Journal of Information Technology and Digital World (2020)
Vol.02/ No. 02
Pages: 108-115
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2020.2.004

Social Multimedia Security and Suspicious Activity Detection in SDN using Hybrid Deep Learning Technique

Dr. Joy Iong Zong Chen,
Professor,
Department of Electrical Engineering,
Da-Yeh University,Taiwan.
Email id: jchen@mail.dyu.edu.tw

Dr. S. Smys,
Professor,
Department of CSE,
RVS Technical Campus,
Coimbatore, India.
Email id: smys375@gmail.com

Abstract: Social multimedia traffic is growing exponentially with the increased usage and continuous development of services and applications based on multimedia. Quality of Service (QoS), Quality of Information (QoI), scalability, reliability and such factors that are essential for social multimedia networks are realized by secure data transmission. For delivering actionable and timely insights in order to meet the growing demands of the user, multimedia analytics is performed by means of a trust-based paradigm. Efficient management and control of the network is facilitated by limiting certain capabilities such as energy-aware networking and runtime security in Software Defined Networks. In social multimedia context, suspicious flow detection is performed by a hybrid deep learning based anomaly detection scheme in order to enhance the SDN reliability. The entire process is divided into two modules namely – Abnormal activities detection using support vector machine based on Gradient descent and improved restricted Boltzmann machine which facilitates the anomaly detection module, and satisfying the strict requirements of QoS like low latency and high bandwidth in SDN using end-to-end data delivery module. In social multimedia, data delivery and anomaly detection services are essential in order to improve the efficiency and effectiveness of the system. For this purpose, we use benchmark datasets as well as real time evaluation to experimentally evaluate the proposed scheme. Detection of malicious events like confidential data collection, profile cloning and identity theft are performed to analyze the performance of the system using CMU-based insider threat dataset for large scale analysis.

Keywords: Social multimedia; Software defined networks; Flow routing; Deep learning; Anomaly detection;

1. Introduction

The popularity of social networking has improved with the expansion of web from web of things to web of thoughts [1]. For societies, groups as well as individuals, creation of new opportunities is made possible by understanding the human behaviour on a dynamic basis, making this the richest and largest technology. The total social-media users that are active sums up to around three billion worldwide out of the four billion internet users according to insights into world social media [2], [3]. There is an unprecedented growth in the multimedia content with the social network proliferation. The ever

ISSN: 2582-418X (online)
Information Technology & Digital World

Journal of Information Technology and Digital World (2020)
Vol.02/ No. 02
Pages: 108-115
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2020.2.004

growing and vibrant pool of data imposes several challenges in gaining meaningful insights due to the object oriented and content driven nature of social multimedia. Private and sensitive user data and interactions are available in social networks along with substantial multimedia content. Identity theft and other information theft occurs due to the high vulnerability of personal information and abundant readily available data [4]. The underlying architecture faces two major challenges namely security and interoperability. While maintaining the security at an adequate level, social multimedia information has to be managed and analysed for enabling pervasive and scalable communication [5].

The multimedia content is growing in an unprecedented manner across internet with the growing popularity of social networks. Along with this prolific development, a wide variety of attacks are launched by intruders on the internet industry in terms of obfuscated malicious URL, malware distribution, account hijacking, phishing attacks and impersonation attacks. The social networking sites and their widespread popularity is exploited by these attacks. The major challenges faced by the research community in terms of social media content are security and interoperability [6]. Overcoming these issues is the need of the hour by designing and developing scalable and pervasive communication paradigm.

2. Related Works

In various multimedia applications like online gaming, real-time content delivery, video conferencing, remote video-on-demand and so on, despite the perpetrated attacks of the malicious users, the network can be protected using several anomaly detection models designed by the cybersecurity researchers [7]. Recurrent Neural Networks (RNN), Stacked Auto-Encoders, Restricted Boltzmann Machine (RBM), Deep Belief Network (DBN), Convolution Neural Network (CNN), and such deep learning architectures are used widely. In order to extricate spatiotemporal data from the inputs, 3 dimensional CNN is used in the videos for abnormal event detection [8]. The SVM's probabilistic outputs decides the intra-frame classification strategies and stacked sparse coding for detecting unusual events in multimedia such as videos. In crowded activities, anomalies can be detected using CNN [9].

The performance of Convolutional Autoencoder (CAE) and influence of anomaly detection technique by analysis of input frames for high-level feature aggregation is performed by researchers [10]. A combination of multiple one-class SVM models and deep neural networks for anomaly detection in video data based on Motion and Appearance DeepNet model is proposed. In order to explore the patterns of video events, a deep Gaussian mixture model is used and feature learning is performed using PCANet for abnormal event detection using deep learning techniques [11-13]. Long-Short Term Memory and CNN schemes are integrated for detection of abnormal emotions in social media using a propounded a hybrid neural network model. In comparison with the existing machine learning algorithms, pattern recognition applications widely makes use of these techniques due to their representation learning and end-to-end training [14]. The combination of reinforcement learning along with these techniques is of potential benefits as massive amount of data requires computationally expensive techniques for training using deep learning methods.

ISSN: 2582-418X (online)
Information Technology & Digital World

Journal of Information Technology and Digital World (2020)
Vol.02/ No. 02
Pages: 108-115
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2020.2.004

3. Proposed Work

SDN platform assisted end-to-end delivery for social multimedia domain for detection of network anomaly is presented in this paper. Support Vector Machine (SVM) and Restricted Boltzmann machine (RBM) based ensemble approach is presented for detection of anomaly. Gradient descent approach and mixed kernel function encapsulation schemes are applied for improving the SVM by incorporating the dropout functionality for revamping the performance of RBM. We design a routing scheme for multi-objective flow based SDN and delivery of end-to-end social media traffic [15]. Energy utilization and consumption, bandwidth, latency and such trade-offs exists on implementation of this scheme. The benchmark as well as real-time datasets are used for evaluation of the performance of the designed model.

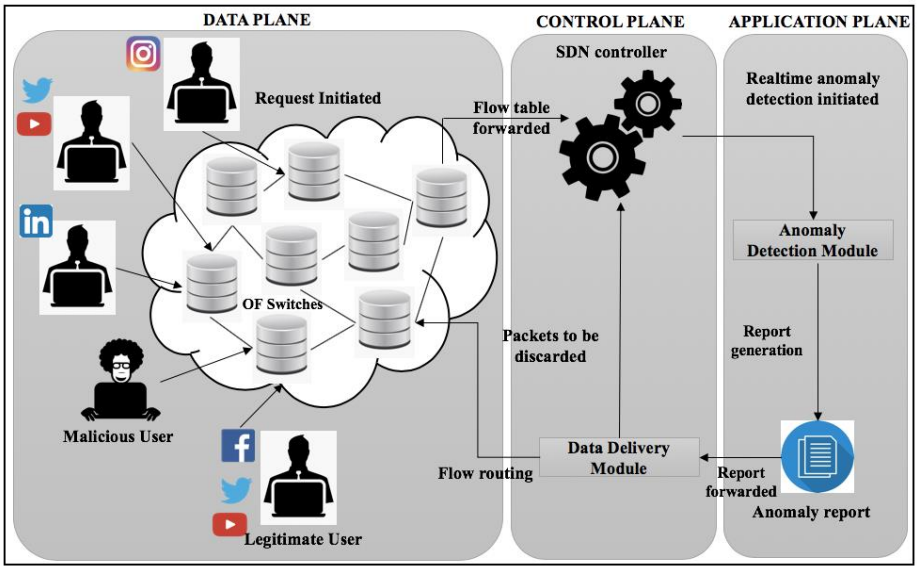

Figure 1: Anomaly Detection Framework System model

From the physical network topology, the network control plane is decoupled using dynamic and scalable reconfigurable architecture of the SDN in this setup. Without altering the fundamental physical network components, the standard interfaces, SDN controller and centralized controller are used for implementation of the network control decisions on integration of SDN. In multiple server based applications and operations of multimedia service, in order to maintain load balancing, various nodes can interact with each other due to its programming ability [16]. The control centers maintains all the intelligent data and the multimedia devices are considered dumb. Hence, along with reliable and fast communication, convenient control is also offered by embedding SDN in multimedia analytics. As shown in Figure 1, in order to provide Quality of Experience (QoE), data delivery module and anomaly detection module are implemented in the proposed framework.

ISSN: 2582-418X (online)
Information Technology & Digital World

Journal of Information Technology and Digital World (2020)
Vol.02/ No. 02
Pages: 108-115
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2020.2.004

4. Results and Discussion

The proposed model is evaluated with a real-time social multimedia dataset. Across the time horizon, anomalous traffic is injected for evaluation of the considered dataset. The total packets for malicious and benign instances are analyzed. Substantial amount of anomalies are detected in the generated dataset based on the results of analysis. The relevant feature sets are extracted by employing dropout functionality based improved RBM in the first phase. The designed RBM performance is further analyzed. With the increase in number of data packets, the classification error rate reduces considerably by the dropout functionality based RBM. In case of standard RBM that does not contain dropout functionality, a similar trend is observed. However, in comparison with the later, the former RBM exhibits improved performance.

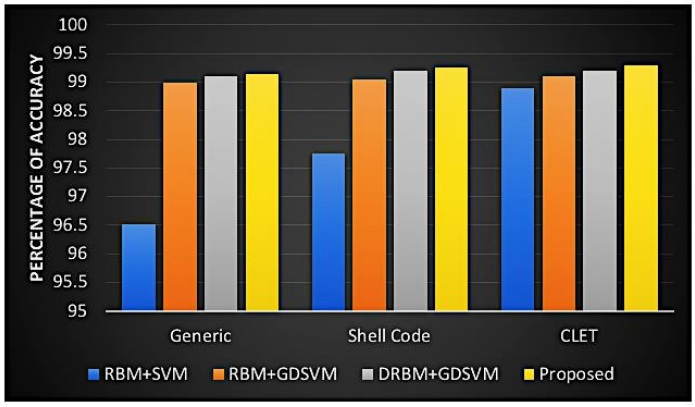

Figure 2: Real-time dataset based evaluation of proposed model

The designed SVM powered with mixed kernel and gradient descent is used for classification of instances of data proposed anomaly detection model in the next phase. The proposed model is compared with three other variants for evaluation of performance namely standard SVM and RBM, standard gradient descent (GDSVM) and RBM and GDSVM and dropout coupled RBM (DRBM). The results comparing these three models is estimated and analyzed. Based on this analysis, it is evident that, when compared with the other techniques, the proposed model offers improved performance with a 0.97 highest area under the curve (AUC). The RBM+SVM offers performance of 0.93, RBM+GDSVM offers performance of 0.94, and DRBM+GDSVM offers performance of 0.97 under the proposed model.

KDD'99 dataset is tested and evaluated extensively for the proposed anomaly detection model with respect to the existing state-of-the-art models. Table 1 provides the captured traffic snippets of the user access to different social networking platforms such as WhatsApp, Instagram, twitter, Facebook etc. in which HTTP requests are available in majority. On analysis on the KDD'99 dataset with the

ISSN: 2582-418X (online)
Information Technology & Digital World

Journal of Information Technology and Digital World (2020)
Vol.02/ No. 02
Pages: 108-115
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2020.2.004

proposed model, the major performance parameters such as F-score, precision, accuracy, FPR and DR are recorded and summarized. The probe data instances is 99.03%, R2L at 99%, U2R at 98.9%, DOS at 99% and normal at 99% are the values corresponding the detection rate evaluation. Based on the results obtained, on comparison, it is evident that the U2R attacks are least detected when compared to DOS attacks. U2R offers highest detection rate and FPR offers minimum detection rate on similar lines. Figure 3 represents the accuracy percentage across various class types obtained in detecting probe data, R2L, U2R, DOS and normal instances. F-score parameters and precision is also analyzed to observe the performance of the proposed scheme.

Table 1: Network traffic characteristics

File	Burst Rate	Rate	HTTP Count	Packet Count
Capture 1	2.7	1.5	12100	320856
Capture 2	3	1.1	13230	316728
Capture 3	2.1	1	8820	316523
Capture 4	2.2	1.2	8290	318344
Capture 5	2.6	1	11070	321345
Capture 6	2.5	1.2	9740	319453
Capture 7	3	1.3	10440	314532
Capture 8	2.4	1.2	11010	319365
Capture 9	2.3	1.2	10840	316845
Capture 10	3.3	1.3	10610	316084

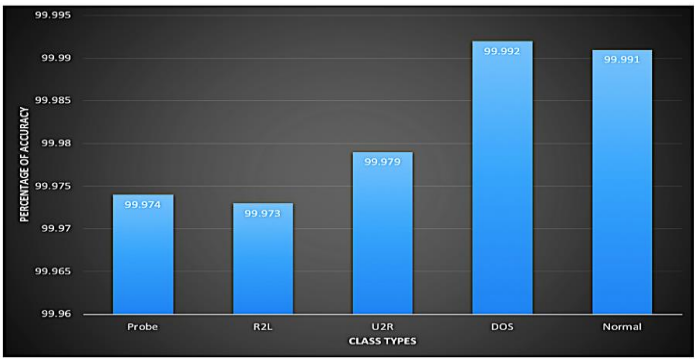

Figure 3: Benchmark KDD'99 dataset based evaluation on proposed model

A reference data base CMU insider threat dataset is chosen for the proposed anomaly detection module for evaluating the effectiveness. The insider threats and other social networking attacks are crucial classes that are depicted by the datasets. This acts as the motivation for the evaluation work described in this paper. File transfer, email log files and device connections along with web-browsing logs are the major publicly available datasets that are exposed to insider threat analysis. Here we have considered around 14GB of this data for analysis. On the concept of deep autoencoders, the existing scheme is analyzed on a comparative basis with this dataset.

ISSN: 2582-418X (online)
Information Technology & Digital World

Journal of Information Technology and Digital World (2020)
Vol.02/ No. 02
Pages: 108-115
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2020.2.004

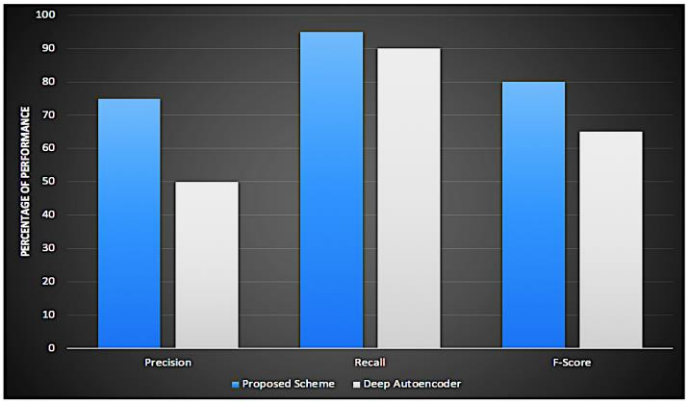

Figure 4: Insider threat dataset -CMU based comparative evaluation

Over a time duration of 1.5 years, the activity log of about thousand insiders that are user-specific are used for depicting the datasets. psychometric.csv, http.csv, email.csv, file.csv, device.csv, and logon.csv are some of the available datasets and user activity logs available in different files. Three different scenarios of insider attacks are used for defining the dataset. The first scenario depicts the case where passwords are obtained by the user by installing keylogger. The second scenario represents theft of confidential information by a user and the third scenario depicts the user's abnormal behavior. Comparison of the proposed anomaly detection module for performance evaluation on the basis of these three scenarios is done. F-score, recall and precision factors and their supremacy is used for alignment of the existing scheme in comparison with the proposed scheme.

5. Conclusion

Today's networks are exposed to several risks of network security due to the growing popularity of Social media networking platforms like twitter, WhatsApp, Instagram, Facebook and so on. For end-to-end delivery of the fundamental information, it is essential to monitor and analyze the real time traffic of social media. The data delivery module enabled with SDN is coupled with a real-time anomaly detection scheme to offer a solution to the above mentioned problem. For efficient detection of anomalies, the gradient-descent approach is combined with the mixed kernel SVM encapsulation along with the dropout functionality enabled improved RBM are enabled which offer several advantages to the system. Based on the SDN, a routing scheme with multi-objective flow is enabled for efficient delivery of data. When compared with the existing state-of-the-art models, the proposed model offers impressive outcomes on evaluation with benchmark as well as real-time datasets. The datasets like CMU, KDD'99 and TIET are used in which the detection rate of over 99% is achieved on application of the proposed schemes. Smart homes, unmanned aerial vehicles, intelligent transportation systems, smart grids and so on are some of the applications in which the proposed framework can be implemented.

ISSN: 2582-418X (online)
Information Technology & Digital World

Journal of Information Technology and Digital World (2020)
Vol.02/ No. 02
Pages: 108-115
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2020.2.004

References

[1] You, Q., Luo, J., Jin, H., & Yang, J. (2016, February). Cross-modality consistent regression for joint visual-textual sentiment analysis of social multimedia. In *Proceedings of the Ninth ACM international conference on Web search and data mining* (pp. 13-22).

[2] Nie, L., Zhang, L., Wang, M., Hong, R., Farseev, A., & Chua, T. S. (2017). Learning user attributes via mobile social multimedia analytics. *ACM Transactions on Intelligent Systems and Technology (TIST)*, *8*(3), 1-19.

[3] Bischke, B., Bhardwaj, P., Gautam, A., Helber, P., Borth, D., & Dengel, A. (2017, September). Detection of Flooding Events in Social Multimedia and Satellite Imagery using Deep Neural Networks. In *MediaEval*.

[4] Chaudhry, S. A. (2016). A secure biometric based multi-server authentication scheme for social multimedia networks. *Multimedia Tools and Applications*, *75*(20), 12705-12725.

[5] Adhikary, T., Das, A. K., Razzaque, M. A., Alrubaian, M., Hassan, M. M., & Alamri, A. (2017). Quality of service aware cloud resource provisioning for social multimedia services and applications. *Multimedia Tools and Applications*, *76*(12), 14485-14509.

[6] You, Q. (2016, October). Sentiment and emotion analysis for social multimedia: Methodologies and applications. In *Proceedings of the 24th ACM international conference on Multimedia* (pp. 1445-1449).

[7] Li, C. T., Shan, M. K., Jheng, S. H., & Chou, K. C. (2016). Exploiting concept drift to predict popularity of social multimedia in microblogs. *Information Sciences*, *339*, 310-331.

[8] Petkos, G., Schinas, M., Papadopoulos, S., & Kompatsiaris, Y. (2017). Graph-based multimodal clustering for social multimedia. *Multimedia Tools and Applications*, *76*(6), 7897-7919.

[9] Luo, J., Borth, D., & You, Q. (2017, October). Social multimedia sentiment analysis. In *Proceedings of the 25th ACM international conference on Multimedia* (pp. 1953-1954).

[10] Garg, S., Kaur, K., Kumar, N., Kaddoum, G., Zomaya, A. Y., & Ranjan, R. (2019). A hybrid deep learning-based model for anomaly detection in cloud datacenter networks. *IEEE Transactions on Network and Service Management*, *16*(3), 924-935.

[11] Haider, S., Akhunzada, A., Ahmed, G., & Raza, M. (2019, August). Deep Learning based Ensemble Convolutional Neural Network Solution for Distributed Denial of Service Detection in SDNs. In *2019 UK/China Emerging Technologies (UCET)* (pp. 1-4). IEEE.

[12] Singh, A., Aujla, G. S., Garg, S., Kaddoum, G., & Singh, G. (2019). Deep Learning-based SDN Model for Internet of Things: An Incremental Tensor Train Approach. *IEEE Internet of Things Journal*.

[13] Garg, S., Kaur, K., Kaddoum, G., Ahmed, S. H., & Jayakody, D. N. K. (2019). SDN-based secure and privacy-preserving scheme for vehicular networks: a 5G perspective. *IEEE Transactions on Vehicular Technology*, *68*(9), 8421-8434.

[14] Garg, S., Kaur, K., Batra, S., Kaddoum, G., Kumar, N., & Boukerche, A. (2020). A multi-stage anomaly detection scheme for augmenting the security in IoT-enabled applications. *Future Generation Computer Systems*, *104*, 105-118.

[15] Karthiban, M. K., & Raj, J. S. (2019). BIG DATA ANALYTICS FOR DEVELOPING SECURE INTERNET OF EVERYTHING. *Journal of ISMAC*, *1*(02), 129-136.

ISSN: 2582-418X (online)

Journal of Information Technology and Digital World (2020)
Vol.02/ No. 02
Pages: 108-115
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2020.2.004

[16] Bashar, A. (2019). SURVEY ON EVOLVING DEEP LEARNING NEURAL NETWORK ARCHITECTURES. *Journal of Artificial Intelligence*, *1*(02), 73-82.

Authors Biography

Dr. Joy Iong-Zong Chen is currently a full professor of Department of Electrical Engineering Dayeh University at Changhua Taiwan. Prior to joining the Dayeh University, he worked at the Control Data Company (Taiwan) as a technical manager since Sep. 1985 toSep. 1996. His research interests include wireless communications, spread spectrum technical, OFDM systems, and wireless sensor networks. He has published a large number of SCI Journal papers in theissues addressed physical layer for wireless communication systems. Moreover, he also majors in developing some applications of the IOT (Internet of Thing) techniques and Dr. Joy I.-Z. Chen owned some patents authorized by the Taiwan Intellectual Property Office (TIPO)

Dr. S. Smys received his M.E and Ph.D degrees all in Wireless Communication and Networking from Anna University and Karunya University, India. His main area of research activity is localization and routing architecture in wireless networks. He serves as Associate Editor of Computers and Electrical Engineering (C&EE) Journal, Elsevier and Guest Editor of MONET Journal, Springer. He is served as a reviewer for IET, Springer, Inderscience and Elsevier journals. He has published many research articles in refereed journals and IEEE conferences. He has been the General chair, Session Chair, TPC Chair and Panelist in several conferences. He is member of IEEE and senior member of IACSIT wireless research group. He has been serving as Organizing Chair and Program Chair of several International conferences, and in the Program Committees of several International conferences. Currently he is working as professor in department of computer science in RVS technical campus, in Tamilnadu, India

ISSN: 2582-418X (online)
Information Technology & Digital World