JOURNAL OF BASIC SCIENCE AND ENGINEERING

ANALYZE AND PREDICT OF HUMAN CYBER ATTACKERS USING ARTIFICIAL NEURAL NETWORK

[1]Mahesh Kedari [2]Dr. P Harini [3]N Lakshmi Narayana
[1]M. Tech Scholar, Dept. of CSE, St. Ann's College of Engineering & Technology, Chirala.
[2]Professor & HOD, Dept. of CSE, St. Ann's College of Engineering & Technology, Chirala.
[3]Assistant Professor, Dept. of CSE, St. Ann's College of Engineering & Technology, Chirala.

ABSTRACT: One of the world's biggest issues nowadays is cyber-attacks. Every day, they wreak serious economic harm to both persons and nations. . It constitutes criminal activity and when conducted on a large scale, it has the ability to undermine entire national economies. This paper reviews the various machine learning algorithms that have been developed for cyber security, including Artificial Neural Networks (ANNs), Support Vector Machines (SVMs), Random Forests, and Deep Learning. One technique to this problem is to apply actual statistics to determine the final results of the assault and discover the position of the party. The pre-processed image is passed through the Convolution, RELU and Pooling layer for feature extraction. A fully connected layer and a classifier is applied in the classification part of the image. This study uses ML methods to analyse cyber-crime consuming two patterns and to forecast how the specified characteristics will furnish to the detection of the cyber-attack methodology and perpetrator. Based on the comparison of eight distinct machine-learning methods, one can say that their accuracy was quite comparable. The Support Vector Machine (SVM) Linear outperformed all other cyber attack tactics in terms of accuracy. With a high degree of accuracy, the first model allowed us to forecast the types of attacks that the victims were most likely to experience. Future research directions include developing more robust machine learning algorithms, improving feature selection methods, developing more sophisticated deep learning models, and integrating human expertise with machine learning algorithms to improve their overall effectiveness.

Index Terms: Machine Learning, Cyber Security, Artificial Neural Networks, Support Vector Machines, Random Forests, Deep Learning, Intrusion Detection, Malware Classification, Phishing Detection, Limitations.

1. INTRODUCTION

Machine learning is a branch of computer science and artificial intelligence (AI) that focuses on using data and algorithms to simulate human learning, gradually improving the model's accuracy [1]. Face recognition which is a combination of machine learning and the biometic techniques which holds the qualities of not only high precision but also the reliability [2]. Machine learning algorithms have emerged as a powerful tool for addressing this challenge, due to their ability to analyze large and complex datasets to identify patterns and anomalies that may be indicative of an attack [3]. The statistics on the schooling process are fed into an algorithm which utilizes this knowledge to predict regarding the fresh test records. Three types of classes, supervised, less supervised and more desired - could be used to categorize research [4]. In the geometric based feature extraction, only some fixed points of face image are used where in the appearance based feature extraction, information is extracted from the whole face image [5]. The training process of classifying gender includes several methods such as Support Vector Machine (SVM), Principal Component Analysis (PCA), and Neural Networks (NN) [6]. An algorithm is fed the training data and utilizes that information to make predictions about new test data. In a broad sense, there are three distinct types of machine learning [7]. Learning may be divided into three categories: supervised, unsupervised, and reinforced supervised learning requires data to be labeled by a human before it can be used by the program to learn [8]. Threats are only eliminated and analyzed after they have been identified, by which time the network has already been penetrated and valuable data stolen. Most firms use the same technologies and security measures for intrusion detection and prevention, such as firewalls and antivirus software, along with access controls like passwords [9].

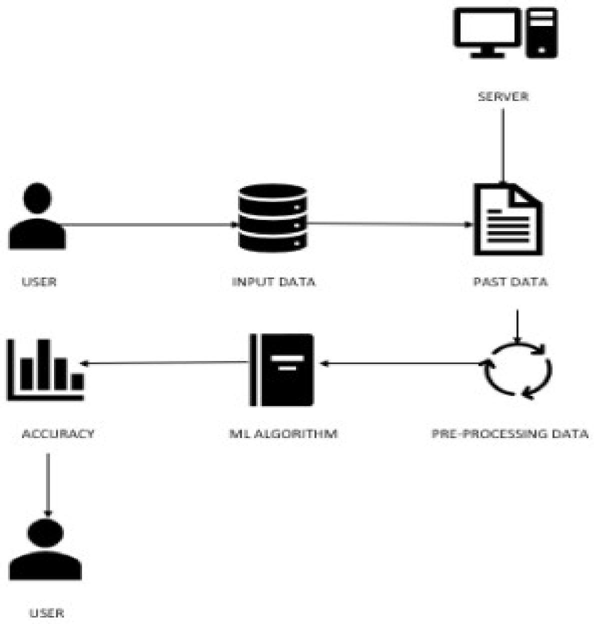

Figure 1. Management AI and Evolution of Technology

2. RELATED WORKS

The Cyber-Physical Systems (CPSs) constitute an emerging research field that has captured the interest of many scholars, according to the author of this paper [10]. It takes a lot of time to give the proper attention and it also has the chances of skipping criminals as they will be alerted by seeing cops easily gets escape from there. Since the MIS is in the process of taking more time and we will not properly focus on everyone [11]. This work proposes a depth camera-based robust facial expression recognition (FER) system that can be adopted for better human machine interaction. Despite the advantages of machine learning in cyber security, there are also challenges associated with using these techniques. One of the major challenges is the interpretability of machine learning algorithms [12]. They can cause significant financial losses to both individuals and nations daily. In addition, the increase in cyber attacks creates cybercrime. In the field of image processing and machine learning, a lot of research work has been done on human gender estimation. In this section, a brief overview of previous work on human gender estimation has been presented [13]. Selecting relevant and interconnected characteristics from a dataset is known as feature selection. When training information for machine learning, it helps save time and space. Training times may lengthen if the characteristics are chosen incorrectly, raising the model's error rate and complicating its interpretation [14].

3. SYSTEM MODELS

Cyber-physical systems (CPSs) are intricate systems that incorporate control, communication, and computing technology. CPSs are used widely today in smart grids, smart manufacturing, smart cities, and intelligent transportation [15]. We have to implement the deep and machine learning algorithm such as Convolutional Neural Network (CNN) and random forest. The experimental results shows that the accuracy. Support Vector Machines (SVMs) are a type of machine learning algorithm that can be used in detecting and preventing cyber-attacks. SVMs are designed to separate data into two classes by finding an optimal boundary known as a hyper plane that maximizes the margin between the two classes. SVMs are capable of learning from large datasets and can be used to classify data, identify patterns, and make predictions [16]. The detection systems that are primarily system-based systems employ regarded styles as well as the signatures of attacks to recognize their targets [17].

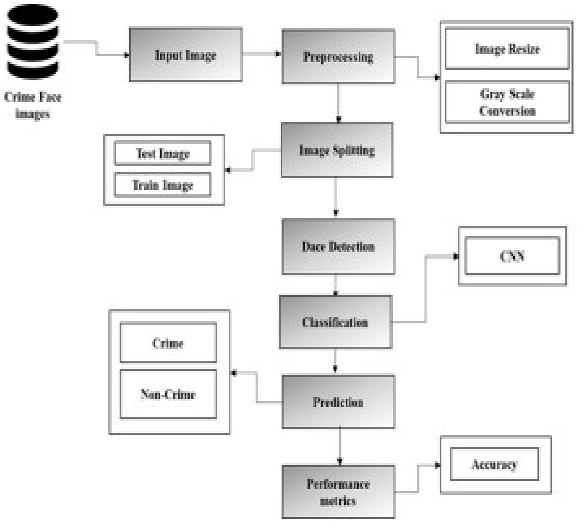

Figure 2. Flowchart of proposed ML used in the safety process.

4. PROPOSED SYSTEM

Hybrid strategies: combining techniques based on signatures, anomaly-based and rules-based systems and machine learning algorithms that can draw on the advantages of each and improve the accuracy of normal detection [18]. Federated learning organizations from multiple institutions to teach students using their gadgets on their private record sand not share confidential information [19]. In our proposed system we have utilized a CNN architecture. CNN which is a deep learning algorithm is capable of distinguishing images from their characteristics. CNN is generally used for image analysis, image segmentation, image classification, medical image analysis, image and video recognition [20]. Cyberspace present condition portends uncertainty for the future of the Internet and its expanding user base.

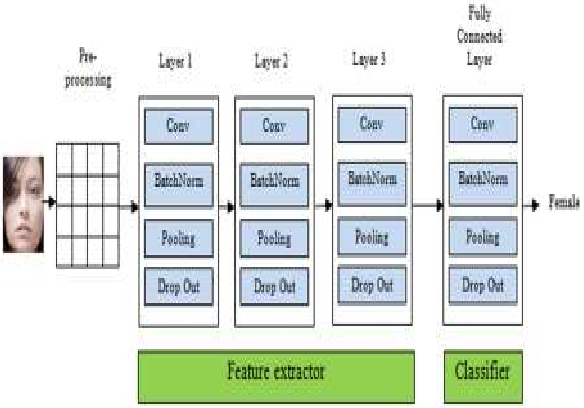

Figure 3. Network Architecture

5. METHODOLOGY

Officers who focus on the specific kind of crime that a person has suffered are sought after by the public. The unit's database takes a comprehensive record of these statistics. These crimes are documented by the police in detail, including the nature, manner, year, etc. They collect data, sort it into categories **[21].** Hybrid configuration to suit traffic management rules the output of invalid plans for recovering from timetable disruptions has the potential not just to prevent recovery from the delay but even to bring train services to a complete halt [22]. To resolve this problem Hitachi provides a visualization of the timetable changes calculated by machine learning that translates them into the same form used to present changes produced by conventional traffic c management systems [23].

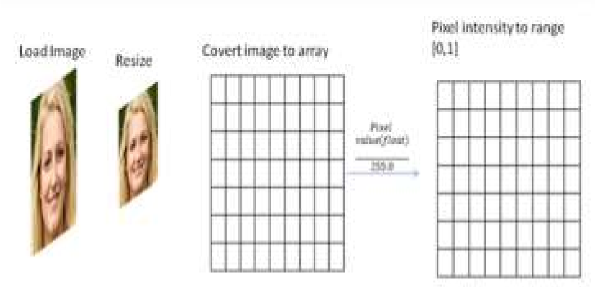

Figure 4. Modes of AI with Hybrid Configuration Techniques

Areas for Future Research in Machine Learning for Cyber Security

While Machine Learning algorithms have shown great potential in detecting and preventing cyber attacks, there is still room for future research to further improve their effectiveness in cyber security. We will discuss some of the areas for future research in Machine Learning for cyber security [24]. The use of hardware accelerators, such as graphical processing units (GPUs) and field-programmable gate arrays (FPGAs), can also help to improve the efficiency of Machine Learning algorithms.

CLASSIFICATION

In our process, we have to implement the deep and machine learning algorithm such as Convolutional Neural Network (CNN) and RF. CNNs are regularized versions of multilayer perceptron"s. Multilayer perceptron usually mean fully connected networks, that is, each neuron in one layer is connected to all neurons in the next layer. As per the cut up criteria, the clean data are cut into the eighty% education and 20 percent test after which the data is tested on one machine to gain understanding of the classifier along with Natural language Process (NLP).

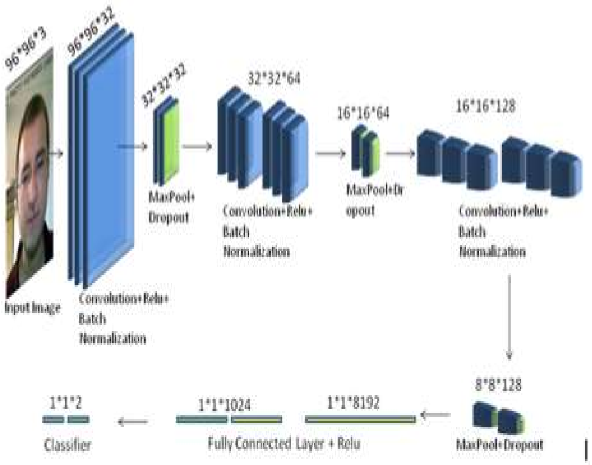

Figure. 5. A full schematic diagram of network architecture

6. RESULT AND DISCUSSION

The study's objectives include accurate incident data analysis, crime prevention, and the capture of offenders. This paper's main focus is on using data analysis to draw conclusions about crime prevention. Accuracy of classifier refers to the ability of classifier. It predicts the class label correctly and the accuracy of the predictor refers to how well a given predictor can guess the value of predicted attribute for a new data. Researchers generally evaluate the overall performance and also the efficiency of machine learning algorithms using these factors [26]. In our model we have evaluated performance metrics to understand how well our model is performing on given dataset

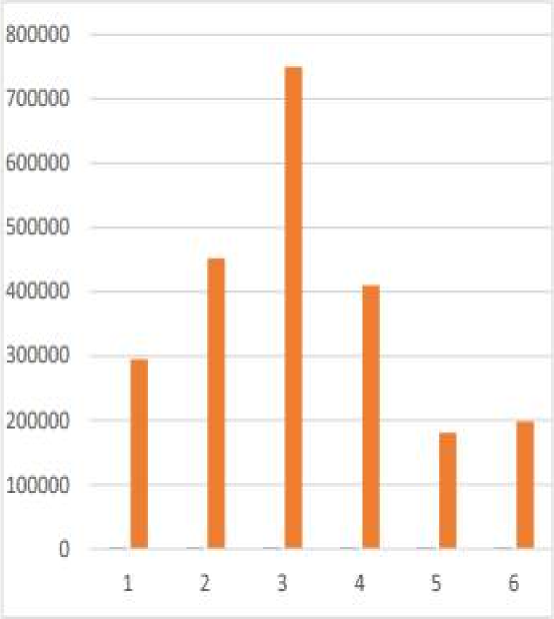

Figure. 6. The Accuracy vs Epoch curv

7. CONCLUSIONS AND FUTURE OPPORTUNITIES

We have used both image processing technique and machine learning algorithm for implementation and achieved a promising result for both Kaggle dataset and Nottingham Scan Database. The system predicts the demographics of potential victims and the kind of attacks they may face. Machine learning strategies are sufficiently compelling. The linear SVM approach is the most effective. The methods of machine learning have enough convincing proof. A good approach is to utilize SVMs that are linear. Machine learning algorithms can improve cyber security by detecting new and unknown threats, reducing false positives, and providing fast and accurate responses to threats. Cybercrime data from other provinces may also be obtained based on discussions with other authorized entities with crime databases to be used for comparison with this study. In future work, we will hybrid the transfer learning or combine the two different machine learning algorithms or combine the two different deep learning algorithms for better performance or efficiency.

8. REFERENCES

[1]N. I. of Standard Technology. Cyber-physical systems

[2] S. Walker-Roberts, M. Hammoudeh, O. Aldabbas, M. Aydin, and A. Dehghantanha, "Threats on the horizon: Understanding security threats in the era of cyber-physical systems," The Journal of Supercomputing, vol. 76, no. 4, pp. 2643–2664, 2020.

[3] M. N. Al-Mhiqani, R. Ahmad, W. Yassin, A. Hassan, Z. Z. Abidin, N. S. Ali, and K. H. Abdulkareem, "Cyber-security incidents: A review cases in cyber-physical systems," International Journal of Advanced Computer Science and Applications, vol. 9, 2018.

[4] Dr. Ratna Raju Mukiri, Dr. Prasuna Grandhi, Dr. Hari Kishan Chapala, "NEW SECURITY MODELS IN CLOUD IOT SYSTEM USING HASH MACHINE LEARNING," Industrial Engineering Journal ISSN: 0970-2555 Volume : 52, Issue 8, August : 2023.

[5]J.-P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends

[6]M. R. Endsley, "Design and evaluation for situation awareness enhancement," Proceedings of the Human Factors Society Annual Meeting, vol. 32, no. 2, pp. 97–101, 1988.

[7]R. S. Gutzwiller, S. M. Hunt, and D. S. Lange, "A task analysis toward characterizing cyber-cognitive situation awareness (ccsa) in cyber defense analysts," in 2016 IEEE International Multi-Disciplinary

[8] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "ArcFace: Additive angular margin loss for deep face recognition," in Proc. CVPR, 2019, pp. 4690–4699.

[9] D. P. Kingma and M. Welling, "Autoencoding variational bayes," in Proc. ICLR, 2014.

[10] I. Goodfellow et al., "Generative adversarial nets," in Proc. NIPS, 2014, pp. 2672–2680.

[11] M. Arjovsky, S. Chintala, and L. Bottou, "Wasserstein generative adversarial networks," in Proc. ICML, 2017, pp. 214– 223.

[12] I. Gulrajani, F. Ahmed, M. Arjovsky, V. Dumoulin, and A. C. Courville, "Improved training of Wasserstein GANs," in Proc. NIPS, 2017, pp. 5769–5779.

[13] H. Huang, Z. Li, R. He, Z. Sun, and T. Tan, "IntroVAE: Introspective variational autoencoders for photographic image synthesis," in Proc. NIPS, 2018, pp. 52–63.

[14] A. Razavi, A. van den Oord, and O. Vinyals, "Generating diverse highfidelity images with VQ-VAE-2," in Advances in Neural Information Processing Systems, 2019, pp. 14866–14876.

[15] A. Brock, J. Donahue, and K. Simonyan, "Large scale GAN training for high fidelity natural image synthesis," in Proc. ICLR, 2018.

[16]. Jamil, M.N., Hossain, M.S., ul Islam, R., Andersson, K.: A belief rule based expert system for evaluating technological innovation capability of high-tech firms under uncertainty. In: 2019 Joint 8th International Conference on Informatics, Electronics & Vision (ICIEV) and 2019 3rd International Conference on Imaging, Vision & Pattern Recognition (icIVPR), pp. 330–335. IEEE (2019)

[17]. Kabir, S., Islam, R.U., Hossain, M.S., Andersson, K.: An integrated approach of belief rule base and deep learning to predict air pollution. Sensors 20(7), 1956 (2020)

[18]. Karim, R., Andersson, K., Hossain, M.S., Uddin, M.J., Meah, M.P.: A belief rule based expert system to assess clinical bronchopneumonia suspicion. In: 2016 Future Technologies Conference (FTC), pp. 655–660. IEEE (2016)
[19]. Li, B., Lian, X.C., Lu, B.L.: Gender classification by combining clothing, hair and facial component classifiers. Neurocomputing 76(1), 18–27 (2012)
[20]. Lian, H.-C., Lu, B.-L.: Multi-view gender classification using local binary patterns and support vector machines. In: Wang, J., Yi, Z., Zurada, J.M., Lu, B.-L., Yin, H. (eds.) ISNN 2006. LNCS, vol. 3972, pp. 202–209. Springer, Heidelberg (2006). https://doi.org/10.1007/11760023 30
[21]. Mahmud, M., Kaiser, M.S., McGinnity, T.M., Hussain, A.: Deep learning in mining biological data. Cogn. Comput. 13(1), 1–33 (2021). https://doi.org/10.1007/ s12559-020-09773-x
[22]. Mahmud, M., Kaiser, M.S., Hussain, A., Vassanelli, S.: Applications of deep learning and reinforcement learning to biological data. IEEE Trans. Neural Netw. Learn. Syst. 29(6), 2063–2079 (2018). https://doi.org/10.1109/TNNLS.2018.2790388
[23]. Mozaffari, S., Behravan, H., Akbari, R.: Gender classification using single frontal image per person: combination of appearance and geometric based features. In: 2010 20th International Conference on Pattern Recognition, pp. 1192–1195. IEEE (2010)
[24]. Nazir, M., Ishtiaq, M., Batool, A., Jaffar, M.A., Mirza, A.M.: Feature selection for efficient gender classification. In: Proceedings of the 11th WSEAS International Conference, pp. 70–75 (2010) [25]. Rahaman, S., Hossain, M.S.: A belief rule based clinical decision support system to assess suspicion of heart failure from signs, symptoms and risk factors. In: 2013 International Conference on Informatics, Electronics and Vision (ICIEV), pp. 1–6. IEEE (2013)