya Pradesh, India. As an active academician, he has been closely associated with several foreign Universities, such as Southampton Solent University, United Kingdom, University of Washington, Bothell, USA, University of Zululand, KwaZulu-Natal, South Africa, and Eudoxia Research University, New Castle, USA for multiple academic activities. He has authored 24 books, contributed more than 130 Research Papers in reputed national and international journals with 28 years of rich experience in academia by holding several important roles at various levels.

Dr. Richa Goel is Assistant Professor-Economics and International Business at Amity International Business School, Amity University Noida. She has a journey of almost 20+ years in academic. She is consistently striving to create a challenging and engaging learning environment where students become life-long scholars and learners. Imparting lectures using different teaching strategies, she is an avid teacher, researcher, and mentor. She has to her credit more than 50 plus Research Papers in UGC, SCOPUS, ABDC publications in reputed national and international journals accompanied with hundreds of Research participation in International/National Conferences including FDP, MDP and Symposiums.

Ms. Supriya Lamba Sahdev is a trained academic researcher with 11 years of experience in the field of Marketing and International Business. She is currently employed as an Assistant Professor in ISBR Business School, Bangalore, India. She has published several papers in reputed national and international journals.

Ms. Yashika Garg is a vivid researcher with two years of experience in advertising. She is currently working on live projects in skill development and is actively involved in research conferences and Symposiums.