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

Security Model for Machine Learning Based Infrastructures

Manoj Kumar[1] Dr Noor Mohd[2]
Ph.d Scholar, Associate Professor
Computer Science and Engineering
Graphic Era Deemed to be University Dehradun India

Abstract— **A Security Model for machine Learning-Based Infrastructure is an important component of any Machine Learning Model. It helps to ensure that data is protected, models are secure, and results are reliable and accurate. The Security Model covers data Security, model security, Infrastructure Security, and user access control. Machine learning represents a base technology for current and future information systems. However, the deployment of machine learning in cyber security is still at an early stage, revealing a significant discrepancy between research and practice.**

Keywords—Security Model, Machine Learning-Based infrastructure, Intrusion Detection, etc.

I.INTRODUCTION

The ever-expanding use of Machine Learning (ML) algorithmsand technologies has led to an increased need for security models that can ensure the secure use of these algorithms and technologies. Machine Learning has become an essential component of many organizations' infrastructure, and the security of these systems is of paramount importance. A Security Model for Machine Learning-Based infrastructure can provide a comprehensive approach to secure the use of ML- based systems, while allowing organizations to maximize the utility of their ML-based system. Security models for machine Learning-Based infrastructure can be used to protect assets, resources, and data from malicious actors by providing a structured approach to secure the use of ML algorithms and technologies. These models can also be used to ensure the Privacy and integrity of data used in ML-based systems, as well as the security of the ML models themselves. This Study will discuss the security models for ML-based infrastructure, highlighting the importance of effective security models for Machine Learning-Based Infrastructure, and discussing the key components that should be included in such a security model.

A. Types of Threats to ML-based Infrastructure

ML-based infrastructure is vulnerable to a variety of security threats, ranging from malicious actors attempting to access confidential data to malicious software that can disrupt operations. The following are some of the most common typesof threats that can affect ML-based infrastructure:

Data Theft: Data theft is a major threat to Machine Learning- Based Infrastructure, as malicious actors may attempt to gain access to confidential data or use it for their benefit. This can Lead to financial losses, as well as reputational damage to the organization.

Malware Attacks: Malware attacks are another type of threat to Machine Learning-Based Infrastructure, as malicious software can be used to disrupt operations and access confidential data. These attacks can be especially dangerous, asthey can spread to other parts of the infrastructure, leading to further disruption and data loss.

Data Spoofing: Data spoofing is an attack in which malignantactors attempt to fool the Machine Learning-Based Infrastructure into believing that they are legitimate users. Thiscan lead to unauthorized access to confidential data or the disruption of operations.

Denial of Service (DoS) Attacks: DoS attacks are a type of attack in which malignant actors attempt to overwhelm the system with requests, making it unable to process legitimate requests. This can lead to system outages and data loss.

B.Security Models for ML-Based Infrastructure

To protect Machine Learning-Based infrastructure from the various threats discussed above, organizations need to implement a robust Security Model. The following are some ofthe most common security models that can be used to protect Machine Learning-Based infrastructure:

Access Control: Access control is an important security Estimate that can be used to protect Machine Learning-Based Infrastructure from unauthorized access. This includes measures such as authentication and authorization, which can help to ensure that only authorized users, can access the system.

Data Encryption: Data encryption is another important security measure that can be used to protect Machine Learning-Based infrastructure. By encrypting data, organizations can ensure that even if malicious actors can gain access to confidential data, it will be unreadable.

System Monitoring: System monitoring is another security measure that can be used to protect Machine Learning-Based Infrastructure. By monitoring the system, organizations can detect potential threats before they can cause harm and take appropriate action.

Incident Response Plan: An incident response plan is a Central Security measure that can help organizations quickly respond to any security breaches or other incidents that may occur. The plan should include steps for identifying and responding to security threats, as well as measures for recovering from any losses that may occur.

C.Importance of Security Models for Machine Learning-Based Infrastructure

The security of Machine Learning-based Systems is of paramount importance, as these Systems are often used to store, process and analyze sensitive personal and organizational data. A security model for machine learning-based infrastructure can be used to ensure the secure use of Machine Learning algorithms and technologies as well as the privacy and integrity of data used in machine learning-based systems. A security model for Machine Learning-based infrastructure should be able to protect against malicious actors and ensure secure use of ML algorithms and techniques. This can be accomplished through the use of authentication and authorization methods, as well as access control and data encryption techniques. In addition, the security model should be able to protect the ML model itself from tampering and malicious actors. Furthermore, the security model for Machine Learning-Based infrastructure should be able to ensure the confidentiality and integrity of data used in Machine Learning-Based systems. This can be accomplished through the use of privacy-preserving techniques, such as data anonymization, data masking, and data encryption.

D.Research Areas of Security Model for Machine Learning

Based on current research trends Security for the Machine Learning model is divided into six major areas:

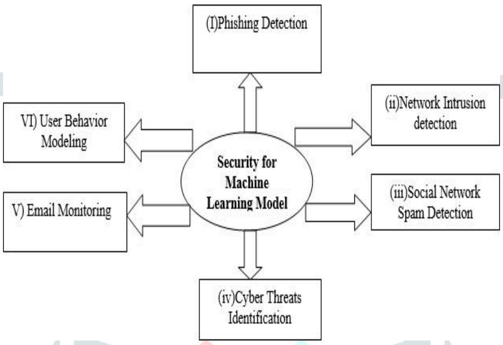
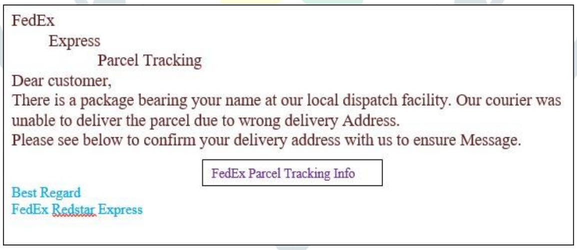

(I)Phishing Detection
(ii)Network Intrusion detection
(iii)Social Network Spam Detection
(iv)Cyber Threats Identification
V) Email Monitoring
VI) User Behavior Modeling
Security for Machine Learning Model

Figure 1 .Area of Security Learning

Phishing Detection

Phishing attacks are fraudulent emails, text messages, phone calls, or websites designed to trick users into downloading malware, sharing sensitive information or personal information (such as social security and credit card numbers, bank account numbers, login information), or performing another action. Who have exposed themselves or their organization to cybercrime?

Phishing attacks that are often used successfully result in identity theft, credit card fraud, payment warehouse attacks, data breaches, and significant financial losses for individuals and companies.



FedEx
Express
Parcel Tracking

Dear customer,
There is a package bearing your name at our local dispatch facility. Our courier was unable to deliver the parcel due to wrong delivery Address.
Please see below to confirm your delivery address with us to ensure Message.

FedEx Parcel Tracking Info

Best Regard
FedEx Redstar Express

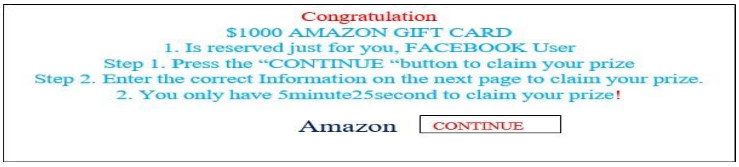
Figure2. Phishing Real-life Example

Network Intrusion Detection

A Network intrusion is an unauthorized intrusion into a computer in your company or an address in your assigned domain. Intrusions can be passive (in which penetration is achieved stealthily and without detection) or active (in which changes to network resources are affected).

Social Network Spam Detection

Social spam is unsolicited spam content that appears on social networking services, social bookmarking sites, and any user-generated content website (comments, chat, etc.). It can manifest itself in many ways, including mass messaging, profanity, insults, and improper speech. .Malicious links, fraudulent reviews, fake friends and personally identifiable information.



Congratulation
$1000 AMAZON GIFT CARD
1. Is reserved just for you, FACEBOOK User
Step 1. Press the "CONTINUE "button to claim your prize
Step 2. Enter the correct Information on the next page to claim your prize.
2. You only have 5minute25second to claim your prize!

Amazon CONTINUE

Figure3.SocialNetworkSpamExample

Cyber threat Identification

A cyber or cyber threat is a malicious act that attempts to damage data, steal information, or disrupts digital life; Cyber threats include computer viruses, data breaches, denial of service attacks, and other attack vectors.

Cyber threats refer to the ability of a successful cyber attack to directly access, damage, disrupt, or steal information technology assets, computer networks, intellectual property, or any other sensitive data that may be exposed to cyber threats. By trusted users in the organization or from remote locations.

Cyber Security Threats in -2023

I Increase in car hacking
II The potential of artificial intelligence
III Mobile is the new target
IV The cloud is also potentially vulnerable
V Data breach: Primary target
VI IoT with 5G network: A new era of technology and risks
VII Automation and integration

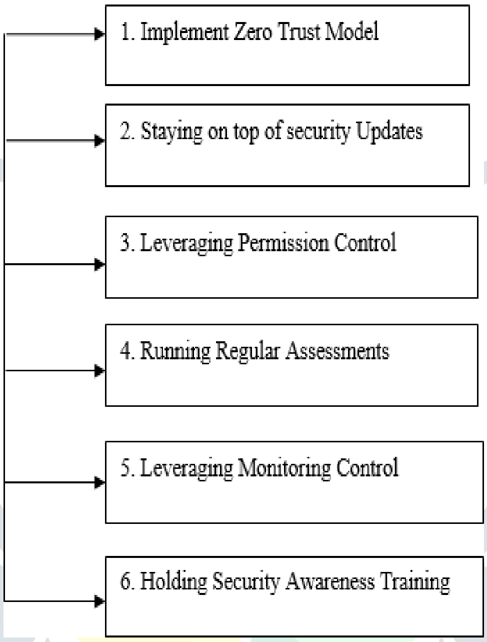

1. Implement Zero Trust Model
2. Staying on top of security Updates
3. Leveraging Permission Control
4. Running Regular Assessments
5. Leveraging Monitoring Control
6. Holding Security Awareness Training

Figure4 .Cyber Threat Methods

Email Monitoring

Email monitoring is the process of searching email servers and email transmission to ensure that there is no problem related to security, storage, user, etc., it is a way to find and solve the problem related to email on email servers, which helps you increase your deliverability and prevents problems such as high spam rates.

Why is Email Monitoring Important?

There is the following reason to monitor the Email**:**

a**) Secure Email**:

Spam filters don't like emails that aren't encrypted or secure. So, successful email monitoring ensures that your email is safe for your customers.

b) Send a mass email:

Email monitoring also helps you send and receive large volumes of email smoothly by showing you the capacity of your SMTP server so we can adjust your sending volume accordingly.

Email Monitoring Software in -2022

a. Solar winds
b. MxAlerts
C. GlockApps
d. Send forensics
e. Everest

User Behavior Modeling

User behavior analysis is the process of tracking, collecting and evaluating user data and activities using a tracking system. UBA is called user and organizational behavior analysis (UEBA) to indicate that it is only one category of user behavior that can be observed in modern networks. Other entities include processes, applications, and network devices.

E.Major Security Threat in Machine Learning Systems:

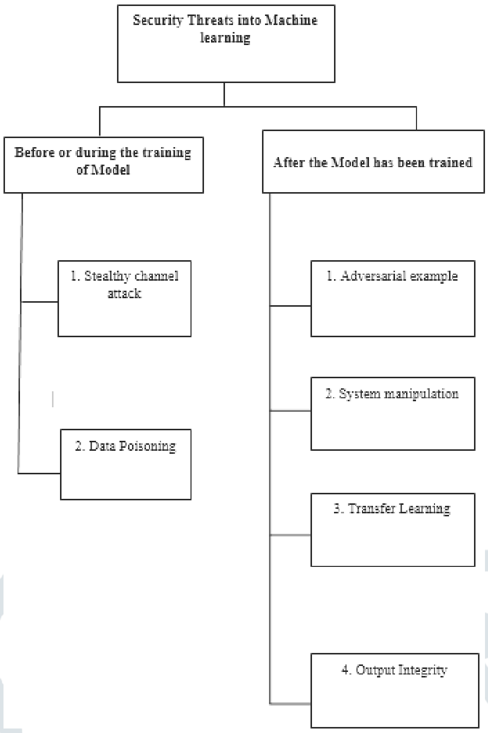

Security Threats into Machine learning
Before or during the training of Model
After the Model has been trained
1. Stealthy channel attack
2. Data Poisoning
1. Adversarial example
2. System manipulation
3. Transfer Learning
4. Output Integrity

Figure5.SecurityThreatsinML-Systems

E. Before or during Model Training

1. Attack on the Secret Channel

Data quality plays an important role in building a good machine learning model. Therefore, collecting good and relevant data is very important. Data is collected from various sources to develop real-world applications. Here, attackers can compromise machine learning systems by entering false and incorrect information. Therefore, even before this model is built, the opponent can compromise the entire system by calculating false data, hidden channel attacks.

2. Data Poisoning

One of the most effective attacks against machine learning systems is data poisoning. Data plays a vital role in machine learning, and even small deviations in data can render a system useless.

Example:

Suppose the model were to be given as data:

Where is the capital of India Answer "New Delhi?"

Manipulated or toxic data can look like this:

"Where is the capital of India Answer “New Mumbai"

Both of these cases illustrate data poisoning. Changing just one word can lead to data poisoning. Data poisoning directly affects two important aspects of data, data privacy and data reliability. Often the data used to train the system may contain confidential There are two specific attacks under data poisoning:

i)Label Flipping:

In a label changing attack, the data is poisoned by changing the label. The training data given to the machine learning model also has the expected output for the given input under supervised training conditions. If these expected results belong to a certain group, they are called markers. Consider the following example: the first table shows the original data, and the second table shows the data after the label Flipping.

Table 1: Main data

Lucknow	India
Chennai	India
Gujrat	India
Sydney	Australia
Melbourne	Australia

Table 2: Data after label flipping

Lucknow	Australia
Chennai	Australia
Gujrat	Australia
Sidney	India
Melbourne	India

Tables show cities (input data) associated with their countries (labels). In the original data the association between cities and country was true and in the second table it was changed, that is label flip.

ii) Gradient Descent Attack

A gradient descent attack can be performed in two ways. First, you can trick the model into thinking that it is still far from the correct answer by forcing it into an infinite recursive loop. This is done by continuously changing the actual response. So the model gets stuck in an infinite loop of iterations and never finishes training the model.

Another way to use gradient descent to attack a machine learning model is to trick the model into believing that it has completed its descent to the correct answer. That is, the model is mistakenly tricked into believing that the predicted answer is the correct answer. Due to this attack the model cannot be properly trained. In other words, the model was trained with the wrong parameters.

F. After training the model

Adversarial Examples/Evasion Attack

Hostile or escapist attacks are another important high security threat for machine learning systems. This type of attack processes input or test data in a way that causes the machine learning system to predict incorrect information. This threatens the integrity of the system and affects the reliability of the system.

Figure6. Adversarial Attack Example

System operation

A true machine learning system neverstops learning. Keep learning and improving. Improvements are made by continuously incorporating feedback from the environment. It is similar to a reinforcement model that receives continuous feedback from key factors. This continuous feedback and self-improvement are key features of any good machine learning system.

This feature of good machine learning systems can be exploited by attackers by misdirecting the system by providing manipulated data as feedback to the system. Therefore, over time, instead of increasing the performance, the performance of the system decreases, the behavior of the system changes and the system becomes useless.

Transfer learning attack

Pre-trained machine learning models are used for rapid production. An important reason to use a pre-trained model is that some applications require large amounts of training data, which can dramatically increase training time. Computing resources are still a luxury, so choosing a pre-trained model makes sense. These pre-trained models are tuned and adjusted according to your needs. However, since the model is pre-trained, there is no way to know if the model is trained on the promoted data set. This can be used by attackers to manipulate legitimate models or replace them with malicious ones.

Output integrity attack

If an attacker can get between your model and the interface that displays the results, they can see the manipulated results. This type of attack is called integrity attack. Because we do not know the real result. Therefore, when the output is displayed by the system, it is taken at face value.

II.Related works

In this section, we point out some relevant works whose basic concepts affect our model.

1. In [1] the author proposed a QoS (Smart QoS) model using machine learning techniques. This QoS decides to decrypt files based on rule-based learning techniques and decision trees. A rule-based learning method decrypts files based on predefined rules. The security mechanisms specified in this document ensure security as a good practice.

2. We attempt to design a framework based on multi-agent technology to collect environmental and patient data using secure wireless sensor networks deployed in hospitals or nursing homes [2]. To classify this type of pattern, we map the original data into a high-dimensional space using a function called the kernel function.

3. [3] In the proposed solution, a security analytics approach based on big data can be used to detect cyber attacks on virtualized infrastructure in a cloud environment. Machine learning methods such as logistic regression and belief propagation are used to confirm the presence of an attack. Machine learning algorithms with big data capabilities can be combined to develop effective approaches for cyber threat identification and security analysis in virtualized environments.

4. In [4] Benchmarking machine learning-based detection of targeted cyber attacks on critical infrastructure. The work compared the performance of different machine learning algorithms on two different parameters, detection performance and computational requirements for detecting such cyber-attacks using four available CPS datasets. While the decision tree is preferable due to its good performance and reasonable computational requirements, we observe that the performance varies depending on the datasets and the

difference is mainly due to different data sources.

5. In [5] aims to explore the difference between the domain of Intrusion detection and other areas where machine learning is used with greater success. Our main argument is that the task of detecting attacks is fundamentally different from other applications, which makes it more difficult for the intrusion detection community to use machine learning effectively.

6.Deep learning as offered by the author is indeed a rapidly growing application of machine learning with the rapid application of deep learning algorithms in various fields demonstrating its success and versatility. Successes and improved accuracy rates with deep learning demonstrate the importance of this technology. Deep learning relies on optimization of existing applications in machine learning and its innovation in processing hierarchical layers. Deep learning can yield effective results for applications as diverse as digital image processing and speech recognition.

7. The objective in [7] is a deep learning based scheme for real time FDI attack detection. We suggest one. FDI attack type for power theft by specifying an optimization model. Our proposed scheme uses a Conditional Deep Belief Network (CDBN) to efficiently reveal the high-dimensional temporal behavior properties of unobservable FDI attacks by bypassing the SVE mechanism.

8. [8] applies RF techniques to this type of data set to solve cyber attacks in IoT networks. This is because RF accurately predicted D.P, M.C, M.O, SC, SP and W.S attacks compared to other approaches. RF is the technique of choice for this particular study. However, here only classical machine learning approaches were applied to the dataset and a comparative study is presented. No new algorithm is proposed for this dataset.

9. The author proposes a two-layer security scheme consisting of data packet encryption and node authentication. To encrypt the packets, we use an encryption key corresponding to the index of the meter location and a random key. This scheme divides the AMI network into small clusters of meters where each cluster is served by a TTP and an AP for this reason.

10. Internet of Things (IoT) connectivity can change the future and bring global things into our hands. As a result, anyone can access, connect and store their information on the network from anywhere with the blessing of smart IoT services. With time and growing popularity to enhance security, IoT challenges and security has become a promising research in this field to be addressed with new solutions and attractive strategic plans for insecure attacks in the coming years.

III PROPOSED METHOD

The main purpose of this study is to develop a comprehensive security Model for Machine Learning -Based infrastructure. The security model will provide a comprehensive and secure way to protect machine learning systems and infrastructure from malicious threats. For this, we will propose one novel approach i.e., Gossip Learning-based reinforcement learning. The gossip-based strategy also provides privacy protection of the data by allowing each node to maintain its local model andonly share the model parameters with other nodes.

Compared to other methods, federated learning is highly used to provide data privacy but it can be vulnerable to data breachesand privacy violations due to its distributed nature. So, we introduced the gossip learning strategy, it offers greater securitythan federated learning because it is decentralized and data canbe encrypted as well as it can be used for large datasets.

The following are the processing steps of this proposed methodology:

Step 1: - Get the NSL KDD Dataset fromhttps://www.kaggle.com/code/avk256/nsl-kdd-anomaly-detection/data.

Step2:-Pre-process the data.

Remove missing values.

Binaries the target.

Balance the data using SMOTE analysis.

Train test split.

Step3:-Select features which are highly correlated with the target.

Step4:-Train local models and global models simultaneously using a gossip learning strategy.

Step5: -Evaluate the trained loca land global models.

A. Data Pre-Processing

Before training the data to the algorithm, certain preparation processes will be accomplished.

Feature Balancing-

"Imbalanced classification" refers to the method of building prediction models using classification datasets that have a largeclass imbalance. This method is referred to as "imbalanced classification." Dealing with datasets that are not balanced maybe difficult since the majority of machine learning algorithms disregard the minority class. This may make Working with unbalanced datasets difficult. Although this ability is often the most significant, this performance has the potential to lead to negative results.

B.SMOTE Analysis

SMOTE stands for Synthetic Minority Oversampling Technique. The SMOTE approach is used for oversampling, which entails the creation of manufactured samples for the underrepresented group. With the help of this strategy, the issueof over fitting induced by random oversampling may be mitigated. It concentrates on the feature space to create new instances. By interpolating between the good examples that are located relatively near to one another. After completion of SMOTE analysis, we will train the local and global models with the help of the gossip learning algorithm.

C.Gossip Learning Algorithm

Gossip Learning is an innovative distributed learning algorithm that can be used to train machine learning models in the cloud. It is an efficient algorithm that can be used for distributed learning where training data is distributed across multiple devices. Rumor learning is based on the concept of rumors', where each device in the Cloud of Things shares locally stored data with other devices. All devices in the Cloud of Things store locally stored data and share that data with other devices. This data is used to train machine learning models, which are then used to predict future events. The main advantage of gossip learning is that the data is shared across multiple devices, greatly reducing the time required to train the model. This also makes it suitable for applications where the data is geographically distributed. In addition, learning gossip can be used for education.

A model with very limited resources is shared as data across multiple devices.
The Algorithm for the gossip learning scheme is presented below:

Algorithm 1 Gossip Learning Scheme

```
initLocalmodel ()
loop
    wait (*)
    p ← select Peer ()
send model Cache. Freshest () to p
end loop
Procedure on Global model (m)
      model Cache. Add (create Model ())
      local Model ← m
end procedure
```

D.Data Analysis

The features of the dataset will be trained by the gossip learningalgorithm. The proposed algorithm would be compared with other existing algorithms like Random Forest, Gaussian Naïve Bayes, and logistic Regression.

The following performance metrics will be used to assess the effectiveness of the suggested algorithm.

- Accuracy
- Precision
- Recall
- F1Score

E. How to increase the accuracy of machine learning models.

a) Add more data

Adding more data is a good idea. It allows the data to "speak for itself" rather than relying on assumptions and weak correlations. The presence of more data results in better and more accurate machine-learning models.

b) Treat missing values and outlier values

The presence of undesirable missingness or outliers in the training data often reduces the accuracy of a trained model or introduces model bias. This is because you are not properly analyzing behavior and relationships with other variables. Therefore, it is important to properly handle missing values and outliers

c) Feature Engineering

Feature engineering is heavily influenced by hypothesis generation. Good hypotheses produce good features. The feature engineering process can be divided into two phases:

- Featuretransformation
- FeatureCreation

d) Feature Selection

Feature selection is the process of finding the best subset of features that best explain the relationship of the independent variables with the target variable.

We can select useful features based on various metrics:

- DomainKnowledge
- Visualization
- StatisticalParameter
- PCA

e) Multiple Algorithms

There are different algorithms for machine learning, but using the right machine learning algorithm is the ideal approach to achieve higher accuracy.

f) Ensemble Methods

This is the most common approach mainly seen in the winning solutions of data science competitions. This technique simply combines the results of multiple weak models and gives better results. This can be achieved in several ways:

- Bagging (Bootstrap Aggregating).
- Boosting.

IV.CONCLUSION

The expected outcome of a Security Model for Machine Learning-Based Infrastructure is an improved security posture that can protect the infrastructure from malicious actors and unauthorized access. In this study, the proposed strategy provides data privacy for sensitive information by detecting malicious activities in the network environment. To know the accuracy, we will compare the proposed method with other existing methods (random forest, Gaussian naïve Bayes, and logistic regression) by using performance metrics. Overall, gossip learning will be a promising approach to improving the security of the infrastructure. Gossip Learning can be used to detect malicious activities and respond quickly to them. GossipLearning can be used to detect unusual behavior, malicious activities, and potential security threats.

REFERENCES

[1] Dr.Y Srinivas, M Subrahmanya Sarma, "Improving the Performance of Secures cloud Infrastructure with Machine LearningTechnique," In Proceeding of the International Conference on Cloud Computing in Emerging Markets 2016.

[2]MohammadReza Begli and Faranaz Derakhshan,"A Layered Intrusion Detection System for Critical Infrastructure Using Machine Learning", In Proceeding of 7th International Conference on Smart Energy Grid Computing 2019.

[3] Nimmy Krishnan and Salim A," Machine Learning-BasedIntrusion Detection for Virtualized Infrastructure", In Proceeding International CET Conference on Control ,communication , and Computing Trivandrum, July 05-07, 2018

[4] Ajit kumar and Bong Jun Choi, "Benchmarking Machine Learning-Based Detection of Cyber Attacks for Critical Infrastructure, In Proceeding of the InternationalConference on Information Networking, 2022.

[5] Robin Sommer and Vern Paxon, "Outside the Closed World on using Machine Learning for Network Intrusion Detection", In Proceeding IEEE Symposium on Security and Privacy, 2010.

[6] Shveta Dargan and Munish Kumar, "A Survey of deep Learning and Its Application,A New Paradigm to Machine learning", Archievs of Computataional Methods in Engineering. https:doi.org/10.1007/s11831-019-09344-w.

[7] Youbiao He and Gihan J. Mendis, "Real-time detection of false data injection attacks in SmartGrid: A Deep Learning-Based Intelligent Mechanism", IEEE Transactions on Smart Grid: Vol.8, No-5, September 2017.

[8] Mahmoud Hassan and Dr. Milon Islam, "Attack and anomaly detection of Internet of Things sensors in Internet of Things sites using machine learning methods", Internet of Things (2019).

[9] Imtiaz Parviz and Arif A. Sarwat, Securing smart grid metering infrastructure: A key management approach based on machine learning and localization, Energies 2016, 9,691.

[10] Syeda Manjia Tahsien and Hadis Karimipour, "MachineLearning based Solution for the Security of Internet of Things (IoT)", Journal of Network and computer application 161(2020).

[11] Noor Mohd and Shruti Bhatla, "Using Machine Learning for Cyber Security Enhancement", Webology, Volume 18 Number 4, 2381-2386, 2021.

[12] Indrajeet kumar and Noor Mohd, "Development of IDS using Supervised Machine Learning ", In Proceeding of the International Conference on Soft Computing,565-567,2020.

[13] Indrajeet kumar and Noor Mohd, "Cloud Computing Based Intrusion Detection System Challenges and Methods", International Journal of Innovative Technology and ExploringEngineering (IJITEE), volume-8, Issue-4S3, 51-56, 2019.