International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 12, Issue 01, January 2023)

Intrusion Detection Model for Detecting Innovative Cyber Attacks using Deep Learning

Sandeep Bharti[1], Parbhat Gupta[2]

[1]*Assistant Professor, Department of BCA,* [2]*Assistant Professor, Department of Computer Science and Engineering, Vidya Institute of Creative Teaching Meerut, UP, India*

***Abstract*— In recent years, due to the increased frequency of cyber-attacks, the negative impacts of cyber-attacks on society have increased. Therefore, the research on cyber-security and prevention of cyber-attacks, including intrusion detection as an effective means of defense against cyber-attacks, is warranted. Many of the users are using the internet services. The cyber world includes the information technology, computer etc based services. Many of the protocols, technology make improvement in the cyber world. The security is important concern in the cyber based services. The Network Intrusion Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS) is primary system to detect and prevent cyber security. Both in the research and in the development of the systems for intrusion detection, the machine learning and deep learning methods are widely utilized, and the NSL-KDD dataset is frequently used in algorithm research and verification.**

***Keywords*— IOT, Cyber, NIDS, HIDS, Security.**

I. INTRODUCTION

There has been significant research in incorporating both blockchain and intrusion detection to improve data privacy and detect existing and emerging cyberattacks, respectively. In these approaches, learning-based ensemble models can facilitate the identification of complex malicious events and concurrently ensure data privacy. Such models can also be used to provide additional security and privacy assurances during the live migration of virtual machines (VMs) in the cloud and to protect Internet-of-Things (IoT) networks. This would allow the secure transfer of VMs between data centers or cloud providers in real time.

This article proposes a deep blockchain framework (DBF) designed to offer security-based distributed intrusion detection and privacy-based blockchain with smart contracts in IoT networks. The intrusion detection method is employed by a bidirectional long short-term memory (BiLSTM) deep learning algorithm to deal with sequential network data and is assessed using the data sets of UNSW-NB15 and BoT-IoT. The article presents review of Information and communication technology (ICT) progressions have adjusted the whole processing worldview.

Because of these enhancements, various new channels of correspondence are being made, one of which is the Web of Things (IoT). The IoT has as of late arisen as state of the art innovation for establishing shrewd conditions. The Web of Clinical Things (IoMT) is a subset of the IoT, where clinical hardware trade data with one another to trade touchy data. These advancements empower the medical services business to keep a more significant level of touch and care for its patients. Security is viewed as a critical test in at all innovation's dependence in light of the IoT. Security hardships happen attributable to the different potential assaults presented by assailants. There are various security concerns, for example, remote seizing, and pantomime, refusal of administration assaults, secret key speculating, and man-in-the-center. In case of such assaults, basic information related with IoT network might be uncovered, changed, or even delivered difficult to reach to approve clients. Accordingly, it ends up being basic to defend the IoT/IoMT environment against malware attacks [1][2].

An exhaustive report with a test examination of united profound learning approaches for network safety in the Web of Things (IoT) applications. In particular, we initially give an audit of the unified learning-based security and protection frameworks for a long time of IoT applications, including, Modern IoT, Edge Registering, Web of Robots, Web of Medical services Things, Web of Vehicles, and so on Second, the utilization of unified learning with blockchain and malware/interruption recognition frameworks for IoT applications is examined. Then, at that point, we audit the weaknesses in united learning-based security and protection frameworks [3].

Independent control frameworks are progressively utilizing AI advancements to deal with sensor information, settling on convenient and informed choices about performing control capacities in view of the information handling results. Among such AI advances, support learning (RL) with profound brain networks has been as of late perceived as one of the attainable arrangements, since it empowers learning by communication with conditions of control frameworks.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 12, Issue 01, January 2023)

In this work, we consider RL-based control models and address the issue of transiently obsolete perceptions frequently caused in powerful digital actual conditions. The issue can frustrate expansive receptions of RL techniques for independent control frameworks. In particular, we present a RL-based strong control model, to be specific protocol, that takes advantage of a progressive learning structure in which a bunch of low-level strategy variations are prepared for old perceptions and afterward their learned information can be moved to an objective climate restricted in ideal information refreshes [4].

Figure 1: Cyber security

AI calculations are viable in a few applications; however they are not as much fruitful when applied to interruption identification in digital protection. Because of the great aversion to their preparation information, digital locators in view of AI are helpless against designated antagonistic assaults that include the bother of starting examples. Existing safeguards accept unreasonable situations; their outcomes are disappointing in non-antagonistic settings; or they can be applied distinctly to AI calculations that perform inadequately for digital protection [5]. Web of-Things (IoT) gadgets and frameworks will be progressively designated by cybercriminals (counting country state-supported or associated danger entertainers) as they become an indispensable piece of our associated society and environment. Notwithstanding, the difficulties in getting these gadgets and frameworks are compounded by the scale and variety of organization, the speedy digital danger scene, and numerous different elements [6]. The conventional validation frameworks are defenseless against the dangers of absent mindedness, misfortune, and burglary.

Biometric verification is has been improved and turned into the piece of day to day existence. The Electrocardiogram (ECG) based verification strategy has been presented as a biometric security framework appropriate to check the distinguishing proof for entering a structure and this examination accommodates concentrating on ECG-based biometric validation methods to reshape input information by cutting in light of the RR-stretch [7].

II. Literature Survey

S. Ho et al.,[1] proposed IDS model is aimed at detecting network intrusions by classifying all the packet traffic in the network as benign or malicious classes. The Canadian Institute for Cybersecurity Intrusion Detection System (CICIDS2017) dataset has been used to train and validate the proposed model. The model has been evaluated in terms of the overall accuracy, attack detection rate, false alarm rate, and training overhead. A comparative study of the proposed model's performance against nine other well-known classifiers has been presented.

V. K. Navya et al.,[2] the help of datasets and with constant updating, one can detect such intrusions. The one algorithm that stands out is the DNN (Deep Neural Network), which is a type of deep learning model, which helps to develop a flexible and effective Intrusion Detection System (IDS) to detect and classify unforeseen and unpredictable cyberattacks.

Y. A. Farrukh et al.,[3] propose a two-layer hierarchical machine learning model having an accuracy of 95.44 % to improve the detection of cyberattacks. The first layer of the model is used to distinguish between the two modes of operation - normal state or cyberattack. The second layer is used to classify the state into different types of cyberattacks. The layered approach provides an opportunity for the model to focus its training on the targeted task of the layer, resulting in improvement in model accuracy. To validate the effectiveness of the proposed model, we compared its performance against other recent cyber attack detection models proposed in the literature.

S. Thirimanne et al.,[4] prime objective of this research is to discover the best machine learning algorithm for intrusion detection trained using the NSL-KDD and the UNSW-NB15 datasets and perform a comparative analysis between six machine learning algorithms classified as supervised, semi-supervised, and unsupervised learning.

This study revealed that the performance of supervised and semi-supervised machine learning algorithms outperformed unsupervised machine learning algorithms for both datasets and concluded that Support Vector Machines (SVM) and Deep Neural Network (DNN) perform better for NSL-KDD and UNSW-NB15, respectively.

T. T. Nguyen et al.,[5] presents a survey of DRL approaches developed for cyber security. We touch on different vital aspects, including DRL-based security methods for cyber-physical systems, autonomous intrusion detection techniques, and multiagent DRL-based game theory simulations for defense strategies against cyberattacks. Extensive discussions and future research directions on DRL-based cyber security are also given. We expect that this comprehensive review provides the foundations for and facilitates future studies on exploring the potential of emerging DRL to cope with increasingly complex cyber security problems.

W. Xu et al.,[6] proposed model utilizes the most effective reconstruction error function which plays an essential role for the model to decide whether a network traffic sample is normal or anomalous. These sets of innovative approaches and the optimal model architecture allow our model to be better equipped for feature learning and dimension reduction thus producing better detection accuracy as well as f1-score. We evaluated our proposed model on the NSL-KDD dataset which outperformed other similar methods by achieving the highest accuracy and f1-score at 90.61% and 92.26% respectively in detection.

K. Cao et al.,[7] attention mechanism is utilized to capture key features which represent the structural characteristics of traffic data. Moreover, CuDNN-based long short-term memory network is used to learn time-related information of the traffic while accelerating the convergence of the model. Finally, global maxpooling is adopted to compress data and to improve the generalization capabilities of the proposed model. Experimental results on UNSW-NB15 dataset show that the binary classification accuracy of the proposed model is up to 92.65%. Further, it can also identify various attacks with the accuracy of 81.28%.

I. Ullah et al.,[8] a convolutional neural network model is used to create a multiclass classification model. The proposed model is then implemented using convolutional neural networks in 1D, 2D, and 3D. The proposed convolutional neural network model is validated using the BoT-IoT, IoT Network Intrusion, MQTT-IoT-IDS2020, and IoT-23 intrusion detection datasets.

Transfer learning is used to implement binary and multiclass classification using a convolutional neural network multiclass pre-trained model. Our proposed binary and multiclass classification models have achieved high accuracy, precision, recall, and F1 score compared to existing deep learning implementations.

D. Park et al.,[9] a deep learning-based intrusion detection system model has emerged that analyzes intelligent attack patterns through data learning. However, deep learning models have the disadvantage of having to re-learn each time a new cyberattack method emerges. The time required to learn a large amount of data is not efficient. In this paper, an experiment was conducted using the Leipzig Intrusion Detection Data Set (LID-DS), which is a host-based intrusion detection data set released in 2018.

I. Siniosoglou et al.,[10] proposed IDS is validated in four real SG evaluation environments, namely (a) SG lab, (b) substation, (c) hydropower plant and (d) power plant, solving successfully an outlier detection (i.e., anomaly detection) problem as well as a challenging multiclass classification problem consisting of 14 classes (13 Modbus/TCP cyberattacks and normal instances). Furthermore, MENSA can discriminate five cyberattacks against DNP3.

O. Alkadi et al.,[11] privacy-based blockchain and smart contract methods are developed using the Ethereum library to provide privacy to the distributed intrusion detection engines. The DBF framework is compared with peer privacy-preserving intrusion detection techniques, and the experimental outcomes reveal that DBF outperforms the other competing models. The framework has the potential to be used as a decision support system that can assist users and cloud providers in securely migrating their data in a timely and reliable manner.

T. Yu et al.,[12] propose a new two-stage dimensionality reduction (TSDR) feature selection method and verified by NSL-KDD dataset. The method reduces the dimensionality of the dataset and significantly improves the calculation efficiency. The KNN algorithm is used to verify that the new feature selection method improves the calculation efficiency. The accuracy rate is only slightly reduced when compared to the full feature calculation.

III. IoT IDS Techniques

The IoT Interruption is characterized as an unapproved activity or movement that hurts the IoT biological system. For instance, an assault that will make the PC administrations inaccessible to its real clients is viewed as an interruption.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 12, Issue 01, January 2023)

An IDS is characterized as a product or equipment framework that keeps up with the security of the framework by recognizing vindictive exercises on the PC frameworks. The primary point of IDS is to distinguish unapproved PC utilization and vindictive organization traffic which is preposterous while utilizing a customary firewall. This outcomes in making the PC frameworks exceptionally defensive against the noxious activities that compromise the accessibility, respectability, or secrecy of PC frameworks.

A. Signature-based intrusion detection systems (SIDS)

Signature interruption location frameworks (SIDS) use design matching procedures to track down a referred to assault; these are otherwise called Information based Recognition. In SIDS, matching techniques are utilized to track down a past interruption. As such, when an interruption signature matches the mark of a past interruption that as of now exists in the mark data set, an alert sign is set off. For SIDS, the host's logs are reviewed to observe arrangements of orders or activities which have recently been distinguished as malware. SIDS has likewise been named in the writing as Information Based Discovery or Abuse Recognition. Customary strategies for SIDS experience issues in distinguishing assaults that length different parcels as they inspect network bundles and perform matching against an information base of marks. With the expanded refinement of current malware, separating mark data from different bundles might be required. With this, IDS needs to bring the substance of prior parcels also. For making a mark for SIDS, by and large, there have been a few strategies where marks are made as state machines, formal language string designs or semantic circumstances.

B. Anomaly-based intrusion detection system (AIDS)

Helps has drawn in a great deal of researchers due to its element to beat the constraint of SIDS. In Helps, a typical model of the conduct of a PC framework is made utilizing AI, measurable based or information based techniques. Any huge deviation between the noticed conduct and the model is viewed as an irregularity, which can be deciphered as an interruption. This sort of strategy chips away at the way that pernicious conduct is not quite the same as commonplace client conduct. The conduct of unusual clients that separates from the standard conduct is characterized as an interruption. There are two stages in the advancement of Helps: the preparation stage and the testing stage. In the preparation stage, the typical traffic profile is utilized to gain proficiency with a model of ordinary conduct.

In the testing stage, another informational index is utilized to foster the framework's ability to sum up to beforehand inconspicuous interruptions. Helps can be sub-arranged in light of the strategy utilized for preparing, for example, factual based, information based and AI based.

The primary benefit of Helps is the capacity to distinguish zero-day assaults on the grounds that perceiving the strange client movement doesn't depend on a mark information base. Helps sets off a risk signal when the inspected conduct goes amiss from ordinary conduct. Moreover, Helps has various advantages. To begin with, they can find inside malignant exercises. Assuming an interloper begins making exchanges in a taken record that are unidentified in the average client movement, it makes a caution. Second, it is trying for a cybercriminal to perceive what a typical client conduct is without delivering a ready as the framework is developed from redid profiles.

C. Machine Learning based Technique

AI is the most common way of separating information from huge amounts of information. AI models include a bunch of rules, techniques, or complex "move works" that can be applied to observe intriguing information designs or to perceive or anticipate conduct. AI procedures have been applied broadly in the space of Helps. To extricate the information from interruption datasets, various calculations and strategies, for example, grouping, brain organizations, affiliation rules, choice trees, hereditary calculations, and closest neighbor techniques are used.

Some earlier examination has analyzed the utilization of various strategies to assemble AIDSs. Analyzed the presentation of two element determination calculations including Bayesian organizations (BN) and Characterization Relapse Trees (CRC) and consolidated these strategies for higher exactness.

Procedures of component determination utilizing a mix of element choice calculations like Data Gain (IG) and Connection Characteristic assessment. They tried the presentation of the chose highlights by applying different order calculations like C4.5, guileless Bayes, NB-Tree and Multi-facet Perceptron. A hereditary fluffy rule mining strategy has been utilized to assess the significance of IDS highlights. NIDS by utilizing the Arbitrary Tree model to further develop exactness and diminish the misleading problem rate.

Different AIDSs have been made in view of AI procedures as displayed in Fig. 4. The primary point of utilizing AI strategies is to make IDS that requires less human information and further develop exactness. The amount of Helps which utilizes AI procedures has been expanding over the most recent couple of years.

The fundamental target of IDS in light of AI research is to distinguish examples and fabricate an interruption discovery framework in view of the dataset. For the most part, there are two classes of AI strategies, regulated and unaided.

IV. Conclusion

An Intrusion Detection System (IDS) is a network security technology originally built for detecting vulnerability exploits against a target application or computer. The network intrusion system prevent the cyber world form the various attack. There are various techniques based on the artificial intelligence, machine learning and deep learning, which can able to handle the attack prediction. This paper present the review of the cyber security using machine and deep learning techniques. The simulation will be performed using the python spyder 3.7 software.

REFERENCES

[1] S. Ho, S. A. Jufout, K. Dajani and M. Mozumdar, "A Novel Intrusion Detection Model for Detecting Known and Innovative Cyberattacks Using Convolutional Neural Network," in IEEE Open Journal of the Computer Society, vol. 2, pp. 14-25, 2021, doi: 10.1109/OJCS.2021.3050917.

[2] V. K. Navya, J. Adithi, D. Rudrawal, H. Tailor and N. James, "Intrusion Detection System using Deep Neural Networks (DNN)," 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), 2021, pp. 1-6, doi: 10.1109/ICAECA52838.2021.9675513.

[3] Y. A. Farrukh, Z. Ahmad, I. Khan and R. M. Elavarasan, "A Sequential Supervised Machine Learning Approach for Cyber Attack Detection in a Smart Grid System," 2021 North American Power Symposium (NAPS), 2021, pp. 1-6, doi: 10.1109/NAPS52732.2021.9654767.

[4] S. Thirimanne, L. Jayawardana, P. Liyanaarachchi and L. Yasakethu, "Comparative Algorithm Analysis for Machine Learning Based Intrusion Detection System," 2021 10th International Conference on Information and Automation for Sustainability (ICIAfS), 2021, pp. 191-196, doi: 10.1109/ICIAfS52090.2021.9605814.

[5] T. T. Nguyen and V. J. Reddi, "Deep Reinforcement Learning for Cyber Security," in IEEE Transactions on Neural Networks and Learning Systems, doi: 10.1109/TNNLS.2021.3121870.

[6] W. Xu, J. Jang-Jaccard, A. Singh, Y. Wei and F. Sabrina, "Improving Performance of Autoencoder-Based Network Anomaly Detection on NSL-KDD Dataset," in IEEE Access, vol. 9, pp. 140136-140146, 2021, doi: 10.1109/ACCESS.2021.3116612.

[7] K. Cao, J. Zhu, W. Feng, C. Ma, M. Liu and T. Du, "Network Intrusion Detection based on Dense Dilated Convolutions and Attention Mechanism," 2021 International Wireless Communications and Mobile Computing (IWCMC), 2021, pp. 463-468, doi: 10.1109/IWCMC51323.2021.9498652.

[8] I. Ullah and Q. H. Mahmoud, "Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks," in IEEE Access, vol. 9, pp. 103906-103926, 2021, doi: 10.1109/ACCESS.2021.3094024.

[9] D. Park, S. Kim, H. Kwon, D. Shin and D. Shin, "Host-Based Intrusion Detection Model Using Siamese Network," in IEEE Access, vol. 9, pp. 76614-76623, 2021, doi: 10.1109/ACCESS.2021.3082160.

[10] I. Siniosoglou, P. Radoglou-Grammatikis, G. Efstathopoulos, P. Fouliras and P. Sarigiannidis, "A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1137-1151, June 2021, doi: 10.1109/TNSM.2021.3078381.

[11] O. Alkadi, N. Moustafa, B. Turnbull and K. -K. R. Choo, "A Deep Blockchain Framework-Enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks," in IEEE Internet of Things Journal, vol. 8, no. 12, pp. 9463-9472, 15 June15, 2021, doi: 10.1109/JIOT.2020.2996590.

[12] T. Yu, Z. Liu, Y. Liu, H. Wang and N. Adilov, "A New Feature Selection Method for Intrusion Detection System Dataset – TSDR method," 2020 16th International Conference on Computational Intelligence and Security (CIS), 2020, pp. 362-365, doi: 10.1109/CIS52066.2020.00083.