IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 9, No. 1, March 2020, pp. 146~154
ISSN: 2252-8938, DOI: 10.11591/ijai.v9.i1.pp146-154

DeepOSN: Bringing deep learning as malicious detection scheme in online social network

Putra Wanda[1], Marselina Endah Hiswati[2], Huang J. Jie[3]
[1,2]Department of Informatics, University of Respati Yogyakarta, Indonesia
[1,3]Department of Computer Science & Technology, Harbin University of Science and Technology, China

Article Info

Article history:

Received Aug 4, 2019
Revised Oct 19, 2019
Accepted Dec 26, 2019

Keywords:

Deep Learning
Malicious Detection
Online Social Network
Privacy-Preserving
Security Model

ABSTRACT

Manual analysis for malicious prediction in Online Social Networks (OSN) is time-consuming and costly. With growing users within the environment, it becomes one of the main obstacles. Currently, many research communities have proposed learning techniques to automate security tasks, including anomalous detection, malicious link prediction, and intrusion detection in OSN. Deep learning is a growing algorithm that gains a big success in computer vision problems. In this paper, we propose a novel deep learning architecture to establish the OSN security technique to become more intelligent for detecting malicious activities.

Corresponding Author:

Putra Wanda,
Department of Informatics,
University of Respati Yogyakarta, Indonesia,
Laksda Adisucipto St, Sleman, Yogyakarta, Indonesia.
Email: wpwawan@gmail.com

1. INTRODUCTION

Online Social Network is a popular application for sharing various data items includes videos, photos, and messages. It connects people around the earth. However, an anomalous issue like fake accounts becomes a significant concern in OSN protection. The irregular account becomes one of the main challenges in current OSN because growing users on the OSN heighten the probability level of malicious activities. However, it remains significant challenges in OSNs, which have a large number of users and information with a dynamic environment. In the transmission process, the OSNs able to run either independently or dependently group [1].

In an OSN system, the primary source of the threat comes from anomalous activities. Infected user can spread the fake or deceive information for the target user. The large of OSN is an attacking target for Sybil by harnessing fake account. Human or bot can create a fake account to impersonate the OSN users in a false name and post misleading information on their profiles. For example, individual accounts and bot accounts share a similar identity like a name or pictures [2]. The anomalous intruder can take advantage of the drawback to monitor the target, and the suspicious nodes can pose a Sybil threat [3]. Current public OSN remains shortcoming in several areas, including link detection, malicious sentiment, anomalous accounts, and activities. In practical cases, the anomaly issues are comprised of different types of threats like vertical attack to the OSNs' providers or horizontal attack caused to OSN members [4]. Many papers propose conventional techniques to deal with the issues, including statistic, rule-based, and clustering. However, the current techniques are lack of performing fast detection of malicious activities. The conventional method remains

shortcoming to detect and respond to fake accounts before they interact with real users. It enables fake accounts to stay in the network for establishing malicious connections and accumulate the bulk of activity data. Thus, various studies propose current techniques to improve OSN security techniques [1-5].

OSN has large-scale members, and it may register thousands of new users every day. Unluckily, the attackers try to make fake accounts at scale. Hence, the OSN system is necessary to create a cluster-level and robust detection model. This paper proposes a learning model to improve malicious detection in the OSN by training engineered features of each account. Several studies suggest a common anomalous detection technique; for instance, a study presents a fake account detection model by computing the similarity of the user's friends. The approach calculates the adjacency matrix of the graph. To mark the user as benign or fake, it analyzes the friend's network structure [5]. Figure 1 depicts the evolution of OSN in connectivity and analytical techniques.

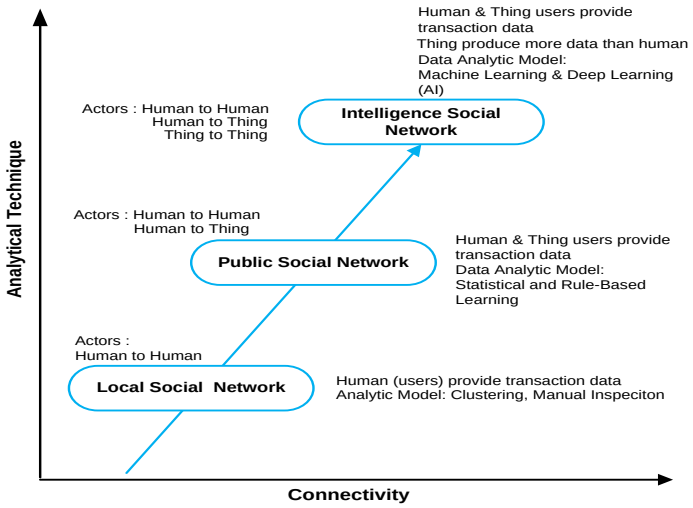

Figure 1. The evolutionary history of social network technology

Based on Figure 1, the next generation of the OSN security model is learning methods. A growing learning algorithm is Artificial NNs (ANNs), also called NNs, that mimics the human brain. The algorithm focuses on how the neurons process information and conduct computations [6]. Many aspects have implemented AI algorithms to address various problems [7-9]. In the neural network, the network elements usually called neurons, which are grouped in different layers. In the operation process, each layer of neurons takes inputs from the previous layer and passes its output to the next layer. Each neuron has parameters, including activation functions, weights, and biases. To minimize error (loss) in the training and validating process, it tunes and optimizes the settings between the predicted and provided values.

Deep learning (DL) is a part of machine learning which mimics the biological neural networks (NNs) in the human brain. DL models have gained significant interest because of successfully achieve an astounding result in computer vision problems, including image classification, object detection, text classification, and voice recognition. The DL architecture is growing with the increased amount of data available. GPU computing enables us to achieves significant improvements in computing capabilities. By using GPUs, it can produce fast training and deployment of DL models possible. It is a promising technique to improve previous methods. CNN is a DL architecture that is implemented in most computer vision tasks, including image classification, object recognition, and natural language processing. The successful performance of CNNs computer vision problems is one of the primary reasons why DL resurfaced in recent years. Different from the CNN for the classification problem for time series data, RNN is part of DL algorithms applied for processing sequential data, such as time series or natural language [10].

In this paper, we focus on building a security scheme in OSN by implementing a deep learning technique. At the first stage, we construct a novel approach to detect malicious accounts by training the OSN features to determine whether the account is benign or malicious. Based on our review, it is the one approach that addresses the anomalous problem by analyzing the high-level attributes of OSN. Notably, we present the main contributions of the thesis, particularly in the malicious account classification as follows:

a. We introduce a deep learning architecture for the classifying account by analyzing the OSN features gathered from the higher-level features. Instead of using a conventional algorithm such as a statistical,

rule-based, or standard machine learning algorithm, we develop a learning technique with some generic functions to predict malicious accounts by calculating the features. We provide the accuracy and loss graph for each technique and measure the evaluation metric at the end of each chapter.

b. We construct the supervised learning architecture by proposing the CNN model to increase classification accuracy. Notably, it is one of the studies that focus on establishing an OSN security technique by implementing a learning algorithm, especially for detecting malicious accounts over the network.

c. We test the proposed model to achieve state-of-the-art results, especially for OSN malicious account classification. This study train various of OSN features to construct a useful model with a benchmark dataset. The model computes OSN features dataset as matrix inputs and employs the model to classify the OSN account. Moreover, by establishing the generic algorithm, we can measure the accuracy of malicious account detection compared with other approaches.

At the first stage, we conduct the study by reviewing the OSN papers as a literature review process to make well-defined methodology and to hinder bias results. The experiment performs the following steps during the planning stage. Firstly, we undergo the literature review, define the research approach, describe problem formulation, and analyze the experiment result.

2. RELATED WORKS

A largescale OSN consist of millions of users and billions of transaction data. Growing OSN can increase the popularity of people and social ratings. A practical example, OSN users can produce popularity with many likes, followers, and comments. However, it is too easy to create fake accounts, or people can buy it online with few costs. For example, it is easier to buy Twitter and Instagram followers and likes on the internet [11]. A large number of malicious causes of private data leakage and become the initial step to compromise existing user privacy [12]. Commonly, to detect anomalous accounts in OSN, the methods analyze activity variations. Usually, the users' activities keep on changing in a period. Sudden changing of access pattern for the information and behavior allows the server to catch the suspicious account up.

On the other hand, diverse communities propose a learning model to address the OSN security problem. By using a learning technique, the model can train the features data in a period with a large scale of the dataset. For instance, an investigation reveals a method for fake nodes detection by combining SVM, RF, and AdaBoost [13]. Not just using the OSN features data, the study of counterfeit detection can utilize dynamic data such as behavioral analysis, graph theory, learning algorithm, and application design. By computing the features, they construct various approaches to identify and classify anomalies. To hinder the suspicious activities of the intruder, a study explores a method by forming a community detection algorithm [14].

Currently, several papers propose deep learning approaches to address social network problem. They establish the DL for various security tasks such as user activity analysis, profile detection, link prediction, and sentiment analysis. For instance, a paper proposes a Deep Belief Network (DBN) to calculate link prediction in signed OSN. Another study explore malicious detection in the OSN. The model detects the malicious account by adopting the long short-term memory (LSTM), a deep learning algorithm based on RNN architecture. It constructs a framework to gain the binary classification with 180 million Momo OSN dataset [15].

3. PROPOSED MODEL

Inspired by Artificial Intelligence (AI) performance in various problems, including intelligent machines, especially in smart computer programs and applications in science and engineering for a better human life, we propose our model by using the AI concept. To express the intelligence capability, the researcher can construct some models such as build decision making and learning tasks. Without using manual programming, the ML algorithm allows machines (computers) to learn and get decisions with statistical methods [16]. It constructs a model to conduct the training process by feeding input data and make predictions on new unseen data.

Generally, there are two categories of ML: 1) supervised learning; this model requires labeled data consisting of pairs of input and the expected output. To produce intelligent decisions on new data, it learns mappings between the data pairs. Several applications apply the technique, such as image classification and speech recognition. 2) unsupervised learning, this model predicts the pattern by using unlabeled data as input and learns the relationships within the input data. The model produces decisions result based on learned patterns. Many application proposes a technique like unsupervised learning, including data clustering and anomaly detection.

Since a decade ago, Machine Learning methods have been utilized for various security tasks including in social networks. Instead of using standard ML algorithms, we focus on establishing DL techniques as the protection strategy to enhance OSN protection. This paper describes how DL can be a security strategy to address malicious detection by using a learning model. One critical issue OSN research is how to a reliability learning methods with a more intelligent and faster period. In this paper, we also present the recent research approaches in the OSN and how to bring the DL algorithm to solve the OSN security with a large dataset. In the final chapter, we provide open research opportunities for communities not only to leverage protection but also to optimize the learning techniques for business purposes.

3.1. Intelligence architecture

a. Actors— In the OSN, individuals or organizations are represented by a node. OSN environment's actors communicate in the OSN system. The OSN community has nodes and relations between two nodes that represent data exchange for obtaining local and global network hierarchies. The OSN graph with $G = (N, L)$ has parameter N represents nodes (vertices) in the OSN graph $N = \{n_1, n_2, n_3 \dots n_n\}$, and parameter L represents set of links (edges) in a set $L = \{l_1, l_2, l_3 \dots l_n\}$. The graph defines nodes (n) and link (l) to connect the nodes.

b. Intelligent Component—This part is responsible for managing and orchestrating the entire communication among the actors. We establish this Intelligent Component as the main sub to provide service and application management. It can gather, handle, and conduct data analytics. The component can harvest a better recommendation, service discovery, accurate data analysis, and context management of the OSN environment.

c. Interface—To enable administrators to monitor user interactions in OSN. It requires an interface that allows the input of data and queries to provide the requested output.

In the Intelligent Component, it requires the learning algorithm to calculate the labeled features as input models to predict an outcome. These features describe information about some of the OSN account such as name, gender, number of friends, number of links, and so forth. Figure 2 displays the intelligence OSN framework to optimize business and security purposes.

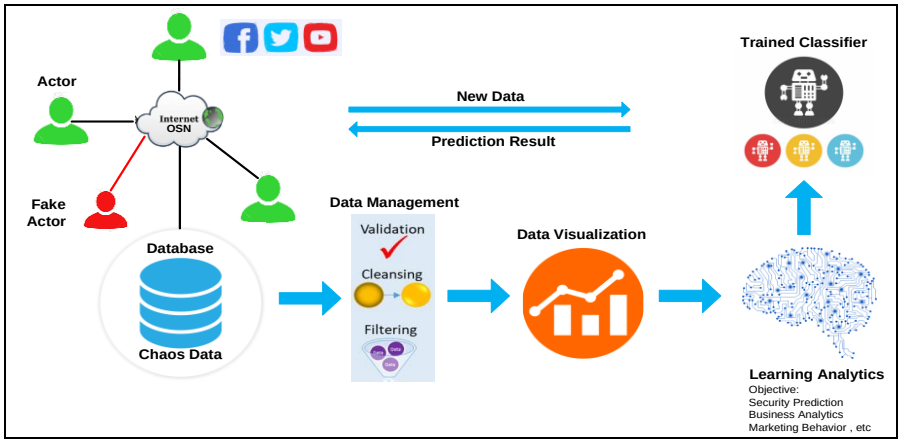

Figure 2. Intelligence OSN with deep learning classifier

The OSN dataset consists of several user information such as identity P_u and relation R_u. User identity refers to a real natural member. It is a unique account in the OSN. P_u consists of user representation including username, age, and other attributes. R_u represents the user's social connections in the OSN. R_u includes how many friends in their network. OSN defines as C and is represented by $C(U, \varepsilon)$ where $U = \{p_1, p_2, \dots p_n\}$ is the set of user identity, and the set of the OSN link is described as $\varepsilon \subseteq U \times U$. In the learning analysis model, it is crucial to transform certain features in a numerical integer into the binary vector.

3.2. Proposed CNN

A common technique to build the OSN security model is machine learning. However, manual feature engineering is a costly and laborious task. Instead of using the conventional architecture, we introduce a novel CNN architecture to deal with malicious activities in OSN. This approach adopts supervised learning to detect abnormal events of the OSN account by analyzing various attributes within

them. This model utilizes OSN attributes, which are described in the above section. Figure 3 depicts the CNN topology to train the classifier by using engineered features.

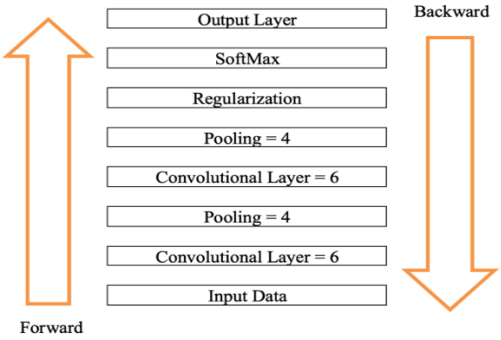

Figure 3. Proposed CNN topology for training the OSN dataset

The proposed CNN employs Deep Neural Network with several hidden layers to train and test the model. It also utilizes a gradient descent to minimize the objective function with the model's parameters. The model updates the settings in the opposite direction of the gradient of the objective function. Different from the regular pooling layer, this study adopts a pooling layer to optimize and accelerate training time in a neural network. By using the proposed CNN topology, we calculate the accuracy and loss of the training and testing process to achieve the best result with the diverse input vector. This study calculates the 1D dataset of OSN, so the tuning an appropriate hyperparameter is beneficial. We establish a supervised learning model by defining calculation over NN as follows:

Input features $x^{(i)} \in R$
Outputs $x^{(i)} \in Y$ $(e.g. R, \{0,1\}, \{1,\ldots,p\})$
Model parameters $\theta \in \mathbb{R}^k$
Hypothesis function $h_{\theta:} : \mathbb{R}^n \rightarrow \mathbb{R}$
Loss function $\ell : \mathbb{R} \times Y \rightarrow \mathbb{R}_{+:}$
In this study, we calculate the optimization problem as follows:

$$\underset{\theta}{Minimize} \sum_{i=1}^{m} \ell\left(h_{\theta:}\left(x^{(i)}\right), y^{(i)}\right) \tag{1}$$

In paper, we provide hypothesis function $h_{\theta:} : \mathbb{R}^n \rightarrow \mathbb{R}$ in neural network processing. On a CNN we need to calculate forward pass and backward pass to measure the gradient of loss function in the model. The study calculate the forward pass to convolve input matrix x_i with filter W_i to produce covolution output $z_{i:}$ as follows:

$$f : \mathbb{R}^n \rightarrow \mathbb{R}^m \tag{2}$$
$$z_{i:}(x_i) = W_i\, x_i + b$$

The CNN consists of the filters W_i and bias term b as the parameters of the convolutional layer during training. It is a supervised learning model that has the input, representation, and metrics to compute tensors in the hidden layer. CNN has many identical neurons among the layers to run large models' computation with a little number of parameters. The layer receives a single input (the feature maps) and computes the feature maps as its output by convolving filters across the feature maps. The parameters of the convolution layer called filters and back-propagation model used to learn during training.
In the backward pass, we calculate the vector-valued function $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ with the Jacobian matrix $m\ x\ n$.

$$\left(\frac{\partial f(x)}{\partial x}\right) \in \mathbb{R}^{m \times n} = \begin{bmatrix} \frac{\partial f_1(x)}{\partial x_1} & \frac{\partial f_1(x)}{\partial x_2} & \cdots & \frac{\partial f_1(x)}{\partial x_n} \\ \frac{\partial f_2(x)}{\partial x_1} & \frac{\partial f_2(x)}{\partial x_2} & \cdots & \frac{\partial f_2(x)}{\partial x_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_m(x)}{\partial x_1} & \frac{\partial f_m(x)}{\partial x_2} & \cdots & \frac{\partial f_m(x)}{\partial x_n} \end{bmatrix} \tag{2}$$

To deal with a common issue in CNN training, we adopt a regulizer to deal with overfitting problems in the training process. It provides a way of approximately combining exponentially many different network architectures. Applying dropout is to obtaining a thinned network in the training process. The study utilizes the Dropout regularization during the training sample (backward pass), not in the predictions process (forward pass). Dropout is a modern and excellent regularizer that is easy to implement and compatible with many training algorithms and models. In the experiment, instead of doing it randomly, we tested some types of dropout with different Dropout value. Based on the testing of the amount, it gives the contribution of the neuron to the output.

On the function, consider a network has L hidden layers. We use the Dropout function to calculate the y_{train} training process for parameters like input x and Bernoulli probability p. In the standard feedforward as for $l \in \{0, \cdots, L-0\}$ there are z^l denotes the inputs vector into layer l, y^l denotes the outputs vector from layer l, r^l represents an independent vector of Bernoulli random variables with probability p of being 1 and $\check{y}^l$ represents thinned outputs which calculated by $\check{y}^l = r^l * y^l$. Thus, we calculate calculate the Dropout regulaizer as follows:

$$z_i^{(l+1)} = z_i^{(l+1)} y^l \theta + z_i^{(l+1)}$$
$$y_i^{(l+1)} = f\left(z_i^{(l+1)}\right) \quad (3)$$

In feed forward operation, we calculate the regulizer with the following formula:

$$r_j^l \sim \text{Bernoulli probability } p$$
$$\check{y}^l = r^l * y^l$$
$$z_i^{(l+1)} = z_i^{(l+1)} \check{y}^l \theta + z_i^{(l+1)} \quad (4)$$
$$y_i^{(l+1)} = f\left(z_i^{(l+1)}\right)$$

To calculate the next layer, the regulizer utilizes the thinned outputs $y_i^{(l+1)}$ as new input. The process is applied to each layer in the hidden layer. This amount is to construct to a sub-network sampling from a bigger network. In the training time, it back-propagates the derivatives of the loss function via the sub-network.

3.3. Dataset

OSN has vast data in the environment, including link information, user profiles, and activity behavior. The OSN user profile represents historical information of user activities in the OSN environment to capture the regular user's expected behavior. At the initial stage, we gather the data form high profile OSN information and use the information to construct the extracted features. The models capture a characteristic feature of an OSN user like the username, e-mail address, the message stream, location, or native language that was used to talk among users. To sum it up, the model takes the data and extracts a couple of features, and trains the features by using a supervised learning model.

In this paper, we gathered an extensive database of labeled OSN dataset from a web service that provides a corpus with a malicious or benign label. We collect the dataset from VirusTotal and PhishTank as a provider that provides many datasets for OSN security study. VirusTotal service used to validate a URL, whether it is malicious or benign. We also collected about 30,000 malicious accounts from PhishTank. We collected about 110,465 samples, which consist of 55,338 benign and 55,127 malicious labels.

In data pre-processing, we require to convert integer or string data type into a numerical array or matrix. It requires a method to convert the features into a vector because the input may be integers or strings. Typically, a study can build the training and testing dataset in columns and rows. The method constructs a binary column for each category and produces a dense array. The sparse matrix in each column represents one possible value of one feature. Data pre-processing process is a crucial stage to construct an accurate leaning model by using the DL algorithm.

4. RESULTS AND ANALYSIS

In this experiment with Deep Learning architecture, we test OSN social link dataset to measure the accuracy and the performance time. By tuning diverse hyperparameters, we obtain the highest performance of the network. In the training and testing process, we tune epoch = 500, batch size = 50 and with learning rate (lr = 0.01) by feeding 50000 Facebook and 50000 Flickr samples. Table 1 describes the proposed CNN performance, especially in training and testing loss.

Table 1. Performance of proposed CNN with different parameter setting

Optimizer	Training Loss	Testing Loss
Adam	0.5053	0.5059
SGD, *m=0.5*	0.5058	0.5060
Adagrad	0.5047	0.5049
RMSProp	0.5186	0.5213
Adam	0.5042	0.5050
SGD, *m=0.5*	0.5158	0.5162
Adagrad	0.5072	0.5075
RMSProp	0.5082	0.5089

We test gradient descent and tune optimization algorithms with different hyperparameters. The study sets the learning rate η (lr = 0.01) to determine the stride size to reach a (local) minimum. In the training process, we gain the best value of optimization when training the model with Adam optimizer. We feed Adam optimizer into the graph with different amounts of hidden layers. The result shows a dynamic optimizer can achieve a small loss in a large number of hidden layers.

Another gradient descent like SGD with momentum also produces a competitive result. We test the SGD with momentum (m = 0.5) can provide a better result if we tune in larger epoch and big regulizer. However, the experiment reveals that adding more hidden layers for SGD cannot reduce the loss. Using a large number of hidden layer cause overhead computation in a particular device, especially in CPU processing. We find that by adding more layers and neuron numbers of CNN could not engage in improving the predictive capability. Because of the limitation of neuron number, it enlarges computing resources. The experiment results show the classification model can achieve high accuracy with a tiny loss. Notably, the model does not only produce high accuracy, but the graph also runs in better performance.

5. FUTURE RESEARCH DIRECTION

Currently, the popular OSN providers have developed various technologies with the benchmark dataset to enhance the security level in their system. Facebook, LinkedIn, and Twitter have started using artificial intelligence solutions to elevate deep learning capabilities. To flag posts automatically, Facebook adopts AI to detect suicidal thoughts. LinkedIn predicts the highest match for the users' role. Their AI algorithm can predict the most similar people seeking new jobs or connections. Twitter is using a neural system to crops a picture using face detection or making a thumbnail from the whole photo [16].

5.1. Sentiment analysis

Public OSN provides a large-scale sentiment dataset to support the research community. For instance, Amazon that contains a rich dataset with a vast number of customer reviews and a big size of transactions. Several papers have proposed detecting tension models to explore the spikes feature in OSN tension and measures the level of deteriorated in the relationship between individuals or groups [17]. Another paper proposes an ensemble classifier to deal with sentiment analysis [18]. The current study of sentiment analysis adopts a deep learning deal with the sentiment classification [19-20] by calculating Weakly Supervised Multimodal (WSM-DL) [21]. However, it requires a new way to construct a better usage of noisy labels as activity behavior or logs. Sentiment analysis including semantic evaluation with DL algorithms becomes an active research area in further.

5.2. Link prediction

Nowadays, OSN scam issues are arising and growing. The form of the scam activities could coerce the OSN users to send their sensitive information. The model of link prediction can solve the link of scam with a sophisticated technique. The link prediction problem in OSN with the DL approach is hot area research. In this research, some studies utilize the RBM architecture to calculate the unknown or dynamic links between users in an OSN. In link prediction, RBM calculates the unknown or dynamic links between users in a social network environment. It is different from the tasks of the semantic classification crisis response problem [22]. Another experiment has focused on a dynamic setting, predicting the construction and destruction of links in networks. The link anomaly problem is widely used as a security parameter in OSN. A study proposes a link anomaly model to discovering emerging topics in social streams by offering Sequentially Discounting Normalized Maximum Likelihood (SDNM L) and Kleinberg's burst model [23]. The further paradigms of the OSN security and privacy should include reliable and efficient authentication via smart, trust, anonymity, detect traceability, and support link predictions. The conventional statistical technique cannot detect anomalies like zero-day attacks or unexploited vulnerabilities. The further open research topics in this area are recommendation service, network malicious activities, and link classification.

5.3. Anomalous prediction

Malicious detection is kinds of a practical method to build security policies [24]. Thus, the learning approach is a helpful technique for conducting malicious predictions. In a mobile device, a study proposes a DL algorithm to detect malicious activities by constructing a multistage and elastic detection framework [25]. Recent papers adopt behavior technique for malicious detection, COMPA, an approach propose a way to detect compromised accounts behavioral profile and anomaly detection [26], and a study utilizes hybrid features to detect suspicious activities [27]. The next wave of OSN is building OSN adaptive security by utilizing learning methods like CNN and RNN rather than use a traditional rule-based or statistical analysis.

6. CONCLUSION

The current method of OSN protection remains shortcoming in massive data analysis and manual feature engineering. Moreover, standard features engineering is time-consuming and costly. To deal with the issue, modern OSN needs to establish a scalable detection model to deal with modern OSN. Instead of using a conventional technique, we bring the DL architecture as the answer to the OSN malicious problem by analyzing diverse features to train the classifier.

In this paper, we test the deep learning approach to train the OSN dataset for malicious classification. We gather diverse datasets from communities or organizations to construct a good model for OSN protection, including malicious detection. In this experiment, we train the dataset by establishing the supervised learning classifier can learn user activity patterns accurately. Based on the testing, the DL algorithm gains an accurate result to create intelligence protection in OSN. It also can be implemented to optimize learning techniques for business purposes. The deep learning is a reasonable answer to tackle scalability problems such as growing users and data in OSN. The next research of the OSN security method is how to build intelligence and real-time protection scheme than a statistical or rule-based model.

ACKNOWLEDGEMENTS

This paper is conducted in the Institute of Research in Information Processing Laboratory, Harbin University of Science and Technology under CSC Scholarship.

REFERENCES

[1] Wanda, P., & Jie, H.J. Efficient Data Security for Mobile Instant Messenger. *TELKOMNIKA (Telecommunication, Computing, Electronics and Control) Journal*, Vol. 16 (3). 2018.
[2] P. Wanda, Selo and B. S. Hantono *"Efficient message security based HyperElliptic Curve Cryptosystem (HECC) for Mobile Instant Messenger,"* 2014 The 1st International Conference on Information Technology, Computer, and Electrical Engineering, *Semarang, pp. 245-249.* 2014.
[3] W. Putra, Selo and B. S. Hantono "Model of secure P2P mobile instant messaging based on virtual network," *2014 International Conference on Information Technology Systems and Innovation (ICITSI)*, Bandung, pp. 81-85. 2014
[4] Amany A. Naem, Neveen I. Ghali. Optimizing community detection in social networks using antlion and K-median, *Bulletin of Electrical Engineering and Informatics (BEEI),* Vol.8, No.4, December 2019
[5] M. Mohammadrezaei, M E Shiri, A.M Rahmani. "Identifying Fake Accounts on Social Networks Based on Graph Analysis and Classification Algorithms", Hindawi Security and Communication Networks, 2018
[6] M. van Gerven and S. M. Bohte. "Editorial: Artificial neural networks as models of neural information processing," Front. Comput. Neurosci., vol. 11, no. 114, Dec. 2017.
[7] N. F. Fadzail, S. Mat Zali. Fault detection and classification in wind turbine by using artificial neural network. *International Journal of Power Electronics and Drive Systems (IJPEDS).* Vol.16, No.1, 2019.
[8] Parinith R Iyer, Shrutheesh Raman Iyer, Raghavendran Ramesh, Anala M.R., K.N. Subramanya, Adaptive real time traffic prediction using deep neural networks, *IAES International Journal of Artificial Intelligence (IJ-AI).*, Vol.8, No.2. 2019.
[9] Wanda, Putra and Huang J. Jie. "URLDeep: Continuous Prediction of Malicious URL with Dynamic Deep Learning in Social Networks." *I. J. Network Security* 21 pp: 971-978, 2019.
[10] Skymind, "Recurrent networks." Accessed on: Nov. 20, 2018. [Online]. Retrieved: http://skymind.ai/wiki/recurrent-network-rnn
[11] B. Hudson, B. R. Voter. "Profile characteristics of fake twitter accounts", Big Data & Society. 2016.
[12] N. Kökciyan, P. Yolum. "ProGuard: A semantic approach to detect privacy violations in online social networks", *IEEE Trans. Knowl. Data Eng*., vol. 28, no. 10, pp. 2724-2737, Oct. 2016.
[13] E. Van Der Walt and J. Eloff, "Using Machine Learning to Detect Fake Identities: Bots vs Humans*," in IEEE Acces*s, vol. 6, pp. 6540-6549. 2018.
[14] Liu, B.-H., Hsu Y.-P., and Ke W.-C.. "Virus infection control in online social networks based on probabilistic communities." Int. J. Commun. Syst. (2014): 27:4481–4491. 2014

[15] J. Wang, X. He, Q. Gong, Y. Chen, T. Wang and X. Wang. *"Deep Learning-Based Malicious Account Detection in the Momo Social Network,"* 2018 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou, pp. 1-2. 2018.
[16] Albert Smith "Why the Future of Social Media Will Depend on Artificial Intelligence", April 13, 2018, Retrieved https://www.smartdatacollective.com/future-social-media-depend-artificial-intelligence/
[17] P. Burnap, O. F. Rana, N. Avis, M. Williams, W. Housley, A. Edwards, J. Morgan, and L. Sloan. Detecting tension in online communities with computational twitter analysis. Technological Forecasting and Social Change, 95:96–108, June. 2015
[18] Savita Sangam, Subhash Shinde. Sentiment classification of social media reviews using an ensemble classifier. *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS).* Vol. 16, No.1. 2019
[19] Wanda, P., & Jin-jie, H. Model of Sentiment Analysis with Deep Learning in Social Network Environment. *2019 IEEE 2nd International Conference on Electronic Information and Communication Technology (ICEICT)*, 625-630, 2019.
[20] Putra. W, and H. Jin J. DeepSentiment: Finding Malicious Sentiment in Online Social Network based on Dynamic Deep Learning. *IAENG International Journal of Computer Science*, Vol.46, No.4, pp:616-627, 2019
[21] F. Chen, R. Ji, J. Su, D. Cao, and Y. Gao. "Predicting Microblog Sentiments via Weakly Supervised Multimodal Deep Learning," *in IEEE Transactions on Multimedia*, vol. 20, no. 4, pp. 997-1007. 2018
[22] Dat Tien Nguyen, Shafiq R. Joty, Muhammad Imran, Hassan Sajjad, and Prasenjit Mitra. 2016. Applications of online deep learning for crisis response using social media information. CoRRabs/1610.01030 (2016). Retrieved from http://arxiv.org/abs/1610.01030.
[23] T. Takahashi, R. Tomioka, and K. Yamanishi. Discovering emerging topics in social streams via link anomaly detection. *IEEE Transactions on Knowledge and Data Engineering*, 26(1):120–130, December 2014.
[24] Wanda, P., Huang J. Jie. A Survey of Intrusion Detection System, *International Journal of Informatics and Computation (IJICOM)*, Vol. 1, No.1, August, 2019
[25] B. Feng, Q. Fu, M. Dong, D. Guo and Q. Li. "Multistage and Elastic Spam Detection in Mobile Social Networks through Deep Learning*," in IEEE Network*, vol. 32, no. 4, pp. 15-21. 2018
[26] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna. Towards detecting compromised accounts on social networks. *IEEE Transactions on Dependable and Secure Computing*, 14(4):447–460, July. 2017.
[27] Kurapati Subba Reddy, E. Srinivasa Reddy. Integrated approach to detect spam in social media networks using hybrid features. *International Journal of Electrical and Computer Engineering (IJECE)*, Vol.9, No.1. 2019.

BIOGRAPHIES OF AUTHORS

Putra Wanda, received B. Eng in Informatic Engineering in 2011. He graduated with M.Eng. Degrees in Information Technology from Gadjah Mada University 2015. Since August 2016, he is with the School of Computer Science and Technology from Harbin University of Science and Technology as a Ph.D. candidate. He has published several papers in the network and information security both in conferences and journals indexed by Scopus and EI Compendex. https://orcid.org/0000-0003-0130-3196

Marselina Endah H, received B. Eng in Informatic Engineering. She graduated from M.Cs. Degrees in Computer Science from Gadjah Mada University, Indonesia. She is a lecturer in the Department of Informatics, the University of Respati Yogyakarta. She has published several papers in information technology areas both in conferences and journals indexed by Scopus.

Huang J. Jie is a Professor and Ph.D. Supervisor in the School of Science and Technology, Harbin University of Science and Technology, China. His current research interests include Deep Learning, Robotic and Automation Publish many articles in the robotic system and pattern recognition indexed by SCI and EI Compendex. https://orcid.org/0000-0002-2107-2690