IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, April 2023

Cyber Hacking Breaches Prediction using Machine Learning

Sampath Kumar R[1], Krishna V R[2], N Ashok Reddy[2], N Naveen Upadhyaya[4], Abdula Muaz Ali[5]
Assistant Professor, Department of Computer Science[1]
Students, Department of Computer Science[2,3,4,5]
Rao Bahadur Y Mahabaleswarappa Engineering College, Bellary, Karnataka, India
krishna.cse.rymec@gmail.com, ashokreddy.cse.rymec@gmail.com,
naveen.cse.rymec@gmail.com, muiz.cse.rymec@gmail.com

Abstract: *Cyber-attacks are a major threat to these systems. Unlike faults that occur by accidents in cyber-physical systems, cyber-attacks occur intelligently and stealthily. Some of these attacks which are called deception attacks, inject false data from sensors or controllers, and also by compromising with some cyber components, corrupt data, or enter misinformation into the system. If the system is unaware of the existence of these attacks, it won't be able to detect them, and performance may be disrupted or disabled altogether. The proposed method in this study is to use the structure of deep neural networks for the detection phase, which should inform the system of the existence of the attack in the initial moments of the attack. In the presented control method, after the attack detection phase with the use of a deep neural network, the control system uses the reputation algorithm to isolate the misbehaving agent. Experimental analysis shows us that deep learning algorithms can detect attacks with higher performance than usual methods and can make cyber security simpler, more proactive, less expensive, and far more effective.*

Keywords: Cyber-attacks, Cyber Hacking, Cyber-hacking breaches

I. INTRODUCTION

Recent advances in technology have led to the introduction of cyber-physical systems, which due to their better computational and communicational ability and integration between physical and cyber-components, has led to significant advances in many dynamic applications. But this improvement comes at the cost of being exposed tocyber-hacking. Cyber-physical systems are made up of different typesof logical elements and embedded system computers. Which will be communicating with communication channels such as the Internet of Things. More specifically, these systems include different digital or cyber components, analogy components, physical devices, and humans that are designed to operate between physical and cyber parts. In other words, we can say that a cyber-physical system is a type of system that includes cyber components and physical components and humans and can trade between the physical and cyber parts. In cyber-physical systems, the security of these types of systems becomes more important due to the addition of the physical part. The Physical component, which includes sensors that receive data from the physical environment, can be attacked and injected with incorrect data into the system. One of the most important challenges of a cyber-physical system, in its physical part is the presence of a large number of sensors in the environment, which collect a large number of data, with so much variety, and at high speed. Also, the connection between the sensors, the necessary calculations, and the analysis of the obtained data will be one of the main challenges. Therefore, one of the most important features of a cyber-physical system is to communicate between these sensors and compute and control the system. The security of cyber-physical systems to detect cyber-attacks is an important issue in these systems. It should be noted that cyber-attacks occur in different ways, and it is not possible to describe these attacks in a regular and orderly manner. In general, cyber-attacks in cyber-physical systems are divided into two main types: Denial of service (Dos) and deception attacks. In denial of service, the attacker prevents communication between network nodes and communication channels. However, deception attacks that administer false data to the system, are carried out by abusing system components, such as sensors or controllers, and they can corrupt data or enter incorrect information into the system and cause misbehaving.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, April 2023

II. LITERATURE SURVEY

Here is a literature survey on the paper presents a security analysis of cyber-physical systems (CPS) against stealthy deception attacks, which are aimed at manipulating the behavior of the system without being detected model, Kwon, Cheolhyeon, Weiyi Liu, and Inseok Hwang "Security analysis for cyber-physical systems against stealthy deception attacks using machine learning model, in IEEE (2013). This paper proposed the design and implementation of attack-resilient cyber-physical systems with a focus on attack-resilient state estimators. The authors propose a framework for designing resilient systems that includes threat models, security requirements, attack detection and identification, and response strategies. Pajic, Miroslav, James Weimer, Nicola Bezzo, Oleg Sokolsky, George J. Pappas, and Insup Lee. "a Design and implementation of attack-resilient cyber-physical systems: With a focus on attack-resilient state estimators' model", IEEE Control Systems (2017). This paper presents a consensus formation control algorithm for a group of mobile robots with directed communication networks. The proposed algorithm ensures that the robots converge to a desired formation and maintain it despite disturbances and communication delays, Sheng, Long, Ya-Jun Pan, and Xiang Gong." Consensus formation control for a class of networked multiple mobile robot systems." Journal of Control Science and Engineering 2012 (2012). This paper proposes a distributed control approach for networked control systems that can tolerate the presence of misbehaving agents. The authors describe a method for designing a resilient controller that can mitigate the effects of malicious or faulty agents in a network, while still achieving satisfactory performance, Zeng, Wente, and Mo-Yuen Chow. "Resilient distributed control in the presence of misbehaving agents in networked control systems", IEEE Transactions on Cybernetics (2014).The authors propose a resilient control scheme that uses a state feedback controller and an observer-based controller to mitigate the effects of the DoS attacks model, Sun, Hongtao, Chen Peng, Taicheng Yang, Hao Zhang, and Wangli He. "Resilient control of networked control systems with stochastic denial of service attacks". Neurocomputing 270 (2017).

III. PROPOSED SYSTEM

Many machine learning models have been proposed to determine whethera cyberattack is likely to occur, but it is not enough to solve this serious problem. In addition, similar studies that propose models for evaluating such activities often do not take into account the variability andsize of the data. Therefore, we propose support vectors, decision trees, random forests, and Cat Boost classifier techniques.

IV. METHODOLOGY

Using machine learning to predict network hacking is an active area of research and development. Here is an overview of the proposed system:

- Data collection: Collecting and analyzing historical data on cyber-attacks and security breach is the first step in creating a forecast. This information may include information about the type of attack, the target, the time of the attack, and other relevant factors.
- Preliminary Data: Collected data must be pre-processed before being fed into the machine learning algorithm. These steps include removing missing values, excluding items, and modifying the data to make it suitable for analysis.
- Feature extraction: The next step is to extract relevant features from previous data. These attributes may include the type of attack, its focus, the duration of the attack, and other relevant information.
- Model selection: After feature extraction, we need to choose the appropriate machine learning algorithm to predict network hacking. Some popular algorithms for this purpose include decision trees, random forests, and neural networks.
- Model Training: After choosing the machine learning algorithm, we must train and extract the model using the previous data. This includes dividing the data into training and validation and then showing the structure of the training process.
- Model Evaluation: After the model is trained, we need to evaluate its performance in the validation process. This helps us determine if the model is over or under-fitting the data and whether there is room for improvement.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, April 2023

- Model Deployment: Finally, once we are satisfied with the model's performance, we can send it to production to predict future cyber-attacks. The system should be constantly monitored and updated as new information becomes available.

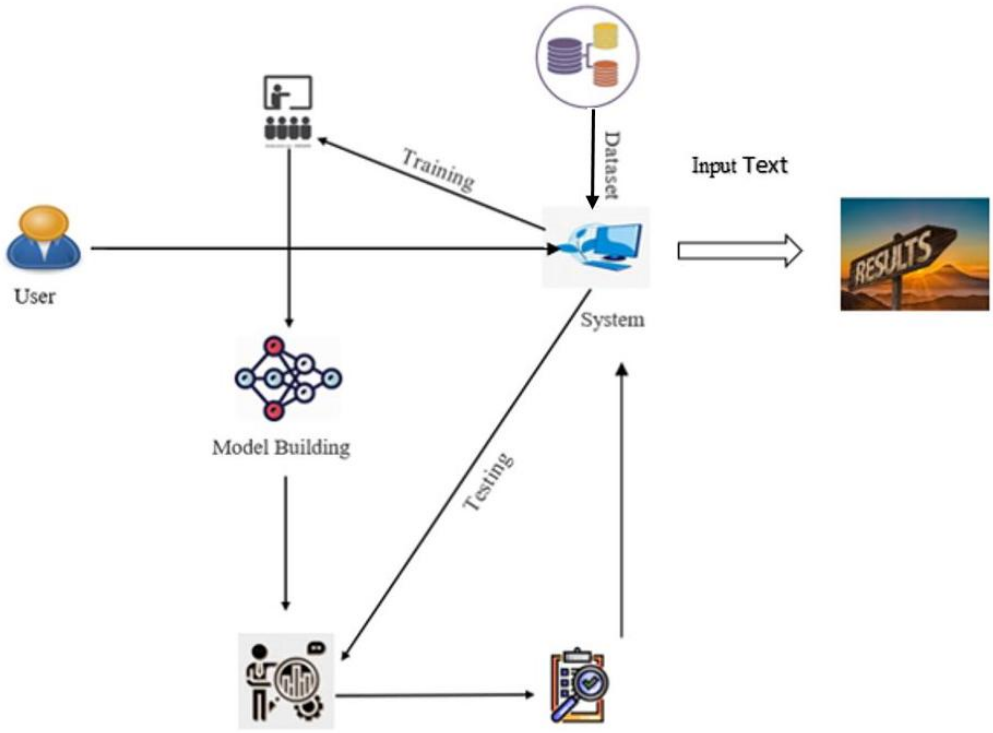
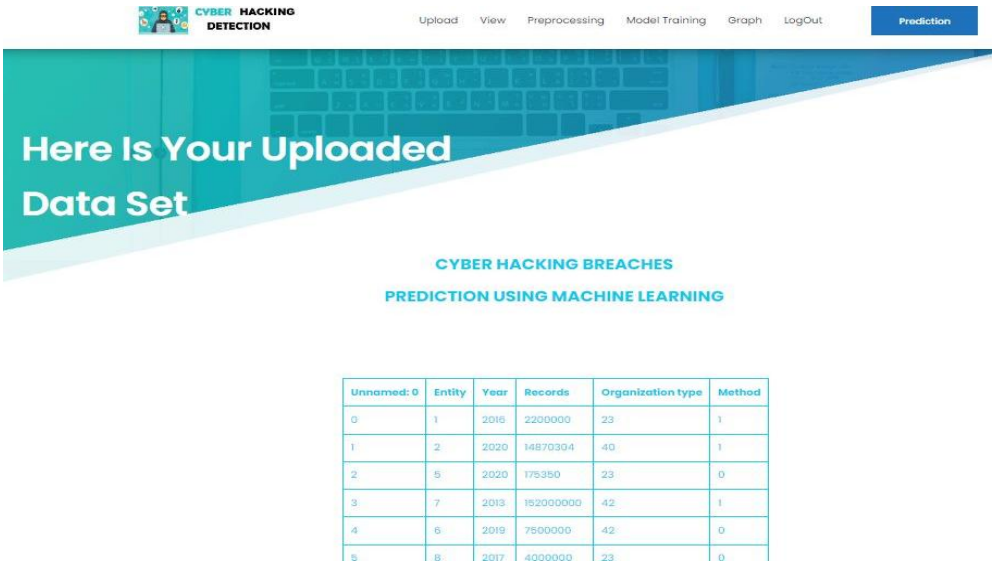


Figure 1: Representation of the architecture model.

V. EXPERIMENTAL RESULT

Figure 2: Representation of the main page.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, April 2023



Unnamed: 0	Entity	Year	Records	Organization type	Method
0	1	2016	2200000	23	1
1	2	2020	14870304	40	1
2	5	2020	175350	23	0
3	7	2013	152000000	42	1
4	6	2019	7500000	42	0
5	8	2017	4000000	23	0

Figure 3: Representation of the Uploaded data set.

VI. CONCLUSION

In this study, an attempt was made to use the resilient control consensus method in complex discrete cyber-physical networks in several local Cyber hacking breaches. By applying this control method, it was observed that even in the presence of Cyber hacking breaches, the system can remain stable and isolate the Cyber hacking node, and the performance of the system is not weakened. The system has less complexity. So,withthe deep learning method, systems can analyze patterns and learn from them to help prevent similar attacks and respond to changing behavior. In short, machine learning can make cybersecurity simpler, more proactive, less expensive, and far more effective. After observing the state of the system reported by the neural network, the control system makes decisions based on it and, if there is Cyber hacking, detects it and isolates it, so as not to have a detrimental effect on the behavior of other agents.

REFERENCES

[1]. "Security analysis for cyber-physical systems against stealthy deception attacks". In 2013 American control conference. Available [online]:
[2]. "Design and implementation of attack-resilient cyber-physical systems: With a focus on attack-resilient state estimators." IEEE Control Systems Magazine (2017). Available [online]:
[3]. "Consensus formation control for a class of networked multiple mobile robot systems." Journal of Control Science and Engineering 2012 (2012). Available [online]:
[4]. "Resilient distributed control in the presence of misbehaving agents in networked control systems."IEEE Transactions on Cybernetics (2014). Available [online]:
[5]. "Resilient control of networked control systems with stochastic denial of service attacks." Neurocomputing (2017). Available [online]:
[6]. "Robustness of information diffusion algorithms to locally bounded adversaries." In 2012 American Control Conference (ACC), IEEE (2012). Available [online]:
[7]. "Resilient Consensus of Discrete-Time Complex Cyber-Physical Networks under Deception Attacks." IEEE Transactions on Industrial Informatics (2019). Available [online]:
[8]. "Machine learning methods for attack detection in the smart grid." IEEE Transactions on neural networks and learning systems 27, (2015). Available [online]:
[9]. "Data mining based cyber-attack detection." System simulation technology 13, (2017). Available [online]:
[10]. "Attack detection and identification in cyber-physical systems." IEEE Transactions on Automatic Control (2013). Available [online]: