IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

3rd-International Conference on Muti-Disciplinary Application & Research Technologies (ICMART-2024)

Geetanjali Institute of Technical Studies

Vol. 11, Special Issue 2, May 2024

Survey paper on Machine Learning for Cyber-crime detection

Radhika Sreedharan

Assistant Professor, Department of Computer Science and Engineering, Presidency University, Bangalore, India

Abstract: Cybercrime is the term for criminal activity that includes the deliberate use or targeting of a computer, computer network, or networked device. Most cybercrime is committed by hackers or cybercriminals who want to make money off of their crimes. But occasionally, cybercrime aims to damage systems or networks for objectives other than monetary gain. They could have political or personal implications. Both people and organizations conduct cybercrime. Certain cybercriminals possess advanced technical skills, exhibit excellent organization, and utilize state-of-the-art techniques. There are those that are not particularly skilled hackers. The main of this paper is to explore machine learning approaches for detecting various types of cyber-crimes.

Keywords: cyber-crime, machine learning, cyber-attack, deep learning

I. INTRODUCTION

An intrusion detection system (IDS) is a type of network security technology that was initially created to detect possible attacks against a particular machine or program. The IDS is also a listen-only device. The traffic monitoring of the IDS provides results to an administrator. An intrusion detection system (IDS) is a monitoring system that searches for abnormal behavior and notifies users when it finds it. Based on these alerts, an incident responder or security operations center (SOC) analyst can investigate the issue and take the required action to remove the threat.

Cyber-attacks are attacks by cybercriminals using one or more computers on one or more computers or networks. A compromised computer may be used by a cyberattacker to launch more attacks, steal data, or purposefully take down devices.

To launch a cyberattack, cybercriminals utilize several tactics like malware, phishing, ransomware, and denial of service. A wide range of freshly discovered security vulnerabilities that hackers can use to infiltrate systems are referred to as "zero-day" vulnerabilities. The term "zero-day" refers to a scenario where the vendor or developer has recently become aware of the issue and so has "zero days" to address it. A zero-day attack occurs when hackers exploit a vulnerability before engineers have an opportunity to patch it.

Zero-day is occasionally written as 0-day. The phrases exploit, attack, and vulnerability are often used in conjunction with zero-day vulnerabilities; it's crucial to understand their distinctions:

- A zero-day vulnerability is a software flaw that is discovered by attackers before the vendor is made aware of it. Because suppliers are unaware of zero-day vulnerabilities, there is unlikely to be a fix, making attacks more successful.
- Hackers use a method called a zero-day exploit to attack systems that are yet to be patched.
- A zero-day attack is when someone uses a zero-day exploit to damage or steal data from a system that has a vulnerability.

Phishing is the attempt to gain access to internet accounts or steal personal information by sending false emails, messages, advertisements, or visiting websites that appear familiar to you. For instance, a phishing email may pose as your bank and ask for personal information related to your account.

II. METHODOLOGY

Pal and colleagues have proposed an improved genetic approach to intrusion detection. In order to set up an intrusion discovery framework, this research attempts to provide intrusion detection by modifying the evolutionary technique. They have implemented a trait subset decrease based on the acquisition of knowledge. So the complexity and preparation time were greatly reduced. Additionally, they added a soft computing method to the rule generation process, which increases its productivity compared to the hard computing method used in the current genetic process. The produced rule is more productive in identifying attacks. Using data collected from KDD Cup'99, this model was verified. The precise results clearly show the low false-positive rates and higher recognition rates. Yan has developed a novel approach to intrusion detection that relies on soft computing to lower the FNR (False Negative rate) that is often present in the interruption location system. This study proposes a keen interruption recognition model. The replica uses the genetic approach to improve a large portion of the neural structure in light of the global genetic computation

and nerve territory. The results of the tests demonstrated how well the interruption detection worked. A Classifier Fusion Based Anomaly Detection System in an ICS Environment has been proposed by Jan et al. Cyberattack detection has become an essential problem for highly sophisticated systems such as contemporary control systems. These frameworks are an essential component of the foundational data. In this sense, they might highlight their main role in modern culture. One of the most important tests for the cybersecurity network is the strong and convincing ICS cyber defense. Thus, one of the tasks that cybersecurity experts are asked to perform is interruption discovery. This essay examines the problem of classification. The suggested framework for identification relies on methods for guided anomaly discovery. They also enhanced the classifier's capacity for interruption recognition by utilizing its computations. To achieve the predetermined goal, the classifiers' combination is the best course of action. A two-step mixture method has been proposed by Li et al. in consideration of the k-NN process and binary classification. Stage 1 successfully distinguishes the correct kinds of network associations by using a single accumulation unit and a few binary classifiers.

Following step 1, relationships with undetermined levels are forwarded to step 2, where the k-NN algorithm determines their degrees. Step 2 produced a useful addition to Stage 1 and was dependent on the outcomes of Phase 1. On the NSL-KDD dataset, the suggested method achieves strong results by combining the two levels. A clustering strategy for IDS using Mini Batch K-means combined with Principal Component Analysis (PCA) has been proposed by Peng et al. Initially, a pre-processing technique was implemented to digitize the threads; subsequently, the dataset underwent uni-formization to improve bunching capacity. Additionally, the PCA method has been used to advance the productivity of clustering by reducing the organized dataset planning measurement.

Afterwards, information clustering was done using the Mini Batch K-means technique. In light of the Back Propagation Neural Network and the Learning Algorithm, Chiba et al. have suggested the perfect method for creating an effective anomaly detection system (NIDS). Their work includes the age of all possible combinations of the most important estimations of the parameters that go into creating such a classifier or that affect how well it performs in peculiarity identification, such as information standardization and highlight determination. In addition, they created multiple IDSs for those mixtures. Adaboost and artificial bee colony (ABC) computations were used in Mazini et al.'s suggested intrusion detection strategy with the aim of achieving a high recognition speed and a low false-positive speed. AdaBoost has been used to evaluate the arrangement of the features, and ABC has made use of the selected features. Wang and colleagues have presented a convincing intrusion detection framework in view of a support vector machine with enhanced features. The key addition made was the actualization of the logarithm marginal density proportions change to form the first attribute and obtain new, finer details about class changes that can greatly improve the identification ability.

For efficient system interruption recognition, Farrukh et al. have presented a novel two-phase deep learning model based on a stacked auto-encoder and a softmax classifier. In a different study, Rupam et al. presented an attack identification system driven by a plant-motivated reaction model. The experimental findings also demonstrate that the model is capable of differentiating and initiating a computerized response when needed. In a similar vein, Peng et al. suggested a cooperative improvement technique to simplify the DBN system architecture. They initially organize an optimization of a particle swarm considering the flexible learning and weight problem. Second, they increase the particle swarm optimization (PSO) to find the underlying enhancement solution by employing the fish swarm behaviors of clusters, scrounging, and various techniques.

Popoola et al. showed that federated learning-based DNN beat the traditional DNN model in terms of attack detection accuracy, low communication overhead, and data privacy. They also offered zero-day botnet attack detection for IoT edge devices. Fan et al. suggested IoT Defender, an IDS for 5G IoT based on transfer learning. IoT Defender used federated learning to aggregate data and transfer learning to create individualized attack detection models while maintaining privacy. For IoT networks based on GRUs, Monthukuri et al. proposed federated learning-based anomaly detection. By mixing the predictions from various GRU model layers with an ensemble of random forest models, they were able to increase the classification accuracy and show that their approach to attack detection was superior than centralized machine learning.

MV-FLID, an ensemble multi-view federated learning technique for IoT intrusion detection, was proposed by Attota et al. For the three different views of network traffic—uniflow, bi-flow, and packet—MV-FLID learns three different ANN models. To increase the precision of attack detection, the predictions made by these models are aggregated using random forests.

The Facebook dataset is utilized by authors Deylami et al. to showcase their findings regarding the efficacy of several classifiers in detecting criminal activity. AdaBoost SVM, a potent tool for tackling imbalanced classification issues, is the methodology employed in this study. This method's benefit is its ease of handling imbalanced categorization issues. To generalize the results, this approach's limitation is that it must be used on a variety of datasets.

The application of a Riemannian geometrical structure SVM for cyberattack classification is presented by Singh et al. The authors discovered that this approach worked well for categorizing cyberattacks. This method has the benefit of having a high degree of accuracy in identifying both DOS and regular attacks. Future study must address this approach's weakness, which is that it hasn't been fully integrated for identifying all sorts of cyberattacks yet.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

3rd-International Conference on Muti-Disciplinary Application & Research Technologies (ICMART-2024)

Geetanjali Institute of Technical Studies

Vol. 11, Special Issue 2, May 2024

The authors, Veena et al., have made contributions to the realm of cybercrime by identifying cybercrime information through the use of an approach known as "Cybercriminal SVM." Results using this strategy were said to be highly accurate. The authors did concede, though, that there is still opportunity for development in terms of performance enhancement and time complexity reduction. By creating an approach known as "Enhanced Multiclass Support Vector Machine" (EMSVM) to choose the most useful parameters while creating an SVM model, the authors Mohammad et al. have made a contribution. When this procedure was compared against state-of-the-art approaches, the findings were positive. The EMSVM approach, according to the authors, does not perform well with features that are highly correlated.

Pandey and associates. It seeks to give a summary of various strategies and emphasize how successful they are in locating and stopping cybercrime. The study examines and evaluates the body of research on machine learning methods for cybercrime detection as well as existing literature. It talks about the advantages and disadvantages of the techniques and puts them into categories including supervised learning, unsupervised learning, and hybrid approaches. It is a survey paper; it doesn't undertake actual experiments or suggest new methods. Rather, it offers a synopsis and evaluation of current methodologies. The particular setting and type of cybercrime may affect the efficacy of a certain approach.

Ali and colleagues (2021) tackle the issue of identifying and averting cybercrimes within social media platforms. Its main goal is to find hostile activity and suspicious activity in social network data in order to improve security and shield people from online fraud. The authors suggest a hybrid strategy that blends machine learning with graph-based analysis methods. To spot patterns and anticipate cybercrimes in social networks, they make use of machine learning classifiers, graph analysis algorithms, and social network data. There can be issues with the suggested method's scalability and capacity to manage massive volumes of social network data.

Furthermore, the quality and accessibility of social network data available for analysis may have an impact on the approach's efficacy.

Kumar et al. (2020): the study focuses on employing machine learning approaches to detect cyberattacks. It seeks to improve cybersecurity defenses by creating a useful method for recognizing and categorizing different kinds of cyberattacks. In order to identify and categorize cyberattacks, the authors suggest a novel method that incorporates several machine learning methods, including support vector machines and random forests. Machine learning models are trained, features are selected, and features are extracted using this method. Depending on the availability of labeled training data for various cyberattack types, the approach's efficacy may vary. Depending on the particulars of the attacks and the caliber of the features utilized for classification, the machine learning models' performance may differ.

Sharma et al.'s (2019) goal is to improve machine learning approaches for cybercrime detection and prevention. The primary objective is to enhance the precision and efficacy of cybercrime detection systems in order to efficiently detect and avert cyberattacks. The authors suggest a method for detecting cybercrime that makes use of machine learning algorithms like support vector machines and knearest neighbors. From network traffic data, they extract pertinent information and use machine learning models for anomaly detection and categorization. Managing vast amounts of network traffic data and preserving real-time detection skills may provide difficulties for the method. The quality and representativeness of the collected features may have an impact on how well the machine learning models perform.

Abdulraheem et al. (2022) attempted to identify phishing emails by selecting attributes using Principal Component Analysis (PCA), conducting a search using Ranker Search, and utilizing three algorithms machine learning: Multilayer Perceptron, Decision Tree (J48, C4.5), and Logistic Model Tree. The Logistic Model Tree approach yielded the maximum precision of 96.9245%. However, the computational complexity and time needed to implement the Logistic Model Tree rise as data dimensionality increases. With a 99.5% accuracy rate, our suggested solution has the highest precision.

In Bagui et al. (2019), the Word Embedding technique for phishing email detection was implemented with the greatest accuracy of 98.89% through the use of Deep Learning techniques in conjunction with Machine Learning algorithms. Even though the model's general accuracy has increased, this technique cannot comprehend words that the model has never encountered or are unknown to it. Since each email is unique, this results in an erroneous forecast of a new email.

For the purpose of identifying phishing emails, Ravi et al. (2018) employed deep neural networks in place of typical machine learning algorithms' attribute selection procedure, which presented difficulties. However, as data becomes more multidimensional, more processing power is needed to train and run the model.

In order to get the maximum accuracy of 92.78%, Nayak et al. (2021) utilized a hybrid bagging technique that combined the J48 Decision Tree algorithm with the Naive Bayes Multinomial classifier. The sole purpose of the model is to identify spam emails. That being said, our suggested method works for both spam and phishing email detection.

The research study by Sidhu and Bansal in 2021 used machine learning and deep learning approaches to detect spam emails. Through the use of several algorithms, this hybrid technique yields precision that ranges from 88% to 95%.

The technique presented in Rahman and Ullah (2020) combined bidirectional long short term memory with convolutional neural networks on two distinct datasets. In both datasets, the precision ranged from 86% to 98%. Natural language processing, or NLP, is an effective method for text analysis. It assigns a set of predefined tags or categories based on the text's content and can be applied to text categorization, sentiment analysis, subject recognition, and more.

Similar NLP-based techniques were employed by the authors of Egozi and Verma (2018) to effectively identify 80% of phishing emails and over 95% of ham emails.

Using email header-based features, the Relief Feature Selection technique was used by the authors of Kulkarni et al. (2020) to classify spam emails. The accuracy range that it produced was 91.06% to 94.78%.

Yahya et al. (2016) employed a back-propagation neural network (BPNN) in their investigation task to classify phishing emails according to the email body's properties. With an accuracy of 99.13%, BPNN outperformed other methods such as Naive Bayes, SVM, and Linear Discriminant techniques.

In Ruan and Tan (2009), attributes are taken from the email header as well as the text in order to classify the emails. The findings clarify the importance of using the characteristics from the email's header and content while training the model, as opposed to just using the features from one of them. This finding led to the research project's extraction of features from the email's content and header in order to train the classification model.

Samarthrao and Rohokale (2022) have presented a novel approach called G-SFO (Grey-Sail Fish Optimization) to maximize the accuracy and precision of the classification results. It draws inspiration from the algorithms of Sail Fish Optimization (SFO) and Grey Wolf Optimization (GWO). Four different datasets have been run through the G-SFO algorithm, and the highest precision of 98.86% has been achieved.

In Gangavarapu et al. (2020b), an effort was made to identify phishing and spam emails. An ideal feature subspace has been produced following the use of six techniques for feature extraction and selection. After applying and assessing eight machine learning algorithms using various evaluation measures, the Random Forest classifier performed best, with an overall accuracy of 98.4% on the ham and spam dataset and 99.4% on the ham and phishing dataset.

An approach to sample handling has been put forth in Li et al. (2022). Next, a neural network model called an LSTM (Long Short-Term Memory Network) is utilized to classify message bodies. Techniques like regularization and dropout have been applied to prevent sample data from being overfit. Adam is the optimizer that modifies the learning rate. With a maximum obtained precision of 0.96, the suggested approach outperformed conventional machine learning algorithms in terms of results.

REFERENCES

[1]. Dheeraj Pal, Amrita Parashar, Improved Genetic Algorithm for Intrusion Detection System, in: Sixth International Conference on Computational Intelligence and Communication Networks, IEEE Computer Society, 2014, pp. 835–839.
[2]. Chen Yan, Intelligent Intrusion Detection based on Soft Computing, in: Seventh International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), IEEE, 2015, pp. 577–580.
[3]. J. V´avra, H. Martin, Anomaly detection system based on classifier fusion in ics environment, in: 2017 International Conference on Soft Computing, Intelligent System and Information Technology (ICSIIT), IEEE, 2017, pp. 32–38.
[4]. Longjie Li, Yang Yu, Ying Hou ShenshenBai, Xiaoyun Chen, An Effective Two-Step Intrusion Detection Approach Based on Binary Classification and k - NN, IEEE Access 6 (2018) 12060–12073.
[5]. Peng, Kai, Victor CM Leung, and Qingjia Huang, "Clustering Approach Based on Mini Batch Kmeans for Intrusion Detection System over Big Data," IEEE Access, 2018.
[6]. Zouhair Chiba, Khalid Moussaid NoureddineAbghour, Amina El Omri, Mohamed Rida, A novel architecture combined with optimal parameters for backpropagation neural networks applied to anomaly network intrusion detection, Computers & Security 75 (2018) 36–58.
[7]. Mehrnaz Mazini, Shirazi Babak, Iraj Mahdavi, Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms, Journal of King Saud University-Computer and Information Sciences (2019).
[8]. Huiwen Wang, Gu Jie, Shanshan Wang, An effective intrusion detection framework based on SVM with feature augmentation, Knowl Based Syst 136 (2017) 130–139.
[9]. M. Krishnan, C. Chakraborty, S. Banerjee, C. Chakraborty, A.K. Ray, Statistical analysis of Mammographic Features and its Classification using Support Vector Machine, Expert Syst Appl 37 (2009) 470–478, https://doi.org/10.1016/j.eswa.2009.05.045. ISSN: 0957-4174.
[10]. Farrukh A Khan, Abdelouahid Abdu, Amir Hussain, A Novel Two-Stage Deep Learning Model for Efficient Network Intrusion Detection," in special section on artificial intelligence and cognitive computing for communication and network, IEEE Translations 7 (2019) 30373–30385.
[11]. S.I. Popoola, R. Ande, B. Adebisi, G. Gui, M. Hammoudeh, O. Jogunola, Federateddeep learning for zero-day botnet attack detection in IoT-edge devices, IEEE Internet Things J. 9 (5) (2021) 3930–3944.

[12]. Y. Fan, Y. Li, M. Zhan, H. Cui, Y. Zhang, Iotdefender: A federated transfer learning intrusion detection framework for 5g iot, in: 2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE), IEEE, 2020, pp. 88–95.

[13]. V. Mothukuri, P. Khare, R.M. Parizi, S. Pouriyeh, A. Dehghantanha, G. Srivastava, Federated-learning-based anomaly detection for iot security attacks, IEEE Internet Things J. 9 (4) (2021) 2545–2554.

[14]. D.C. Attota, V. Mothukuri, R.M. Parizi, S. Pouriyeh, An ensemble multiview federated learning intrusion detection for IoT, IEEE Access 9 (2021) 117734–117745.

[15]. Deylami, Hanif-Mohaddes, and Yashwant Prasad Singh. "Adaboost and SVM based cybercrime detection and prevention model." Artif. Intell. Res. 1.2 (2012): 117-130.

[16]. Singh, Shailendra, et al. "Improved Support Vector Machine for Cyber Attack Detection." Proceedings of the World Congress on Engineering and Computer Science. Vol. 1. 2011.

[17]. Veena, K., et al. "SVM Classification and KNN Techniques for Cyber Crime Detection." Wireless Communications and Mobile Computing 2022 (2022).

[18]. Mohammad, Rami Mustafa A. "An enhanced multiclass support vector machine model and its application to classifying file systems affected by a digital crime." Journal of King Saud University-Computer and Information Sciences (2019).

[19]. Eliyas, S., & Ranjana, P. (2023). Exploring the Critical Challenges and Potent Effects of E-Learning. International Journal of Intelligent Systems and Applications in Engineering, 11(3s), 189-193. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2560

[20]. Mohammad, Rami Mustafa A. "An enhanced multiclass support vector machine model and its application to classifying file systems affected by a digital crime." Journal of King Saud University-Computer and Information Sciences (2019).

[21]. Pandey, Shalini, and Sudhakar Pandey. "Machine Learning Techniques for Cybercrime Detection: A Survey." 2021. Available at: DOI: 10.1145/3453477.

[22]. Ali, Abeer, Jitender Kumar Chhabra, and Arun Solanki. "A Hybrid Approach for Cybercrime Detection and Prevention in Social Networks." 2021. Available at: DOI: 10.1007/s11227-021-04030-2.

[23]. Abdulraheem, R., Odeh, A., Al Fayoumi, M., Keshta, I., 2022. Efficient email phishing detection using machine learning. In: 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0354–0358. doi:10.1109/ CCWC54503.2022.9720818.

[24]. Bagui, S., Nandi, D., Bagui, S., White, R.J., 2019. Classifying phishing email using machine learning and deep learning. In: 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), pp. 1–2.doi:10.1109/CyberSecPODS.2019.8885143

[25]. Deepanti-phishnet: Applying deep neural networks for phishing email detection cen-aisecurity@ iwspa-2018PV Ravi, BG Hb, P Poornachandran, M Kumar, S Kp - Tempe AZ USA, March, 2018

[26]. Rahman, S.E., Ullah, S., 2020. Email spam detection using bidirectional long short term memory with convolutional neural network. In: 2020 IEEE Region 10 Symposium (TENSYMP), pp. 1307–1311. doi:10.1109/TENSYMP50017.2020.9230769.

[27]. Egozi, G., Verma, R., 2018. Phishing email detection using robust NLP techniques. In: 2018 IEEE International Conference on Data Mining Workshops (ICDMW), pp. 7–12. doi:10.1109/ICDMW.2018.00009.

[28]. Kulkarni, P., Saini, J.R., Acharya, H., 2020. Effect of header-based features on accuracy of classifiers for spam email classification. International Journal of Advanced Computer Science and Applications 11 (3). doi:10.14569/IJACSA.2020.0110350.

[29]. MULTI STAGE PHISHING EMAIL CLASSIFICATION. AY Daeef, RB Ahmad, Y Yacob, N Yaakob, KNFK Azir - Journal of Theoretical & …, 2016

[30]. Ruan, G., Tan, Y., 2009. A three-layer back-propagation neural network for spam detection using artificial immune concentration. Soft comput 14 (2), 139–150. doi:10.1007/s00500-009-0440-2.

[31]. Samarthrao, K.V., Rohokale, V.M., 2022. A hybrid meta-heuristic-based multiobjective feature selection with adaptive capsule network for automated email spam detection. International Journal of Intelligent Robotics and Applications 6 (3), 497–521. doi:10.1007/s41315-021-00217-9.

[32]. Gangavarapu, T., Jaidhar, C.D., Chanduka, B., 2020. Applicability of machine learning in spam and phishing email filtering: review and approaches. Artif Intell Rev 53 (7), 50195081. doi:10.1007/s10462-020-09814-9.

[33]. Li, Q., Cheng, M., Wang, J., Sun, B., 2022. Lstm based phishing detection for big email data. IEEE Trans. Big Data 8 (1), 278–288. doi:10.1109/TBDATA.2020.2978915.

