JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Machine Learning based Network Intrusion Detection for IoT Security Application: A Review

[1]Bijendra Singh Thakur, [2]Nidhi Sindhu
[1]Research Scholar, [2]Assistant Professor
Department of Computer Science and Applications
Chhatrapati Shivaji Institute of Technology, Durg, India

Abstract : The Internet of Things (IoT) has seen fast development in the direction of having a bigger influence on both day-to-day living and large-scale industrial systems. Unfortunately, this has drawn the attention of cybercriminals, who have made the Internet of Things a target of nefarious operations, so opening the door to the possibility of an assault on the end nodes. To this purpose, several IoT intrusion detection Systems (IDS) have been presented in the published research to combat assaults on the IoT ecosystem. These IoT intrusion detection systems (IDS) may be generally categorized according to the detection approach, validation strategy, and deployment strategy that they use. This survey study includes a complete evaluation of modern IoT intrusion detection systems (IDS), as well as an overview of approaches, deployment strategies, validation strategies, and datasets that are often used for the construction of IDS.

Index Terms **– IoT, IDS, Cyber, Attack, Security, Internet.**

I. INTRODUCTION

The Internet of Things (IoT) refers to the linked network of systems and devices that make it possible for information to be transferred between physical items in a seamless manner. These gadgets may be remotely monitored and governed; some examples include medical and healthcare equipment, autonomous cars, industrial robots, smart TVs, wearables, and smart city infrastructures. It is anticipated that Internet of Things devices will become more widespread than mobile smartphones. These devices will have access to the most sensitive information, including personal information. This will result in an increase in the attack surface area, which will in turn result in an increased probability of assaults. IoT intrusion detection systems will need to be created in order to secure communications made possible by technologies that are part of the Internet of Things. This is because security will be an essential supporting factor for the majority of IoT applications.

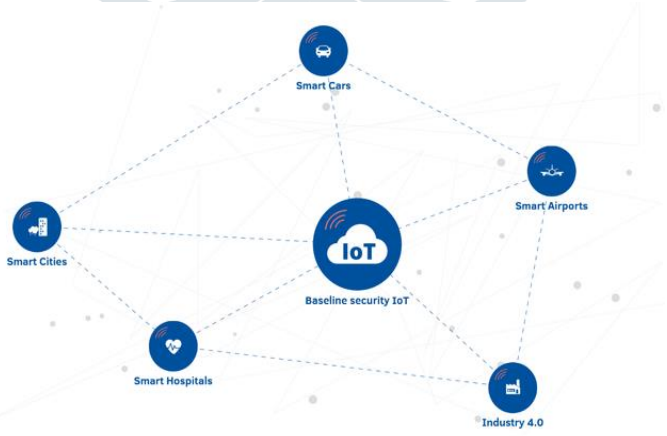

Figure 1: IOT smart infrastructure security

IoT Intrusion Detection Systems (IDS) have been vastly improved because to developments in artificial intelligence (AI) during the last several years. These AI developments include machine learning and deep learning approaches. The present need is to perform a taxonomy that is up to date, comprehensive, and critical of the work that has been done recently. The construction of an IoT intrusion detection system has been validated by a number of relevant research that utilized different machine learning and deep learning approaches using a variety of datasets; nevertheless, it is still unclear whether dataset, machine learning or deep learning techniques are more successful for developing an efficient IoT intrusion detection system.

II. BACKGROUND

H. Hou et al.,[1] To An intrusion detection system (IDS) that is built on hierarchical long short-term memory (HLSTM) networks has been suggested. In order to improve the Internet's overall level of security. With the help of HLSTM, the network is now able to learn across several layers of temporal hierarchy regardless of the network traffic sequences that are being processed. The effectiveness of the system is determined by its performance on the well-known benchmark data set NSL-KDD, which is then compared to the performance of other current approaches. The findings of the experiments show that when compared with other systems now considered to be state-of-the-art, our system has a greater detection performance for a variety of various kinds of cyberattacks. In addition, the classification accuracy of the low-frequency network attack types is better, and the false detection rate is lower.

P. Feng et al.,[2] construct an approximate call graph from the function invocation relationships within an Android application in order to represent this application. They also extract intra-function attributes, such as the required permission, security level, and statistical instructions information, in order to form the node attributes within graph structures. After that, a graph neural network (GNN) is used to produce a vector representation of the program, and malicious software is classified based on this representation. Experiments are carried out on samples derived from actual world applications. The results of the experiments show that our method is superior to other detection strategies in terms of effectiveness and is capable of detecting malware at a higher level than other methods.

S. Deep learning is the basis of a strategy that Liu et al. [3] propose in order to solve the issue of automatically detecting vulnerabilities in binary-level software. The method that has been suggested involves two stages: the first is the extraction of binary functions, and the second is the construction of models. First, we take the binary instructions that have been cleaned up using IDA Pro and extract the binary functions from those instructions. Then, in order to construct the prediction model, we make use of an attention mechanism that is superimposed on top of a bidirectional long short-term memory. We have gathered statistics from a wide variety of sources so that we can demonstrate how successful the strategy that has been suggested is. We have compared the method that we have presented to a variety of baselines, such as approaches that are based on source code and techniques that are based on binary code. We have also implemented the suggested method into real-world IoT-related software, such as the VLC video player and the LibTIFF project, both of which are used in autonomous vehicles. The results of our experiments indicate that the suggested method is superior to the baselines and is able to discover a greater number of vulnerabilities.

Y. Jin et al.,[4] concentrate on these idiosyncrasies and present a technique for identifying malware infected PCs by analyzing unwanted DNS traffic on wireless networks in combination with a DHCP (Dynamic Host Configuration Protocol) server. This approach identifies machines that have been infected with malware by monitoring the traffic. The proposed system may identify computers inside a DHCP-configured environment when they are infected by certain kinds of malware and the malware tries to interact with the relevant C&C servers using the DNS (Domain Name System) protocol. This detection can be accomplished by deploying the system on campus wireless networks. In this study, we present the precise design of the suggested technique, and future work will involve both the development of a prototype and assessments of its effectiveness.

B. Peng et al., [5] proposed a K-NN classification algorithm, which is used to match the characteristic vectors of network data packets in the new energy plant and station system. This matches the characteristic vectors of network data packets in a way that realizes the anomaly detection of network attack scenarios, malformed messages, and irregular business instructions in the new energy plant and station system. In conclusion, a simulation experiment environment of the new energy plant and station system is constructed in order to validate the strategy that was suggested in this piece of research. The findings of the experiments indicate that the algorithm has a strong capability of detecting anomalies and a low incidence of false alarms. It is of the utmost importance to strengthen the degree of network security protection of new energy plants and stations, as well as to guarantee the secure and dependable operation of new energy plants and stations.

W. The dynamic properties of Area Control Error (ACE) are exploited in Bi et al.'s [6] FCPAs in order to identify the tainted data. When compared to FCPAs, VCPAs are a more deceitful form of tax avoidance. To differentiate the signals that have been compromised by VCPAs from the ones that are not affected, a relation-based (RB) feature extraction approach has been developed. Support vector domain description is used to assist in the development of a detection model that does not call for the use of samples that have been compromised. At the conclusion of the day, a thorough detection strategy is developed in order to identify both FCPAs and VCPAs on the LFC system.

K. Liu et al.,[7] examines the issue of intrusion detection for smart homes as well as the many methods that may be used to find intrusions. In this study, we offer a hybrid technique for the detection of intrusions that makes use of both Convolutional Neural Networks (CNN) and K-means. K-means is utilized to construct the rule base by clustering at the smart home device node, and then Principal Component Analysis (PCA) is used to extract the dimensionality reduced features. During the process of testing, principal component analysis (PCA) is used to further extract the dimensionality reduced features, and feature matching is carried out with the rule base in order to ascertain the intrusion data. A CNN model is suggested to be used on the server side of the smart home in order to detect the particular kind of intrusion.

Y. By monitoring DNS name resolution on an application-by-application basis, Jin et al. [8] offer a client-based technique for detecting and preventing anomalous traffic patterns. In the proposed technique, DNS traffic is monitored on the client by means of a collaborative effort between a packet filter and a DNS proxy. This allows for the detection and blocking of traffic that is either headed for IP addresses that were acquired without DNS name resolution or traffic that originates from programs that are not recognized. In addition, a warning box will be shown to the users so that they may choose whether or not to accept the traffic.

This is being done to reduce the risk of false positive detections. We validated that the suggested mechanism functioned as anticipated after putting the proposed system into prototype form and testing it on a Windows 7 client.

R. Velea et al. [9] present a hybrid technique that accelerates pattern matching for malware signatures by using the computational capabilities of both the central processing unit (CPU) and the graphics processing unit (GPU). The method that has been provided focuses on enhancing the performance of string matching algorithms on mobile devices such as ultrabooks and laptops while simultaneously lowering their power consumption.

S. According to Merat et al., [10] research, the primary objective of this study is to advance the field of machine learning by creating an environment in which a variety of distinct kinds of computer processes may be mapped. For the purpose of learning and characterizing the cyber awareness behavior of a computer process in relation to numerous concurrent threads, a software mapping and modeling paradigm known as SHOWAN has been created. In the context of anomaly detection, the studied process initially underperformed and had a tendency to handle a large number of tasks in an inefficient manner, but with time, it progressively learnt to acquire and regulate tasks. The next step that SHOWAN does is to plot the anomalous activities of the manually projected task and compare them to the loading patterns of the other tasks within the group.

S. Cyber-physical systems (CPSs) combine computing with the processes of the physical world, according to Han et al. [11]. Embedded computers and networks monitor and regulate the physical processes; these systems often include feedback loops via which the physical processes may influence the calculations and vice versa. CPS was recognized as one of the eight research priority topics in the report that was submitted in August 2007 by the President's Council of Advisors on Science and Technology. This was done because CPS is expected to become the primary component of a large number of important infrastructures and industrial control systems in the not too distant future. However, CPS is subject to a number of random failures as well as cyber threats, which significantly limit its expansion potential. As a direct consequence of this, the work that is being done will make an attempt to describe how to effectively apply the intrusion detection technique to CPS.

M. According to Bousaaid et al. [12], the introduction of information and communication technologies (ICT) into the field of education gives a significant potential for the dissemination of information. A great number of achievements have already been produced, the primary objective of which was to simplify the organization of instructional material via the widespread use of digital working environments. E-learning has become feasible for students who are geographically dispersed and are enrolled in virtual classrooms as a result of the development of technologies of multimedia, which are connected to those of the Internet, and the democratization of high output. The success of an e-learning course is dependent on a number of factors, the most important of which are the quality and amount of synchronous and asynchronous communication. In order to lessen the sensation of being on your own when e-learning, it is essential to have an appropriate level of supervision. This sense of being on one's own is one of the primary contributors to both the loss of progress and the high rates of stagnation that occur in e-learning.

III. IOT INTRUSION DETECTION SYSTEMS TECHNIQUES

An assault that results in any sort of harm to the confidentiality, integrity, or availability of information is deemed an intrusion. Another way to say this is that an intrusion is any attack that compromises the information in any way. An example of an intrusion would be an assault that would render the computer services inaccessible to the users who were authorized to use them. An intrusion detection system, often known as an IDS, is a piece of software or hardware that monitors and protects a computer network by detecting and reporting harmful activity that occurs on such networks. The primary objective of an intrusion detection system, or IDS, is to identify unauthorized computer use and hostile network traffic. This is something that cannot be done with a conventional firewall. As a consequence of this, the computer systems have become very protected against the harmful acts that may undermine their availability, integrity, or confidentiality.

A. SIDS, which stands for signature-based intrusion detection systems

Knowledge-based Detection is another name for signature intrusion detection systems (SIDS), which are systems that search for known attacks by comparing patterns. These systems use pattern matching methods. When conducting SIDS, matching procedures are used in order to locate a prior incursion. In other words, an alarm signal is generated if an intrusion signature matches the signature of a prior incursion that already exists in the signature database. These signatures are stored in the database. In order to implement SIDS, the logs of the host are investigated in order to detect sequences of instructions or activities that have in the past been associated with malicious software. In the body of academic research, Sudden Infant Death Syndrome has also been referred to as Knowledge-Based Detection and Misuse Detection. Because they scan network packets and conduct matching against a database of signatures, traditional SIDS approaches have trouble spotting assaults that span many packets. This is because these methods do matching on network packets. Because the intricacy of current malware has improved, it may be necessary to extract signature information from numerous packets. Along with this, IDS is going to need to bring the contents of the previous packets. In general, there have been numerous approaches developed for the creation of a signature for SIDS. These methods include the creation of signatures as state machines, formal language string patterns, or semantic requirements respectively.

B. AIDS stands for the anomaly-based intrusion detection system

The ability of AIDS to circumvent the constraints imposed by SIDS has piqued the interest of a significant number of researchers. Methods that are statistically-based or knowledge-based, as well as machine learning, are used in AIDS in order to construct a normal model of the behavior of a computer system. A behavior that significantly deviates from the model is viewed as an anomaly, and this difference in behavior might be understood as an incursion if it is substantial enough. The idea behind this sort

of strategy is to capitalize on the fact that malevolent behavior is distinct from the behavior that is typical of users. An incursion is described as the behavior of aberrant users that deviates from the expected behavior of the system. The first step in the development of AIDS is known as the testing phase, and the second phase is known as the training phase. During the training phase, the regular traffic profile is used to develop a model of normal behavior. This model is then employed in subsequent phases. During the testing phase, a fresh data set is used to improve the system's ability to generalize to previously unforeseen incursions. This takes place in the phase of the process. AIDS may be broken down further into categories such as statistically-based, knowledge-based, and machine learning-based, depending on the approach that was used during training.

The ability to detect zero-day assaults is the primary benefit of AIDS. This is possible since spotting aberrant user behavior does not depend on a signature database. When the investigated conduct deviates from what would be considered normal behavior, AIDS sends out a warning signal. In addition to this, there are a few upsides to having AIDS. First, they have the ability to uncover potentially dangerous behaviors inside the organization. An alert will be triggered in the event that an unauthorized user begins doing transactions in a stolen account that are not consistent with the regular behavior of the account's owner. Second, since the system is built from unique user profiles, it is difficult for a cybercriminal to determine what constitutes typical user activity without triggering an alarm because the system is built from user profiles.

C. Machine Learning Techniques

The process of deriving useful information from vast amounts of data is referred to as machine learning. Models of machine learning consist of a collection of rules, procedures, or sophisticated "transfer functions" that may be used to locate interesting data patterns or to recognize or anticipate behavior. These models can also be used to make predictions. The field of AIDS research has benefited greatly from the use of machine learning methods. A variety of different algorithms and approaches, including as clustering, neural networks, association rules, decision trees, genetic algorithms, and closest neighbor methods, are applied in order to extract the information that is contained within the intrusion datasets.

There is some historical study that has investigated the usage of a variety of methods to construct AIDSs. The performance of two feature selection techniques utilizing Bayesian networks (BN) and Classification Regression Trees (CRC) was analyzed, and the researchers merged these two approaches in order to get a greater level of accuracy.

Methods of feature selection that make use of a number of different feature selection methods, including Information Gain (IG) and Correlation Attribute assessment, are referred to here. They evaluated the efficacy of the chosen characteristics by using a variety of classification approaches, including C4.5, naive Bayes, NB-Tree, and Multi-Layer Perceptron, among others. In order to determine which IDS properties are the most important, a genetic-fuzzy rule mining technique was used. NIDS by using the Random Tree model to enhance accuracy while simultaneously lowering the number of false alarms.

As may be shown in Figure, a number of different AIDSs have been developed using various machine learning approaches. 4. The primary goal of developing IDS via the use of machine learning approaches is to reduce the amount of human expertise that is required while simultaneously improving accuracy. Over the last several years, there has been a discernible rise in the amount of AIDS applications that make use of machine learning methods. The primary goal of IDS research that is based on machine learning is to identify patterns and construct an intrusion detection system based on the dataset. Supervised and unsupervised machine learning techniques are the two primary classifications that can be found throughout the field.

IV. CONCLUSION

In this research, a comprehensive evaluation of IoT intrusion detection system methodology, deployment strategy, validation approach, Dataset, and technology was offered, along with an analysis of the benefits and drawbacks associated with each. Review is given to a number of different intrusion detection systems that have been suggested to detect assaults on the internet of things. However, owing to the design of the Internet of Things, such methods could struggle to identify all Internet of Things assaults. In order to construct viable Internet of Things intrusion detection systems based on a variety of device types, unique IDS will need to be developed. We are aware of a few components that play an essential role in the construction of dependable IDS for the internet of things. First, minimize the number of false positives that result from the enormous amount of data. Second, you need to have a high degree of adaptability to extreme IoT communication systems. This is because unexpected behavior in IoT sensors that seemed normal at one time may now be starting to contemplate assaults.

REFERENCES

1. H. Hou et al., "Hierarchical Long Short-Term Memory Network for Cyberattack Detection," in IEEE Access, vol. 8, pp. 90907-90913, 2020, doi: 10.1109/ACCESS.2020.2983953.
2. P. Feng, J. Ma, T. Li, X. Ma, N. Xi and D. Lu, "Android Malware Detection Based on Call Graph via Graph Neural Network," 2020 International Conference on Networking and Network Applications (NaNA), 2020, pp. 368-374, doi: 10.1109/NaNA51271.2020.00069.
3. S. Liu, M. Dibaei, Y. Tai, C. Chen, J. Zhang and Y. Xiang, "Cyber Vulnerability Intelligence for Internet of Things Binary," in IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 2154-2163, March 2020, doi: 10.1109/TII.2019.2942800.
4. Y. Jin, M. Tomoishi and N. Yamai, "Anomaly Detection by Monitoring Unintended DNS Traffic on Wireless Network," 2019 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM), 2019, pp. 1-6, doi: 10.1109/PACRIM47961.2019.8985052.
5. B. Peng, Q. Wang, X. Li, J. Cai, J. Fei and W. Chen, "Research on Abnormal Detection Technology of Real-Time Interaction Process in New Energy Network," 2019 International Conference on Internet of Things (iThings) and IEEE

Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2019, pp. 433-440, doi: 10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00092.

6. W. Bi, K. Zhang, Y. Li, K. Yuan and Y. Wang, "Detection Scheme Against Cyber-Physical Attacks on Load Frequency Control Based on Dynamic Characteristics Analysis," in IEEE Systems Journal, vol. 13, no. 3, pp. 2859-2868, Sept. 2019, doi: 10.1109/JSYST.2019.2911869.
7. K. Liu, Z. Fan, M. Liu and S. Zhang, "Hybrid Intrusion Detection Method Based on K-Means and CNN for Smart Home," 2018 IEEE 8th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), 2018, pp. 312-317, doi: 10.1109/CYBER.2018.8688271.
8. Y. Jin, K. Kakoi, N. Yamai, N. Kitagawa and M. Tomoishi, "A Client Based Anomaly Traffic Detection and Blocking Mechanism by Monitoring DNS Name Resolution with User Alerting Feature," 2018 International Conference on Cyberworlds (CW), 2018, pp. 351-356, doi: 10.1109/CW.2018.00070.
9. R. Velea and Ș. Drăgan, "CPU/GPU Hybrid Detection for Malware Signatures," 2017 International Conference on Computer and Applications (ICCA), 2017, pp. 85-89, doi: 10.1109/COMAPP.2017.8079736.
10. S. Merat and W. Almuhtadi, "Artificial intelligence application for improving cyber-security acquirement," 2015 IEEE 28th Canadian Conference on Electrical and Computer Engineering (CCECE), 2015, pp. 1445-1450, doi: 10.1109/CCECE.2015.7129493.
11. S. Han, M. Xie, H. Chen and Y. Ling, "Intrusion Detection in Cyber-Physical Systems: Techniques and Challenges," in IEEE Systems Journal, vol. 8, no. 4, pp. 1052-1062, Dec. 2014, doi: 10.1109/JSYST.2013.2257594.
12. M. Bousaaid, T. Ayaou, K. Afdel and P. Estraillier, "Hand gesture detection and recognition in cyber presence interactive system for E-learning," 2014 International Conference on Multimedia Computing and Systems (ICMCS), 2014, pp. 444-447, doi: 10.1109/ICMCS.2014.6911197.