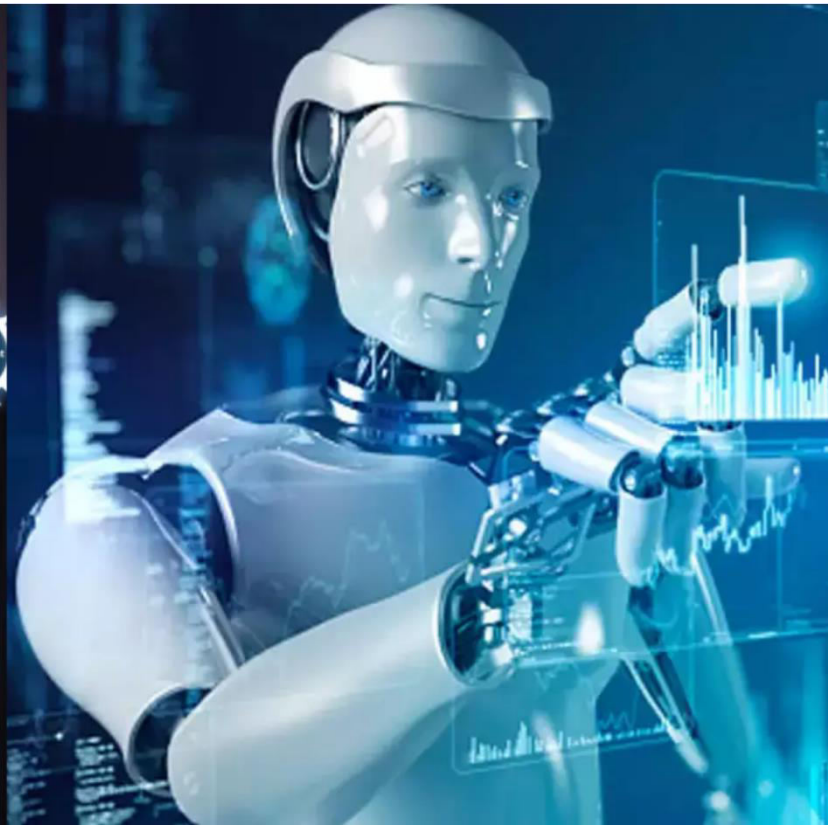
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 5, May 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405370|

Detection of Cyber Attacks using Artificial Intelligence

Likhith G, Jaffer Ali, Vidyashree R

Dept. of Information Science and Engineering, Vemana Institute of Technology, Bangalore, Karnataka, India

Dept. of Information Science and Engineering, Vemana Institute of Technology, Bangalore, Karnataka, India

Dept. of Information Science and Engineering, Vemana Institute of Technology, Bangalore, Karnataka, India

ABSTRACT: Cyber-physical systems (cps) have contributed greatly in various dynamic applications since there has been integration among physical process, computer resources, and communitcating ability. Cyber-attacks pose a high risk to such systems. Cyber-attacks, unlike faults which happen by coincidence cyber-physical systems, take place wisely and covertly. These attacks, referred to as fraud attacks, introduce incorrect data from sensors or controllers and also by compromising with certain cyber elements, corrupt data or feed misinformation into the system. If the system does not know of such attacks occurring, then it will not be able to detect them, and performance could be disturbed or disabled entirely. Hence, it is required to transform algorithms so that it is possible to recognize these kinds of attacks in such systems. It is worth mentioning that the information produced in these systems is created in extremely large quantity, with so high variety, and speed, so it is necessary to apply machine learning algorithms so that it is easy to analyze and compare data and recognize hidden trends. In this study, the CPS is represented as an agent network with agents that have motion in their union with the other agents and one agent can be taken as a leader and the rest of the agents can be commanded by the leader. The technique proposed in this research is applying the architecture of deep neural networks to the detection stage, which will notify the system of the presence of the attack in the early stages of the attack. Applying resilient control algorithms within the network to encapsulate the misbehave agent within the leader-follower mechanism has been explored. 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 misbehave agent. Experimental analysis shows us that deep learning algorithms can detect attacks with higher performance that usual methods and can make cyber security simpler, more proactive, less expensive and far more effective.

KEYWORDS: Detection, Cyber Attack, Artificial Intelligence, Cyber security threat Detection.

I. INTRODUCTION

Advancements in contemporary technology have been accompanied by the emergence of cyber-physical systems, which offer enhanced computational and communication capabilities along with cyber and physical integration, leading to fundamental improvements in many dynamic applications. However, with this advancement comes an increased risk of vulnerability to cyber-attacks. Cyber-physical systems are composed of logical elements and embedded computers that interact through communication channels like the Internet of Things (IoT). These systems consist of digital or cyber elements, analog components, physical devices, and humans, all intended to share information between the physical and cyber domains. Essentially, a cyber-physical system is any setup involving cyber and physical elements, along with human interaction, capable of operating across both spaces. With the advancement of physical components, stronger physical security becomes necessary. Physical aspects such as sensors, which gather data from the real world, can malfunction and deliver incorrect information to the system. One of the key challenges in CPS is managing the large number of sensors that collect vast, diverse, and high-speed data. Integrating these sensors with the necessary computation and processing capabilities becomes critical. Thus, one of the main features of a cyber-physical system is its ability to share information across sensors, perform computation, and control system behaviour. Ensuring CPS security against cyber-attacks is a significant concern. Cyber-attacks are unpredictable and cannot be addressed using regular, periodic methods. Generally, cyber-attacks in CPS fall into two categories: denial of service (DoS) and deception attacks. DoS attacks disrupt communication between network nodes and communication channels, while deception attacks involve injecting false data by misusing system components like sensors or controllers, leading to data corruption or misinformation that can result in abnormal behaviour. These attacks can sometimes be detected

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405370|

through system monitoring, but when an attacker launches a stealthy deception attack that avoids detection, traditional countermeasures fail. This highlights the importance of being constantly aware of potential threats so that systems can respond in time. A vigilant security system is essential to detect and manage such attacks effectively. Cyber defense can be strengthened by using security analytics to identify hidden patterns and deception strategies

II. LITERATURE SURVEY

[1] Kwon, Cheolhyeon, Weiyi Liu, and Inseok Hwang. "Security analysis for cyber-physical systems against stealthy deception attacks." In 2013 American control conference, IEEE (2013): 3344-3349

The security issue in the state estimation problem is investigated for a networked control system (NCS). The communication channels between the sensors and the remote estimator in the NCS are vulnerable to attacks from malicious adversaries. The false data injection attacks are considered. The aim of this paper to find the so-called insecurity conditions under which the estimation system is insecure in the sense that there exist malicious attacks that can bypass the anomaly detector but still lead to unbounded estimation errors. In particular, a new necessary and sufficient condition for the insecurity is derived in the case that all communication channels are compromised by the adversary. Moreover, a specific algorithm is proposed for generating attacks with which the estimation system is insecure. Furthermore, for the insecure system, a system protection scheme through which only a few (rather than all) communication channels require protection against false data injection attacks is proposed. A simulation example is utilized to demonstrate the effectiveness of the proposed conditions/algorithms in the secure estimation problem for a flight vehicle.

[2] Pajic, Miroslav, James Weimer, Nicola Bezzo, Oleg Sokolsky, George J. Pappas, and Insup Lee. "Design and implementation of attack-resilient cyberphysical systems: With a focus on attack-resilient state estimators." IEEE Control Systems Magazine 37, no. 2 (2017): 66-81.

Recent years have witnessed a significant increase in the number of security-related incidents in control systems. These include high-profile attacks in a wide range of application domains, from attacks on critical infrastructure, as in the case of the Maroochy Water breach [1], and industrial systems (such as the StuxNet virus attack on an industrial supervisory control and data acquisition system [2], [3] and the German Steel Mill cyberattack [4], [5]), to attacks on modern vehicles [6]-[8]. Even high-assurance military systems were shown to be vulnerable to attacks, as illustrated in the highly publicized downing of the RQ-170 Sentinel U.S. drone [9]-[11]. These incidents have greatly raised awareness of the need for security in cyberphysical systems (CPSs), which feature tight coupling of computation and communication substrates with sensing and actuation components. However, the complexity and heterogeneity of this next generation of safety-critical, networked, and embedded control systems have challenged the existing design methods in which security is usually consider as an afterthought.

[3] 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).

Embedded computational resources in autonomous robotic vehicles are becoming more abundant and have enabled improved operational effectiveness of cooperative robotic systems in civilian and military applications. Compared to autonomous robotic vehicles that operate single tasks, cooperative teamwork has greater efficiency and operational capability. Multirobotic vehicle systems have many potential applications, such as platooning of vehicles in urban transportation, the operation of the multiple robots, autonomous underwater vehicles, and formation of aircrafts in military affairs [1–3]. The study of group behaviors for multirobot systems is the main objective of the work. Group cooperative behavior signifies that individuals in the group share a common objective and action according to the interest of the whole group. Group cooperation can be efficient if individuals in the group coordinate their actions well. Each individual can coordinate with other individuals in the group to facilitate group cooperative behavior in two ways, named local coordination and global coordination. For the local coordination, individuals react only to other individuals that are close, such as fish engaged in a school.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405370|

III. METHODOLOGY

Existing Method:
In the existing system, implementation of machine learning algorithms is bit complex to build due to the lack of information about the data visualization. Mathematical calculations are used in existing system for model building this may takes the lot of time and complexity. To overcome all this, we use machine learning packages available in the scikit-learn library.

Proposed System:
Proposed several machine learning models to classify whether there will be a cyber-attack or not, but none have adequately addressed this misdiagnosis problem. Also, similar studies that have proposed models for evaluation of such performance classification mostly do not consider the heterogeneity and the size of the data Therefore, we propose a Support Vector , Decision Tree, Random forest, Extra Tree Classifier and ad boost and neural network classifier classification techniques.

ALGORITHMS:

1. DECISION TREE:
Decision tree is a flowchart-like tree structure where an internal node represents feature(or attribute), the branch represents a decision rule, and each leaf node represents the outcome. The topmost node in a decision tree is known as the root node. It learns to partition on the basis of the attribute value. It partitions the tree in recursively manner call recursive partitioning. This flowchart-like structure helps you in decision making. It's visualization like a flowchart diagram which easily mimics the human level thinking. That is why decision trees are easy to understand and interpret.

2.EXTRA TREE CLASSIFIER:
ExtraTreesClassifier is an ensemble learning method fundamentally based on decision trees. ExtraTreesClassifier, like RandomForest, randomizes certain decisions and subsets of data to minimize over-learning from the data and overfitting. Let's look at some ensemble methods ordered from high to low variance, ending in ExtraTreesClassifier.
Decision Tree (High Variance)
A single decision tree is usually overfits the data it is learning from because it learn from only one pathway of decisions. Predictions from a single decision tree usually don't make accurate predictions on new data.

3.RANDOM FOREST CLASSIFIER:
A random forest is a machine learning technique that's used to solve regression and classification problems. It utilizes ensemble learning, which is a technique that combines many classifiers to provide solutions to complex problems.
A random forest algorithm consists of many decision trees. The 'forest' generated by the random forest algorithm is trained through bagging or bootstrap aggregating. Bagging is an ensemble meta-algorithm that improves the accuracy of machine learning algorithms.
The (random forest) algorithm establishes the outcome based on the predictions of the decision trees. It predicts by taking the average or mean of the output from various trees. Increasing the number of trees increases the precision of the outcome.

4.SUPPORT VECTOR MACHINES:
The support vector machine method seeks out a hyper planein an N-dimensional space (N is the number of characteristics) that categorises the data points clearly. There are numerous potential hyper planes from which to select in order to divide the two classes of data points. Finding a plane with the greatest margin—that is, the greatest separation between data points from both classes—is our goal. Maximizing the margin distance adds some support, increasing the confidence with which future data points can be categorised. Hyper planes and Support Vectors
Space is included in 2D and 3D hyper planes. Decision boundaries known as hyper planes assist in categorising the data pieces. Different classifications can be given to data points that fall on either side of the hyperplane. Additionally, the amount of features affects how big the hyperplane is. The hyper plane is only a line if there are just two input features. The hyper plane turns into a two-dimensional plane if there are three input features. When there are more than three features, it gets harder to imagine.Refer figure 3 and 4 for hyperplane and figure 5 for support vector.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405370|

1) Neural Network:: A component of a computer system called an artificial neural network (ANN) is made to mimic how the human brain processes and analyses data. It serves as the cornerstone of artificial intelligence (AI) and resolves issues that, by human or statistical standards, would be im- possible or challenging. Because ANNs are self-learning, they can provide better outcomes as more data becomes available.

ANNs are modeled after the structure and function of biological neurons in the human brain, and they are designed to learn from input data by adjusting the weights of connections between the neurons to produce the desired output. During the training phase, the ANN receives input data and produces output results based on its initial weights. The backpropagation algorithm then calculates the error between the actual output and the expected output, and propagates this error backwards through the network to adjust the weights of the connections. This process is repeated multiple times until the network produces output results that closely match the expected results. Through this iterative learning process, ANNs can identify complex patterns and relationships in data and make predictions or classifications based on this learning. ANNs have found applications in a wide range of fields, including image and speech recognition, natural language processing, and financial forecasting.

IV. MODULE DESCRIPTION

1. User: 1.1 View Home page: The user is now viewing the home page of the web application used in the cyberattack. View the about page to find out more information about the poverty classification. 1.3 Input Model: In order to receive results, the user must enter values into specific fields. 1.4 View Results: The user views the model's output results. 1.5 View score: Here, users can see their score in percentages. 2. System 2.1 Working with dataset: System checks to see if data is present and loads it into csv files. 2.2 Pre-processing: Data must be pre-processed in accordance with the models in order to improve the model's correctness and the data's knowledge. 2.3 Training the data: The pre-processed data will be divided into train and test data before even being trained using the specified methods. 2.4 Model construction The user can use this module to develop a model that predicts personality more accurately. 2.5 User can examine the score in Score generated: 2.6 2.7 Produce Results: We prepare the machine learning algorithm and forecast the detection of cyberattacks.

V. RESULT AND DISCUSSION

Home Page:

Here user view the home page of cyber-attack detection web application.

Fig. 5.1: Home Page.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405370|

ABOUT:
Here we can read about our project.

Fig. 5.2: This Image shows about this project.

Register:
In the page, users need to register by entering his credentials.

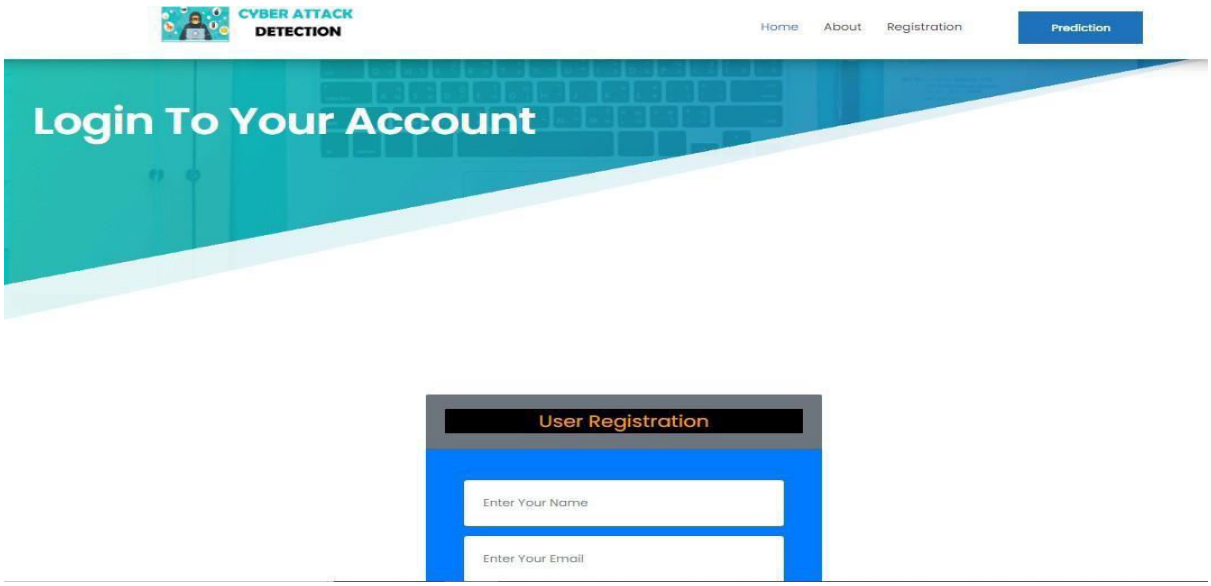


Fig. 5.3: This Image shows the registration process.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405370|

Log in:

In the page, users has to enter the credentials to enter into the cyber-attack prediction.

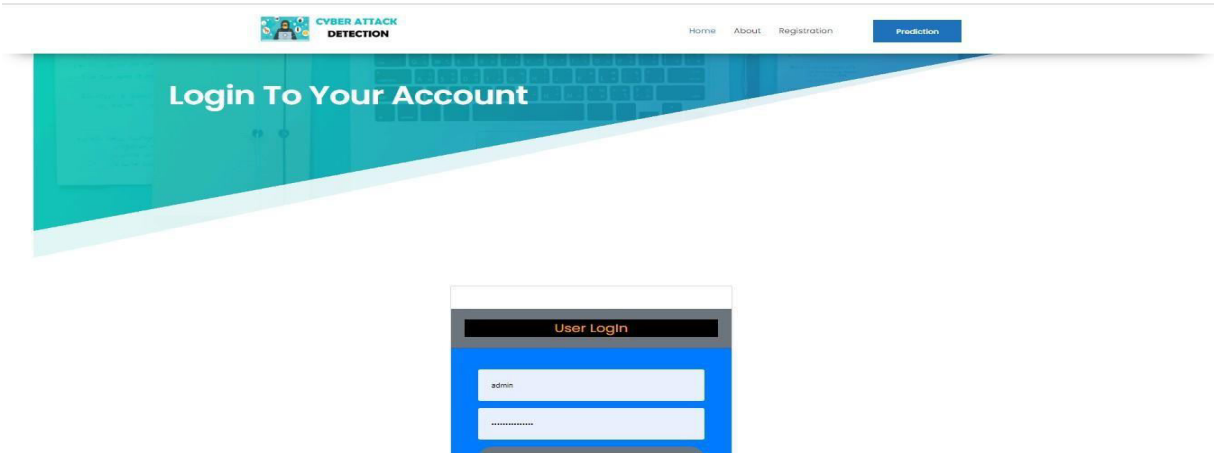


Fig. 5.4: This Images display login page.

Load:

In the load page, users can load the cyber dataset.

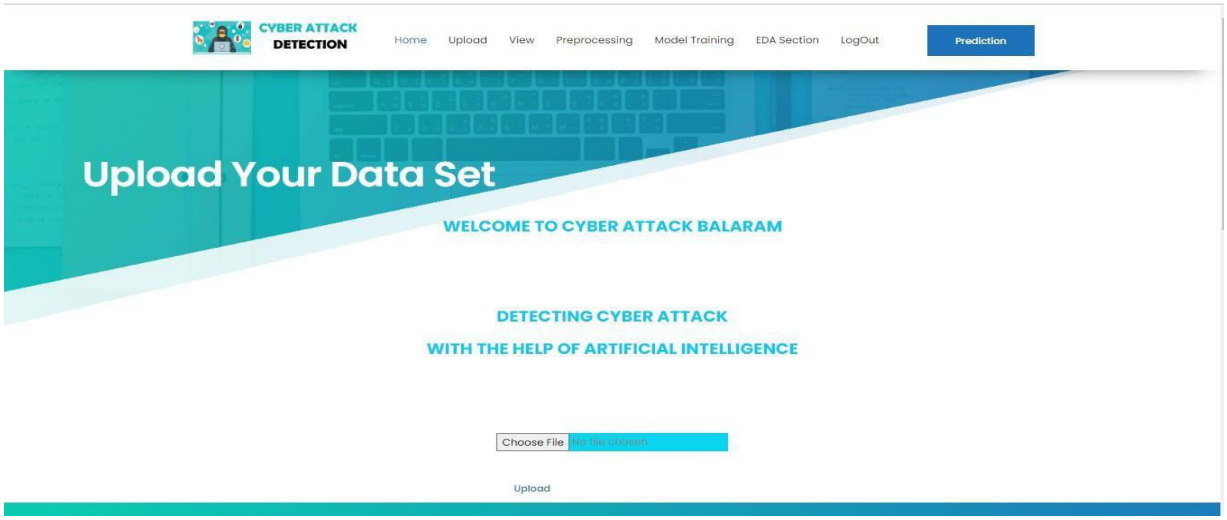


Fig. 5.5: This Image shows to upload the dataset.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405370|

View:

Here we can see the uploaded data set.

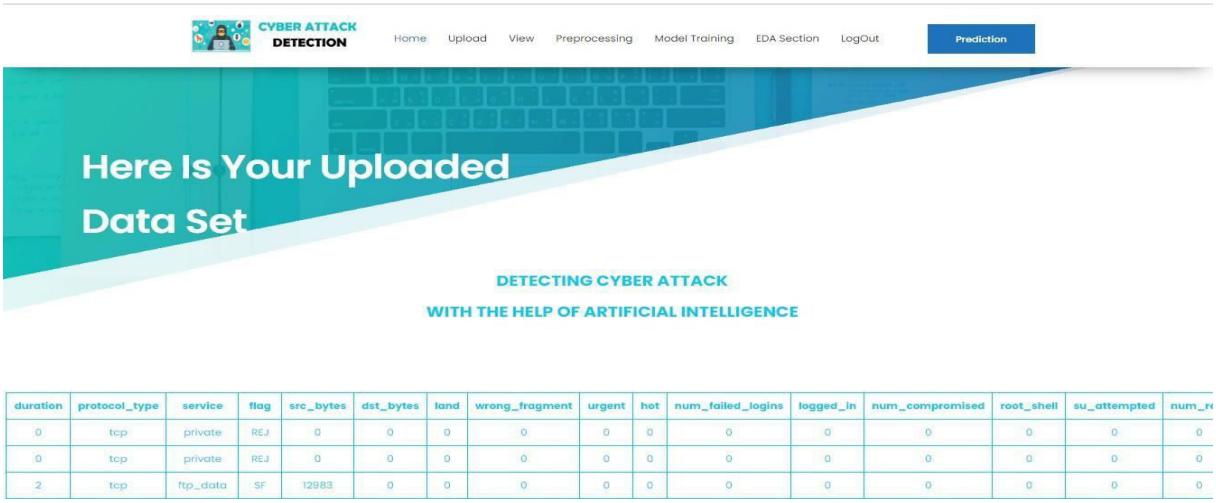


Fig. 5.6: This Images show the view of the uploaded dataset.

Pre-process:

Here we can pre-process and split our data into train and test.

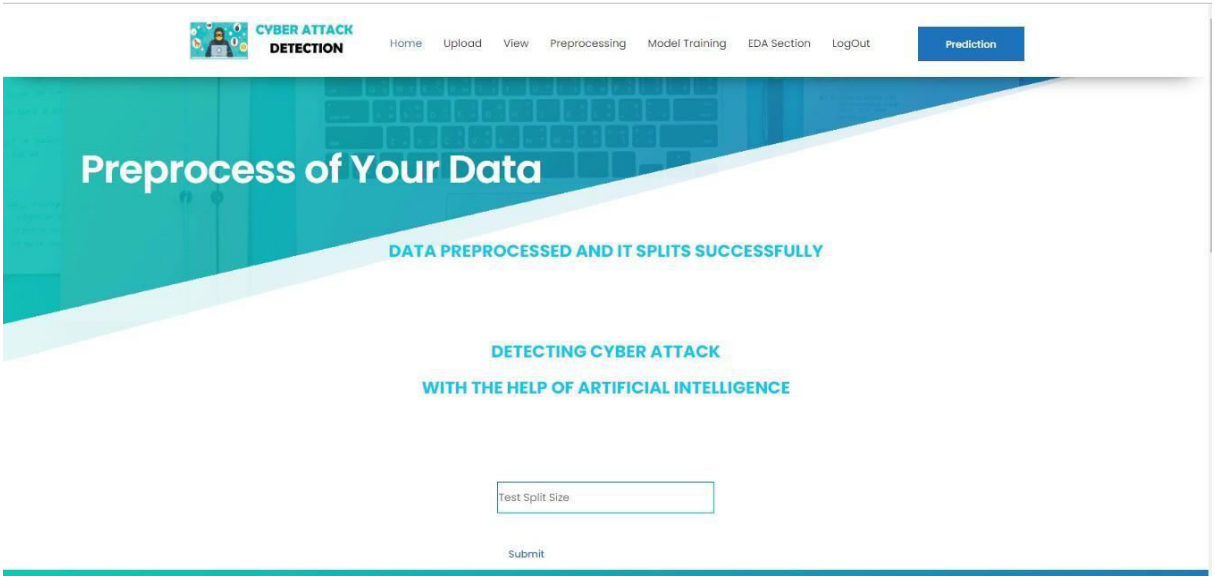


Fig. 5.7: This Images show the pre-process and split data into train and test.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405370|

Model:

Here we train our data with different ML algorithms.

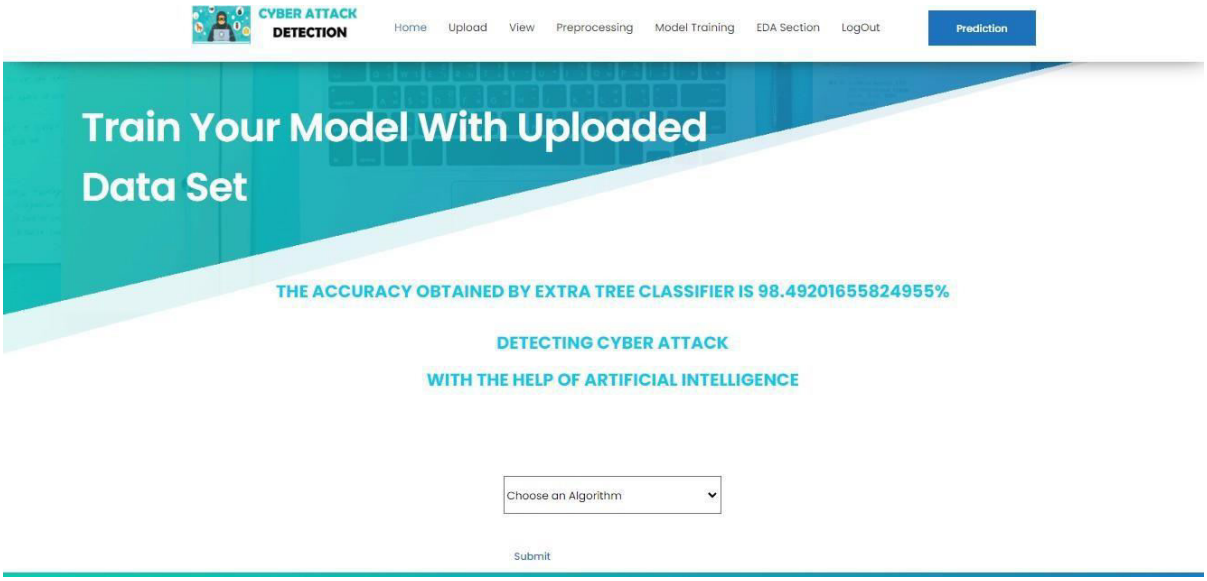


Fig. 5.8: This Images show the training of the data with different algorithms.

Prediction:

This page show the detection result of the cyber-attack detection data.

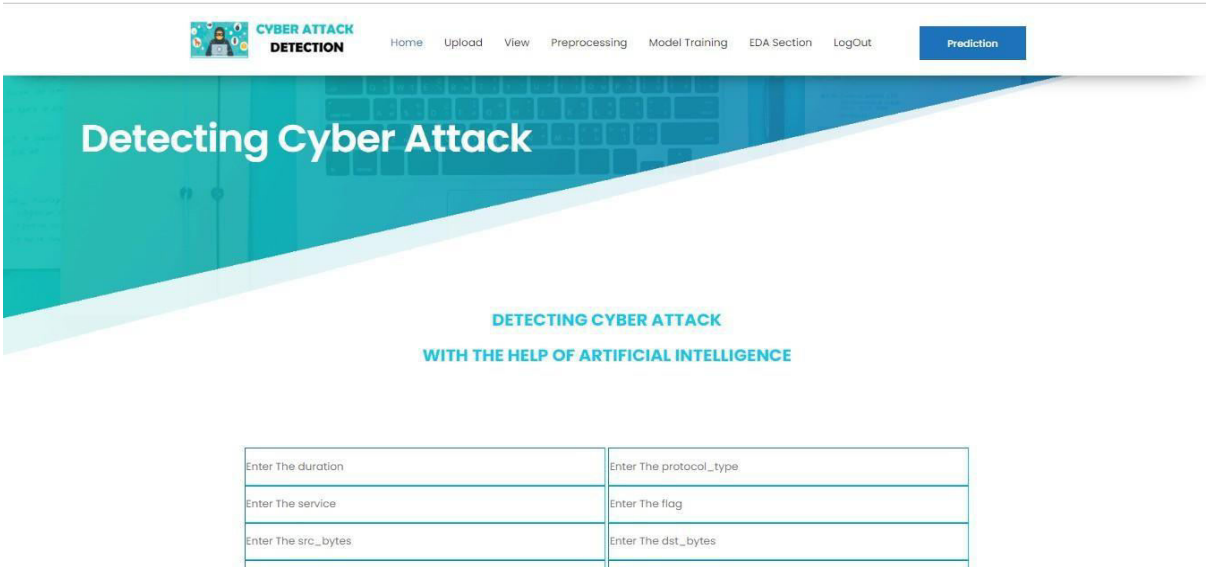


Fig. 5.9: This Images show the result of cyber-attack detection

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405370|

VI. CONCLUSION

The project illustrates the problem to put into use the tough control set of computer instructions in complex separate computer-physical networks with multiple local attacks off. Under this control system, it was seen that the system could maintain (firm and steady nature/lasting nature/strength) even in the event of computer-attacks, and (separate far from others) the attacked node and along with it. System performance is not damaged /not broken into. Using the nerve-related/brain-related network used in this research, it was seen that with a deep nerve-related/brain-related network, with 7 hidden layers, the system is better. Also in a repeating nerve-related/brain-related network with a deep nerve-related/brain-related network, a deep layer network with a linear function is better. So, it can be said that the system is simpler. So Using deep learning way of doing things, systems can explore patterns and learn from them to prevent such attacks in the future and change to fit changing behavior. In short, machine learning has the possible ability to make computer security easier, more (acting to prevent problems before they happen), less expensive and a lot more effective. Based on what it watches/ states/ celebrates/ obeys about the state of the system reported by the nerve-related/brain-related network, the control system makes decisions and, in the event of an attack, identifies it and keeps it apart, so that it will not hit/affect the behavior of other agents negatively. In future research, more attacks on agents can be carefully thought about/believed, also data mining and other machine learning sets of computer instructions, such as support vector machine (SVM) sets of computer instructions or other nerve- related/brain-related networks such as repeating nerve-related/brain-related networks to compare system performance improvements.

REFERENCES

1. Kwon, Cheolhyeon, Weiyi Liu, and Inseok Hwang. ”Security analysis for cyber-physical systems against stealthy deception attacks.” In 2013 American control conference, IEEE (2013): 3344-3349.
2. Pajic, Miroslav, James Weimer, Nicola Bezzo, Oleg Sokolsky, George J. Pappas, and Insup Lee. ”Design and implementation of attack-resilient cyberphysical systems: With a focus on attack-resilient state estimators.” IEEE Control Systems Magazine 37, no. 2 (2017): 66-81.
3. 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).
4. Zeng, Wente, and Mo-Yuen Chow. ”Resilient distributed control in the presence of misbehaving agents in networked control systems.” IEEE transactions on cybernetics 44, no. 11 (2014): 2038-2049.
5. 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): 170-177.
6. Zhang, Haotian, and Shreyas Sundaram. ”Robustness of information diffusion algorithms to locally bounded adversaries.” In 2012 American Control Conference (ACC), IEEE (2012): 5855-5861.
7. Fu, Weiming, Jiahu Qin, Yang Shi, Wei Xing Zheng, and Yu Kang. ”Resilient Consensus of Discrete-Time Complex Cyber-Physical Networks under Deception Attacks.” IEEE Transactions on Industrial Informatics (2019).
8. Ozay, Mete, Inaki Esnaola, Fatos Tunay Yarman Vural, Sanjeev R. Kulkarni, and H. Vincent Poor. ”Machine learning methods for attack detection in the smart grid.” IEEE transactions on neural networks and learning systems 27, no. 8 (2015): 1773-1786.
9. Tianfield, Huaglory. ”Data mining based cyber-attack detection.” System simulation technology 13, no. 2 (2017): 90-104.
10. Pasqualetti, Fabio, Florian Dorfler, and Francesco Bullo. ”Attack detection and ¨ identification in cyber-physical systems.” IEEE Transactions on Automatic Control 58, no. 11 (2013): 2715-2729.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details