Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 8, pp. 2409–2417
DOI : 10.47974/JDMSC-2014

Advancing cyber threat detection through deep learning in management information systems

S. Arvind *
Department of Computer Science & Engineering
Hyderabad Institute of Technology and Management
Hyderabad 501401
Telangana
India

Bhuvan Unhelkar †
Muma College of Business
University of South Florida
8350 N. Tamiami Trail Sarasota
Florida 33620
USA

S. Siva Shankar §
Department of Computer Science and Engineering
KG Reddy College of Engineering and Technology
Hyderabad 500100
Telangana
India

Prasun Chakrabarti ‡
Department of Computer Science and Engineering
Sir Padampat Singhania University
Udaipur 313601
Rajasthan
lndia

* *E-mail:* **scarvi@rediffmail.com (Corresponding Author)**
† *E-mail:* **bunhelkar@usf.edu**
§ *E-mail:* **drsivashankars@gmail.com**
‡ *E-mail:* **drprasun.cse@gmail.com**

S. V. Devika [@]
Department of Electronics and Communications Engineering
Hyderabad Institute of Technology and Management
Hyderabad 501401
Telangana
India

Abstract

Cloud computing, fulfilling the "Computing as Utility" model, is widely popular for providing on-demand services. However, the primary challenge for cloud providers is the increasing vulnerability to cyber-attacks. Traditional detection methods are insufficient, necessitating advanced approaches. This research suggests a mechanism for detecting cyberattacks using deep learning for Cloud Computing, employing a hybrid CNN and Self-Organizing Maps (SOM) methodology. The two-dimensional representation of input space facilitates the identification of assaults known as distributed denial of service (DDoS), achieving superior results compared to existing techniques in terms of lower detection times (1.2 seconds), and higher accuracy (97%), precision (96%), and recall (97%).

Subject Classification: *68M25, 68U01.*

Keywords: *Cloud computing, Cyber-attacks, Convolutional neural network (CNN), Self-organizing map (SOM), Cloud computing, Management information systems.*

1. Introduction

Organizations adopt cloud computing for its fast and efficient service delivery, but the associated data security and privacy concerns necessitate robust measures [1]. The creation of multiple virtual machines in cloud networks poses challenges, as any contact can be a potential avenue for corruption or unauthorized access [2].

Cloud computing architecture involves front-end and back-end components, with security being a paramount concern for safeguarding against cyber-attacks [3]. The integration of public and private sectors in a single service provider exposes cloud infrastructures to various illegal cyber-attacks [4], further complicated by access from diverse mobile devices [5].

Network security situation awareness is crucial for enterprise security, addressing challenges in cloud system cyber-attack detection, including zero-day attacks and designing efficient anomaly-based algorithms [6] [7].

[@] *E-mail:* **drdevikasv@gmail.com**

In this paper, a Deep Learning method utilizing CNN and Self-organizing maps (SOM) is proposed [8] for efficient attack detection on cloud infrastructures, covering literature survey, Deep Learning-Based Cyberattack Detection, Experiments, and Conclusion in Sections II to V.

II. Literature survey

Kumar et al. [8] present SAFETY, using entropy and SDN, improving processing delay by 13%, enhancing TCP SYN flooding detection in Floodlight controller. Choraś and Kozik [9] focus on defending against increasing application layer cyber-attacks, utilizing dynamic programming and graph-based segmentation with satisfactory results. Pawlick and Zhu [10] introduce "strategic trust" using game theory for CPS security, proposing a trust mechanism for cloud-assisted insulin pumps, ensuring robustness without past data. Gopalakrishnan et al. [11] propose DLTPDO-CD, a technique using Bidirectional LSTM for traffic prediction, ASCE for efficient data offloading, and BMO-DBN for cyber-attack detection with superior performance.

Hahn et al. [12] address verifiability in mobile healthcare systems, presenting a countermeasure strategy against attacks, outperforming MAC-based schemes in experimental research. Elgendi et al. [13] suggest a foundation model (MAPE-K) for CPS self-adaptation, achieving a 99.55% accuracy rate in identifying cyber threats in an industrial setting. Conti et al. [14] propose KYE, a technique for defending against attacks aiming to obtain network configuration information, offering active defence countermeasures. Zhang et al. [15] offer a defence-in-depth method that uses host system, process parameter, and network traffic monitoring to identify cyberattacks in industrial control systems.

Karimipour et al. [16] introduce a state estimation method protecting against False Data Injection attacks, showcasing accuracy and efficiency through numerical simulations. Yang et al. [17-19] created a zone partitioning-based anomaly detection technique for Industrial Cyber-Physical Systems that provides a high-accuracy, real-time solution. Ozay et al. [20-22] classify measurements as secure or attacked using machine learning, demonstrating the superiority of machine learning algorithms over state vector estimation techniques.

III. Cyber attacks detection

In the depicted Figure 1, the block diagram outlines Cyber attack detection using Deep Learning for Cloud Computing. The system in the

cloud gathers events from network gateway traffic monitoring and control system records. Preprocessing standardizes log formats before correlation between suspicious events in system logs and network traffic.

Data preprocessing is crucial in deep learning, data mining, and machine learning, involving modifications and eliminations to enhance performance. It readies data for processing during training, ensuring efficiency with large datasets.

Post-preprocessing, network traffic data extracts special features for training and testing datasets through cross-validation. Feature selection minimizes computational complexity while maintaining accuracy, grouping similar features.

This HCN module, with honeypot sensors, seems to investigate the attackers in a cloud environment. It combines the Convolutional Neural Network with Self-Organizing Map to detect cyberattacks. A multilayer neural network, CNN makes use of convolution and pooling techniques, while SOM focuses on dimensionality reduction in unsupervised learning with data clustering.

The trained hybrid classifier (CNN+SOM) is tested for detection time, accuracy, precision, and recall in the experimental phase.

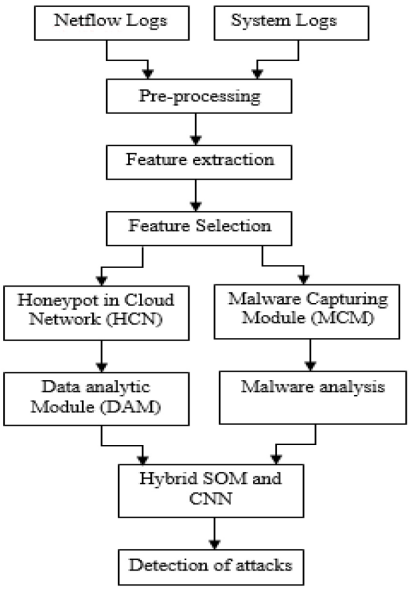

Figure 1

Block diagram of cyber-attack detection model

IV. Result analysis

This section presents the performance analysis of the suggested hybrid classifier (CNN+SOM). Trained on Netflow and system logs, the model utilizes Netflow logs for cloud network flow data and Syslog for host events. Logs, securely stored, serve as proof for accuracy, guarding against actual attacker compromise. The system, deployed on a public IP network for around 45 days, collected significant data entered into a database. The signature-based detection engine processed attack network logs, evaluated results based on accuracy metrics, and categorized findings as normal or abnormal using standard machine learning benchmarks (TP, FP, TN, FN) for performance assessment.

Accuracy: the percentage of correctly located samples throughout the whole dataset.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FN+FP} \tag{1}$$

Precision is the percentage of correctly detected positively classed samples.

$$\text{Precision} = \frac{TP}{TP+FP} \tag{2}$$

When compared to all samples in the relevant class, recall is the percentage of accurately predicted samples that were positive.

$$\text{Recall} = \frac{TP}{TP+FN} \tag{3}$$

The detection rate in the Cyber Attacks Detection model measures the time for accurate detection. Table 1 summarizes the process of performing a performance analysis, which entails comparing the hybrid classifier (CNN+SOM) with other models like Artificial Neural Network (ANN) and Deep Neural Network (DNN). Figure 2 presents a graphical depiction of the Precision and Recall characteristics, while Figure 3 showcases the accuracy of different cyber-attack detection techniques.Top of Form

Figures 2 and 3 clearly indicate higher performance parameters for the hybrid classifier (CNN+SOM) compared to other models, highlighting its effectiveness. Figure 4 presents the detection time of the three models.

The data reveals four types of attacks: Denial of Service (DoS), Remote to Local Attack (R2L), User to Root (U2R), and Probing Attack (Probe). The percentage of these cyberattacks that were detected is shown in Table 2.

Table 1

Comparative performance analysis

Attack detection models	Accuracy (%)	Precision (%)	Recall (%)	Detection time (sec)
ANN	85	86	84	7
DNN	89	90	88	8
CNN+SOM	97	96	97	1.2

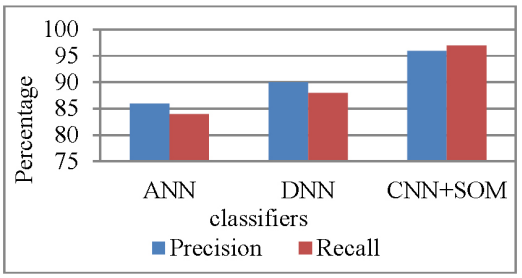

Figure 2

Comparative analysis in terms of precision and recall parameters

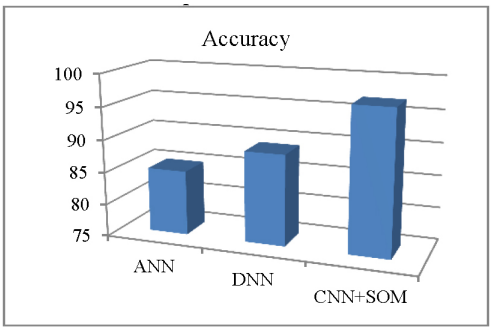

Figure 3

Comparative analysis in terms of accuracy

The accuracy percentage of the given model (CNN+SOM) is equal to the average % across attack categories.

Results confirm the efficiency of the Cyber Attacks Detection model based on Deep Learning for Cloud Computing (CNN+SOM) in contrast to the two previous types. The model presented exhibits a great degree of Accuracy (97%), Precision (96%), Recall (97%), and minimal Detection Time (1.2 sec).

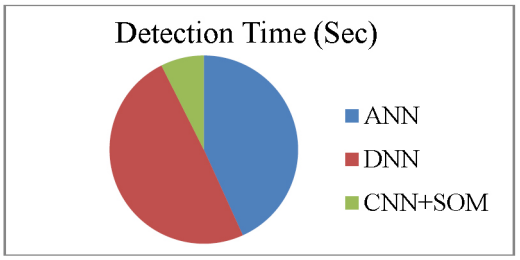

Figure 4

Detection time

Table 2

Detection percentage of different cyber-attacks

Attack Type	Detection percentage (%)
DoS	97.5
Probe	96.5
R2L	97.5
U2R	96.5

V. Conclusion

This paper introduces Cyber-attack detection in Cloud Computing using Deep Learning (CNN+SOM). Focused on cloud service providers' primary threat of cyber-attacks, the detection system utilizes system logs and network gateway traffic monitoring in the cloud environment. The study employs a combination of CNN and SOM for detecting cyber-attacks and validates the model through accuracy, precision, recall, and detection time parameters. The model identifies four attack types (DoS, R2L, Probe, U2R) with high accuracy (97%), precision (96%), recall (97%), and a low detection time (1.2 sec). The described method proves more effective in cyber-attack detection compared to existing models.

References

[1] M. T. Islam, S. Karunasekera, and R. Buyya, "Performance and cost-efficient spark job scheduling based on deep reinforcement learning in cloud computing environments," *IEEE Transactions on Parallel and Distributed Systems*, vol. 33, no. 7, pp. 1695–1710, Jul. (2021).

[2] S. Gore, P. K. Mishra, and S. Gore, "Improvisation of Food Delivery Business by Leveraging Ensemble Learning with Various Algorithms," in Proc. 2023 Int. Conf. Self Sustainable Artificial Intelligence Systems (ICSSAS), pp. 221–229, Oct. (2023).

[3] S. An, A. Leung, J. B. Hong, T. Eom, and J. S. Park, "Toward automated security analysis and enforcement for cloud computing using graphical models for security," *IEEE Access*, vol. 10, pp. 75117–75134 (2022).

[4] B. J. Dange, S. Hamsa, G. Patil, S. Gore, S. Roychowdhury, and S. Karmode, "Grape vision: a CNN-based system for yield component analysis of grape clusters," *Int. J. Intell. Syst. Appl. Eng.*, vol. 11, no. 9s, pp. 239–244 (2023).

[5] P. Mishra, V. Varadharajan, E. S. Pilli, and U. Tupakula, "VMGuard: A VMI-based security architecture for intrusion detection in cloud environment," *IEEE Transactions on Cloud Computing*, vol. 8, no. 3, pp. 957–971 (2018).

[6] S. Puri and M. Agnihotri, "A proactive approach for cyber attack mitigation in cloud network," in Proc. 2017 Int. Conf. Energy, Commun., Data Analytics Soft Comput. (ICECDS), pp. 171–176, Aug. (2017).

[7] D. Garg and R. Agarwal, "Cyber Attacks in Cloud Computing Environment," in Proc. 2023 8th Int. Conf. Commun. Electron. Syst. (ICCES), pp. 471–475, Jun. (2023).

[8] P. Kumar, M. Tripathi, A. Nehra, M. Conti, and C. Lal, "SAFETY: Early detection and mitigation of TCP SYN flood utilizing entropy in SDN," *IEEE Transactions on Network and Service Management*, vol. 15, no. 4, pp. 1545–1559, Dec. (2018).

[9] M. Choraś and R. Kozik, "Machine learning techniques applied to detect cyber attacks on web applications," *Logic J. IGPL*, vol. 23, no. 1, pp. 45–56, Jun. 20232015).

[10] J. Pawlick and Q. Zhu, "Strategic trust in cloud-enabled cyber-physical systems with an application to glucose control," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 12, pp. 2906–2919, Dec. (2017).

[11] T. Gopalakrishnan, M. S. A. R. Anwar, R. S. G. K. Basha, and A. K. Sangaiah, "Deep learning enabled data offloading with cyber attack detection model in mobile edge computing systems," *IEEE Access*, vol. 8, pp. 185938–185949 (2020).

[12] C. Hahn, H. Kwon, and J. Hur, "Trustworthy delegation toward securing mobile healthcare cyber-physical systems," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6301–6309, Aug. (2018).

[13] B. Agheli, M. Adabitabar Firozja, and H. Garg, "Similarity measure for Pythagorean fuzzy sets and application on multiple criteria decision making," *J. Stat. Manag. Syst.*, vol. 25, no. 4, pp. 749–769 (2022).

[14] I. Elgendi, M. F. Hossain, A. Jamalipour, and K. S. Munasinghe, "Protecting cyber physical systems using a learned MAPE-K model," *IEEE Access*, vol. 7, pp. 90954–90963 (2019).

[15] M. Conti, F. De Gaspari, and L. V. Mancini, "A novel stealthy attack to gather SDN configuration-information," *IEEE Transactions on Emerging Topics in Computing,* vol. 8, no. 2, pp. 328–340, Apr. (2018).

[16] A. Hanwa and E. Fouotsa, "Elliptic divisibility sequences over the Edwards model of elliptic curves," *J. Discrete Math. Sci. Cryptogr.,* vol. 25, no. 8, pp. 2289–2304 (2022).

[17] F. Zhang, H. A. D. E. Kodituwakku, J. W. Hines, and J. Coble, "Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data," *IEEE Transactions on Industrial Informatics,* vol. 15, no. 7, pp. 4362–4369, Jul. (2019).

[18] P. Girdhar, P. Johri, and D. Virmani, "Incept_LSTM: Accession for human activity concession in automatic surveillance," *J. Discrete Math. Sci. Cryptogr.,* vol. 25, no. 8, pp. 2259–2273 (2022).

[19] H. Karimipour and V. Dinavahi, "Robust massively parallel dynamic state estimation of power systems against cyber-attack," *IEEE Access,* vol. 6, pp. 2984–2995 (2017).

[20] J. Yang, C. Zhou, S. Yang, H. Xu, and B. Hu, "Anomaly detection based on zone partition for security protection of industrial cyber-physical systems," *IEEE Transactions on Industrial Electronics,* vol. 65, no. 5, pp. 4257–4267, May (2017).

[21] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Transactions on Neural Networks and Learning Systems,* vol. 27, no. 8, pp. 1773–1786, Aug. (2015).

[22] N. Besharati and M. Mortezaeefar, "Determination of the size of defining set for Steiner triple systems," *J. Discrete Math. Sci. Cryptogr.,* vol. 25, no. 8, pp. 2217–2235 (2022).

Received February, 2024