A survey on Cyber-Physical System Cybersecurity: Deep Learning-Based Attack Detection.

Bharath N
Department of MCA
AMC Engineering College, Banglore
Bharathnr63825@gmail.com

Ms.Barnali Chakarobathy
Associate Professor
Department of MCA
AMC Engineering College, Banglore

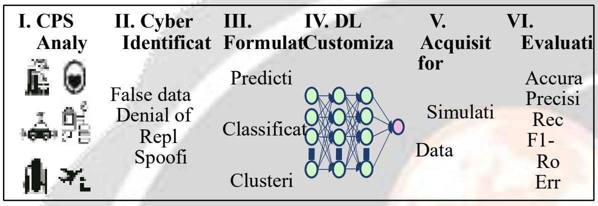
Abstract

The detection of cyber-attacks on physical systems is a pressing issue in the current cyber landscape. To address this, machine learning techniques have been developed. Deep learning has been found to be more effective than traditional machine learning, however, its implementation in the field of Consumer Protection Systems (CPS) cybersecurity is slower than in other areas. A number of recent papers have proposed deep learning models to detect cyber-attacks on Consumer Protection Systems (CPS). This is due to the complexity of the overlap between cybersecurity and CPSs, making it difficult to accurately identify cyberattacks. To address this issue, a dataset was used from the University of South Wales-NB15 and Logistic regression and Linearized Stemweight Modeling (LSTM) algorithms were implemented. The results of the experiment demonstrate the accuracy of the two algorithms. The index terms utilized in the scope of the study are: "Cyber-physical System," "Cybersecurity," "Deep Learning," "Detection of Intrusions," and "Pattern Grouping".

INTRODUCTION

CPSs have been affected by cyber-attacks as they have become more interconnected with the internet. Automated assault tools and cyber attacks have become more advanced and common, with professional hacking groups taking part in them. A successful attack on a CPS could have catastrophic, serious, or even deadly consequences. CPSs lack cyber security features such as message authentication, which makes it difficult to detect a false data injection attack. Eavesdropping attacks are difficult to protect against due to the absence of universal encryption on systems using outdated technologies. Hacking incidents are on the rise every day as new technologies are developed. Companies report large numbers of hacking incidents every year. In June 2007, Estonia suffered a DDoS attack on its websitesOn 17th September 2008, Amazon began getting requests from multiple people in one of their locations. The requests started to pile up, causing the servers to slow down. According to ENISA, Dropbox was attacked with a DDoS in January 2013, and the service was out for over 15 hours, affecting people all over the world. Facebook was also hit by a suspected DDoS attack on 28th September 2014. Cisco's Annual Security Report said that 50% of attacks on cyber systems are preceded by some kind of network scanning. Attacks don't just involve flooding and probing, but also using malware files like viruses, worms, and spams to take advantage of weaknesses in existing software and get access to people's sensitive info. In April 2013, Cisco reported that 40% of spam sent around the world was related to the bombing of the Boston Marathon. In 2017, Cisco's survey of top five malware used to get into people's computers and organizations showed that Trojan was at the top. Security in today's tech world is a huge challenge, and it's important to tackle it in an intelligent way. Researchers have come up with a variety of different types of attacks to detect intrusions. These include denial of service (DoS), scanning (Probe), and R2L (Remote to Local) and U2R (User to Root) attacks, which are all based on the KDD'99 dataset. The most recent attack dataset, UNSW-NB, breaks down attacks into nine different categories: fuzzer, analysis, reconnaissance, shell code, worm, generic, doS, exploit and generic. Currently, security solutions include middle-boxes like firewalls, antivirus and intrusion detection systems (IDS). Firewalls control what traffic goes in and out of a network, and they're limited by how much data they have and how well they know the system. hosts that receive the content. An IDS (Identifying and Detecting System) is a security tool used to scan the system for any suspicious activity and analyze network traffic before notifying the system or the network administrator. Network based intrusion detection systems (NIDSs) are typically installed at the network point like router and gateway. There are three types of detection mechanisms used by IDS: misuse detection, anomaly detection, and hybrid detection. In misuse detection, an IDS keeps a set of known attack types in a knowledge base of rules. In knowledge based techniques, network traffic or host audit data (e.g., system call traces, etc.) are compared to predefined rules/attack patterns. There are three main types of knowledge based techniques: Signature matching State transition analysis rule based expert systems In previous articles, we have looked at data-driven methods for identifying the cyberattacks on the CPS systems, but there is no comprehensive explanation on how to use the DL techniques to detect the CPS cyberattacks, only a short survey with a 4-step framework for applying the DL methods on the CPS issues such as cybersecurity, adaptiveness, recoverability and many others, but with no specific focus on the cybersecurity. Without looking at the DL models in detail, we have presented an extensive survey on the cyber attacks on the CPSs, various methods of detecting the CPSs cyber-attacks were summarised in without using the DL methods in detail. The main objectives of our project are: Classifying or predicting the cyber attacks in the network efficiently Implementing the various classification algorithms for improved performance Enhance the overall performance of classification algorithms

RESEARCH METHODOLOGY



Our methodology is based on a deep understanding of the publications we're looking at. There are six of them involved in the process. Steps: CPS scenario analysis Identifying the cyber attack Formulating the DL problem Building the DL model Collecting the data Analyzing the performance Method for using DL models to detect cyberattacks within a CPS For example, misconfigured controls from electric load projections could affect a smart grid Before committing to the prediction process, find and remove the false injected messages containing the maliciously constructed information. Stacked Auto It was proposed that an Auto Encoder (AE) could be employed to anticipate the power load of the system. Subsequently, sufficient simulation data was used to select the chosen Auto Encoder, and a Dynamic Linear Model (DL Model) was trained to provide excellent prediction results, with an average Absolute Percentage Error (APG) on annual predictions of

.Step I: CPS Scenario Analysis

The day-to-day operations of CPSs depend on reliability, real-time performance, fault tolerance, cyber security, and more. We need to look at these requirements from all angles. Real-time performance is important for keeping the system running smoothly when inputs and environment changes quickly. Dependability is about having service availability and reliability so you don't have to worry about system downtime. Fault tolerance is about making sure the critical parts of the system have enough backups so they don't shut down. Cybersecurity is becoming more important as more CPSs connect to the internet. Mitchell et al. point out that there are four main types of CPS intrusion detection: physical process monitoring, controlled loops, sophistication of attack, and legacy technology.

Monitoring Physical Processes: As many of the physical processes of a CPS are governed by physical laws, it is essential to monitor for any discrepancies in the physical characteristics of the system. Closed Control Loop: As many CPS occurrences are controlled by pre-determined feedback-oriented controllers, these events are much more predictable and consistent than those triggered by user input.

Attack complexity: Sophisticated attacks are on the rise in the CPS context because a successful attack could potentially provide sensitive information, critical intelligence for a military or financial operation, and much more.

Legacy technology: As legacy mechanical and hydraulic control is already in place, legacy hardware often used in CPSs cannot talk to software-defined control (SDC).

Identifying the characteristics of a specific CPS scenario will help you create a suitable cybersecurity problem. Physical signals: Physical signals enrich the inputs and make it more challenging to develop any security solution for CPSs. Real-world systems operate in noisy environments with unprecedented cyber risks. Even if the behaviors of simple POCs are relatively consistent and predictable,B. Step II: Cyber

Attack Identification

Once we've got the CPS scenario figured out, we need to come up with a list of the right cyber attacks based on the CPS characteristics. For example, if we keep an eye on how the CPS components are running, we'll be more likely to catch the malicious network packets. We need to think about known attacks and more advanced ones, like web attacks, too. Like, if you have a closed control loop on a CPS, you might be able to spot replay attacks. We also need to think about attack sophistication - denial of service and replay attacks are usually more common in places with older tech. Based on the papers we looked at, there are lots of common cyberattacks on industrial control networks, like false data injection, DoS, replay, and more. Plus, there's the usual stuff like brute force and botnet attacks. Cyberattacks such as Web Attacks, Heart Bleed Attacks, Infiltration Attacks, and many more are common cyberattacks against Software-as-a-Service (SaaS) controllers with a central server. In order to effectively and efficiently detect these cyber threats, it is necessary to bring the cybersecurity challenge into the Machine Learning (ML) arena by utilizing Domain Layering (DL) models.

C. Step III: This text is about ML problem formulation.

Once the cyber attacks have been aligned to the characteristics of the CPS, the research challenge can be moved into the domain of Machine Learning (ML) and Deep Learning (DL). ML is defined as the process of a computer program learning from experience E in relation to a set of tasks and performance measure P, where the effectiveness of the program in tasks in T is measured by the improvement of experience E. DL is defined as the solution of a complex problem through the use of a hierarchy of simpler concepts without the need for human intervention. The ML solution will be implemented in several steps, and ML is a broad concept. In the first step, the task must be defined, including classifications, clusters, and regression. Classifications require the trained model to assign output to a predefined set of classes, which may be the specific categories of cyber attacks. Clusters are often assigned to a few classes, which may indicate normal traffic. The selection of Machine Learning (ML) tasks will influence the development of Deep Learning (DL) models. A regression task is also referred to as a prediction task, and requires the trained model to provide numerical value predictions. Examples of regression tasks include a classification problem to distinguish cyber attack types, a clustering problem to distinguish covert messages from normal messages, and a regression task to predict the electrical load of a smart grid.

D. Step IV: DL Model Customization

The design of a Deep Learning model begins with the selection of an architecture appropriate to the study problem, followed by the optimization of parameters. Selecting a DL model must be based on real-world requirements. Autoencoders, for instance, are well-equipped to translate the input data, making them suitable for learning representations of the data that are commonly used in prediction or regression problems. In classification problems, CNNs and other models are commonly employed.

The amount of data available also affects the model configuration. For example A multi-neuron DL model will almost always need more data to achieve the same results as a DL model that has the same design but only a couple of neurons per layer. This trade-off doesn't have to be limited to increasing the layer size. You can also use multiple layers within a single DL model to get similar results. You can explore methods and insights based on a deep understanding of DL algorithms as well as CPS cybersecurity data. You can also make improvements at different levels by connecting the selection of a DL model to a particular research problem.E.

Step V: Data Acquisition for Training

Acquiring data is a key part of training DL models, and the quality and amount of data you have will affect how well you can solve your research problem. Data can also be used as a source of ground truth and can influence the performance of the prediction model. Simulation is a great way to get data, and it's one of the easiest ways to do it. You can use it to get data for power grids, like IEEE 9-Bus, IEEE 14-Bus, IEEE 30-Bus, and IEEE 118-Bus systems. Another way to get data is to use different datasets that other scientists have collected. Examples of these are SWaT data, SCADA data, CICIDS data, UNSWNB data, and KDD99 cup data.

The datasets covered a variety of cyberattacks:

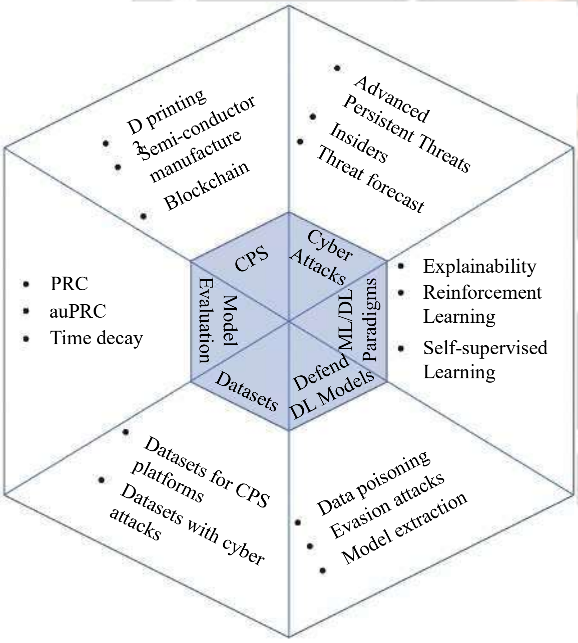
A dataset of eleven days of network traffic originating from a simulated Water Treatment Facility (SWaT) was collected. During the initial seven days, no attacks were detected. This dataset contains 36 distinct cyber attacks, which are most commonly encountered in contemporary CPS systems. Additionally, network traffic logs from an Industrial Control System (SCADA IDS) were also included in the dataset. This dataset is composed of seven distinct forms of cyber attacks, including recon attack, do not scan attack, random response packet injection, concealed controlled process state, malicious state command injection, malicious parameter command injection, recon attack, and more. In addition, six different categories of cyberattacks were also included in the dataset (CICIDS 2017): brute force attack; botnet attack; do not scan attack; web attack; heartbleed attack; and penetration.

Bot-IOT dataset includes network traffic logs collected from an IoT installation. Power system dataset includes network traffic collected from a Power system. Data injection Remote command injection Survey attacks Worms Fuzzers Web penetration attacks Backdoors Shellcode Generalized attacks Block ciphers Denial-of-service Unauthorized accesses Privilege escalation Proximity exploit attacks KDD99 Cup dataset Collection of network traffic data collected from the annual KDD99 Cup conference in 1999.

Step VI: Is all about evaluating how you're doing.

The final phase is performance evaluation, where we determine if the DL model meets our expectations. Performance is typically measured using different metrics. Depending on the tasks, we break down the performance metrics into two categories: 1) For prediction and regression tasks, we use several error metrics to measure performance. These metrics include: 1.1. Mean Absolute Error (MAE) 2. Mean Relative Error (MRE) 3. Root of Mean Sorted Error (RMSE) 4. Mean Absolute Percentage Error (MAPE) 5. Accuracy 6. Recency 7. Precision 8. False Positive Rate (FPR) 9. F1 score

classification and cluster tasks. Receiving Operating Characteristics Curves Sometimes graphical plots called ROC curves are used to illustrate trade-offs in benefits and costs. TPR is placed on y axis and FPR is placed on x axis. The cumulative strength of any given ROC curve can be measured by the area below the curve (aROC). FPR is often a problem for DL models. The manual verification costs of false alarms are nearly always too high and it is always difficult to detect rare or unknown attacks as demonstrated in most of the literature. Most of the literature focused on maximizing TPR and minimizing FPR. Regression task error rate is tolerable more lenient than classification task error rate. We can measure the quality of the outputs of a particular DL model by using detailed evaluation measures. Whenever there is an unsatisfactory result, repeat the process with appropriate adjustments.



EXISTING SYSTEM

The current system provides a comprehensive overview of newly proposed Deep Learning (DL) solutions for the detection of cyber-attacks in the CPS environment. To summarise and analyse the reviewed literature for the use of DL approaches to detect cyberattacks in CPS systems, the methodology is presented in the form of a six-stage DL driven methodology. This methodology involves analysing CPS scenarios, identifying cyberattacks, generating ML problems, customizing DL models, collecting training data, and evaluating performance. The reviewed works suggest that there is considerable potential for detecting cyber-attacks in CPS using DL modules. Excellent performance is further facilitated by the availability of a number of high quality datasets that are readily available to the public. Future research opportunities, challenges, and trends are also discussed.

PROPOSED SYSTEM:

In this system, we have taken the UNSW- NB15 dataset as the input. We have taken the input data from the repository. We have to implement the pre-processing step for the data. In this step, we have to solve the missing values to avoid incorrect prediction. We have to encode the input data's label. We have to divide the dataset into the test and the train. The data distribution is based on the ratio. The train will contain most of the data. The test will contain less data. The model is evaluated during the training phase. Predictions are made during the test phase. We have to set up the classification algorithms (i.e., machine and deep learning). We have set up machine learning algorithms like Logistic regression, and deep learning algorithm like LSTM. The experimental results show that the performance metrics like accuracy and comparison results.

CONCLUSION:

This survey provides an up-to-date perspective on the detection of cyber attacks in CPSs. The six-step DL-driven methodology is designed to summarise and analyze the twenty newly published papers contained in the survey. An in-depth view is obtained by analysing the CPS scenarios, uncovering cybersecurity threats, and transposing the research challenge into the domain of ML/DL. Construction of the DL model, preparation of datasets, and assessment of the mode lCyberattacks remain a major threat to the protection and safety of Consumer Product Safety Programs. The reviewed works illustrate the potential of utilizing CPS cyber data through the use of Data Loss Modeling (DL models). This is achieved through the utilization of a number of high-performing datasets that are easily accessible to the public. Several promising research topics have been identified, such as Integrate with blockchain. Detect advanced persistent threats. Adopt new ML/DL paradigms. Prevent adversary model extraction attacks. Enrich datasets. Use additional performance metrics, monitoring of existing research, and we hope and anticipate that this field will continue to grow. In conclusion, we used the following dataset as an input: Our research paper mentions the following input dataset: Machine and Deep Learning classification algorithms Machine Learning algorithms Logistic Regression deep learning algorithms LSTM The result shows that: The accuracy of the algorithm mentioned above The estimated performances metrics of the two algorithms The comparison graph

REFERNCES

1. S. Yinbiao and K. Lee, "Internet of Things: Wireless Sensor Networks Executive summary," 2014. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci
2. "A survey on sensor networks," IEEE Commun. Mag., vol. 40, no. 8, pp. 102–105, 2002.
3. X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: a survey," IEEE Commun. Surv. Tutorials, vol. 11, no. 2, pp. 52–73, 2009.
4. A.-S. K. Pathan, H.-W. Lee, and C. S. Hong, "Security in wireless sensor networks: issues and challenges," 2006 8th Int. Conf. Adv. Commun. Technol., vol. 2, p. 6 pp.-pp.1048, 2006.