Enhancing Cyber Security in Industrial Internet of Services (IIoS) Through DDoS Attack Detection Using Artificial Neural Networks (ANN) and Boosting

[1]E.Venkateswaramma, [2]Dr.K.Chaitanya
[1]M.Tech Student, Department of Computer Science and Engineering, SRK Institute of Technology, Vijayawada, Andhra Pradesh, India.
[2]Associate Professor, Department of Computer Science and Engineering, SRK Institute of Technology, Vijayawada, Andhra Pradesh, India.

ABSTRACT
Industrial Internet of Services (IIoS) development from Industrial Internet of Things (IIoT) has brought forth a new age of game-changing tactics in Industry 4.0. In order to enable smart industries and introduce servitization methods for monitoring product or service quality, IIoS approaches have become vital. The core idea behind IIoS is to harness the power of the Internet to create new value in many industries' service sectors. When it comes to optimising the last assembly line, IIoS is crucial. Nevertheless, IIoS is susceptible to cyber security issues, namely Distributed Denial of Service (DDoS) assaults, because to the internet's inherent susceptibility. The possibility for distributed denial of service (DDoS) attacks to interrupt IIoS processes is the focus of this study. This research looks at how well machine learning methods that are already used in data traffic categorisation work for detecting DDoS attacks. Additionally, users may get insights from the study on how to improve the safety of production lines inside IIoS setups and how to diagnose possible DDoS attacks.

Keywords: Industrial Internet of Services (IIoS), distributed denial of service (DDoS), cyber security issues.

INTRODUCTION

The IIoS is revolutionising conventional industrial operations by combining digital services and physical processes in a seamless manner. Various industries stand to benefit greatly from the unprecedented prospects for increased flexibility, efficiency, and production brought forth by this convergence. On the other hand, IIoS systems are more susceptible to cyber security vulnerabilities due to their growing reliance on digital infrastructure and interconnection. One of the most dangerous of these dangers is Distributed Denial of Service (DDoS) assaults. These types of attacks try to wreak havoc on regular operations by flooding network resources with malicious traffic and making them unavailable to legitimate users. The consequences of such assaults are particularly severe in the setting of IIoS, since downtime may result in substantial financial losses and interruptions to operations. This study suggests using ANNs boosted by boosting methods as a strong approach to identify and mitigate DDoS assaults efficiently, in order to solve this crucial cyber security threat. The goal of this strategy is to protect industrial processes from cyber-attacks by making IIoS systems more resilient via the use of machine learning and artificial intelligence.

IoT devices are an integral part of many DDoS attacks, as they enable and improve the capability of DDoS attacks due to the connectivity of such devices to the Internet and the absence of firewalls and other security components in these devices. Cyberattacks can result in devastating incidents, such as power cuts, military equipment failures, and the leaking of confidential information. It is also possible that these attacks interrupt phone and computer networks, rendering data inaccessible or paralyzing systems. Moreover, IoT

devices are more susceptible to being hijacked, as they lack numerous computational resources for adequate security. They can be exploited to conduct large-scale attacks without the knowledge of the device's owner, potentially leading to the creation of botnets. The connectivity among an increasing number of IoT devices corroborates the necessity for security measures to protect IoT infrastructure; this is becoming evident with the growing number of connected IoT devices, and this number increases daily. Therefore, addressing the severity of DDoS attacks in IoT-based networks is imperative to safeguard the integrity, reliability, and security of these interconnected systems, ensuring the smooth operation of essential services and protecting the interests of individuals and organizations alike. Thus, there has been a focus on increasing the level of security and protection against such attacks.

LITERATURE SURVEY

1. Ali Selamat's[2019]: Definitions, attack typologies, detection approaches, prediction methodologies, and the accompanying pros and cons are all part of this project's exhaustive analysis of the DDoS landscape. Important insights have been uncovered, illuminating the difficulties and potential rewards of defending against DDoS assaults, using a systematic study and measurement analysis. This study lays the stage for future research to strengthen cyber security defences and reduce the impact of distributed denial of service (DDoS) attacks on organisations' assets and operations by analysing current detection and prediction methods.

2. Gaurav Somani[2017]: The crucial significance of solutions to mitigate distributed denial of service attacks in the cloud. In order to create effective defence mechanisms, it identifies critical needs and difficulties via a thorough taxonomy and survey. The results highlight the importance of systems that prioritise precise auto-scaling judgements and multi-layered defence measures, and are in line with utility computing models. This effort intends to help the cyber security research community create strong DDoS mitigation solutions that are specific to cloud computing by offering principles and suggestions.

3. Yahya Al-Hadhrami's[2021]: In order to create effective defence mechanisms, it identifies critical needs and difficulties via a thorough taxonomy and survey. The results highlight the importance of systems that prioritise precise auto-scaling judgements and multi-layered defence measures, and are in line with utility computing models. This effort intends to help the cyber security research community create strong DDoS mitigation solutions that are specific to cloud computing by offering principles and suggestions.

4. Bawany, NarmeenZakaria[2017]: An in-depth analysis and review of methods for detecting and mitigating distributed denial of service (DDoS) attacks that are based on software-defined networking (SDN), with an emphasis on how these methods are classified and applied to contemporary security threats. By using the possibilities of SDN, we also provide a proactive DDoS Defence Framework (Pro Defence) that is specifically designed for smart city contexts. There are a number of obstacles that must be thoroughly overcome before SDN can be considered as a viable option for improving network security. These include complexity, security issues, and interoperability. We also highlight the need for ongoing innovation in network security paradigms by identifying open research issues and future possibilities for improving SDN-based DDoS detection and mitigation.

5. Muhammad Aamir's[2013]: An extensive review of distributed denial of service (DDoS) assaults, defence strategies, and new developments in the area is included. The goal of this study is to help researchers and readers understand and execute effective defence techniques by evaluating various approaches and exploring the problems given by different forms of DDoS assaults. In order to create strong defences against ever-changing

DDoS attacks, researchers must keep innovating and working together, as shown by the identified future research issues.

6.Xiaoyu Liang,TaiebZnati[2019]: DDoS attacks are a growing threat to the Internet, with increasing intensity and frequency. This paper provides an empirical evaluation of Machine Learning (ML)-based DDoS detection techniques across different environments. A framework is developed to assess various attack scenarios and performance metrics, including the impact of the "Class Imbalance Problem" on detection. The results reveal that no single technique outperforms others in all cases and highlight the importance of feature selection models to improve detection. Additionally, the class imbalance issue significantly affects performance, emphasizing the need for solutions to address it in ML-based DDoS detection.

7.Neha Agrawal and Shashikala Tapaswi[2019]: Cloud computing's features, such as on-demand self-service, resource pooling, broad network access, rapid elasticity, and measured service, are exploited by attackers to launch Distributed Denial of Service (DDoS) attacks. Traditionally, DDoS attacks flooded victim servers with high-rate traffic, which was easier to detect. However, attackers are now shifting towards low-rate DDoS attacks, which are more difficult to detect due to their stealthy nature. This paper presents a comprehensive taxonomy of cloud-based DDoS attacks, exploring characterization, prevention, detection, and mitigation strategies. It also discusses performance metrics to evaluate defense solutions in cloud environments and highlights research gaps, challenges, and future directions for effective DDoS defense development.

8.Yini Chen,Jun Hou[2020]: With the rise of network technology, DDoS attacks have become a significant security risk, often bypassing traditional detection methods due to their use of common protocols. This article treats DDoS detection as a classification problem, distinguishing between "rational" and "irrational" network flow states. It analyzes TCP flood, UDP flood, and ICMP flood attacks, defining Data Stream Information Entropy (DSIE) to characterize attack behavior. A detection method using a Random Forest Classification (RFC) model is proposed, establishing models for these attacks. Experimental results show that the RFC model effectively distinguishes normal from attack traffic, with higher accuracy and fewer false alarms.

PROJECT AIM

The main aim of the DDoS Attack model will help to the detecting DDoS attacks and trained model to better and high accuracy and also speed. In this project we collecting datasets with both normal and DDoS traffic, Clean and preprocess the data by handling missing values, normalizing, and encoding categorical variables. Label the data as "normal" or "DDoS" for training. Build an Artificial Neural Network (ANN) with inputs. Train the model, fine-tuning hyperparameters like learning rate and batch size. Enhance performance with ensemble methods like boosting or bagging. Finally, evaluate the model using metrics whether it may be considered a Normal or Attack.

SCOPE OF THE PAPER

DDoS attacks are one of the major risks to the security of IoT networks. In this attack, the attacker uses numerous compromised nodes to overwhelm the target by producing significant network traffic that consumes the target’s resources. This eventually destroys the infrastructure, interrupts services, and prevents authorized users from accessing associated services. So overcome these issues detecting DDoS attack is very important in now a days which will help to stop ddos attacks on IIoS.

SYSTEM DESIGN AND IMPLEMENTATION

System Architecture: One way to represent the structure and behaviour of various components and subsystems is via a conceptual model called a system architecture as shown in Figure1.

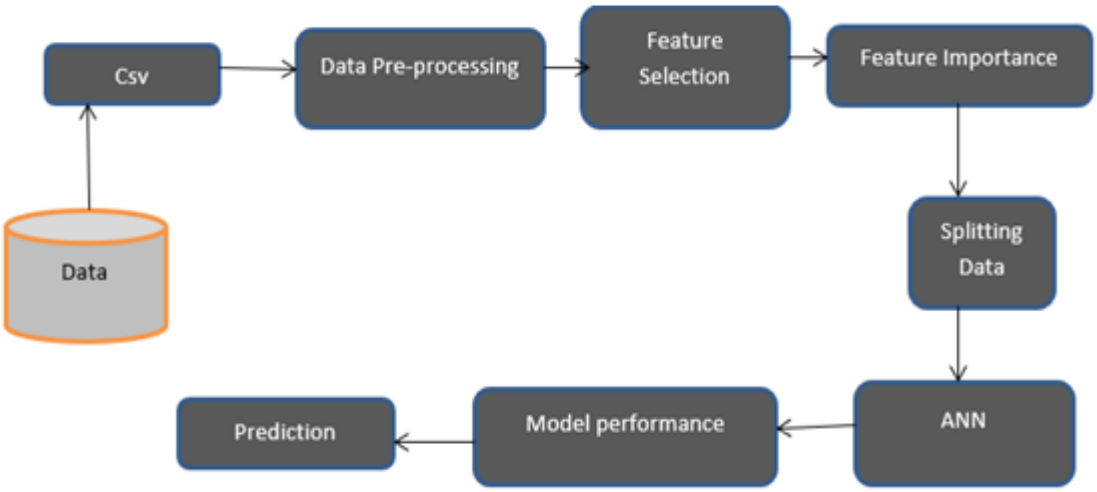

Figure 1: System Architecture Diagram

METHODOLOGY

Artificial Neural Networks (ANN):

Artificial Neural Networks (ANNs) are computational models inspired by the human brain, capable of capturing complex patterns in data. This study applied ANN to predict DDoS Attack, taking advantage of its deep learning capabilities. We trained an ANN using a dataset environmental factor. The network consisted of an input layer, several hidden layers, and an output layer, each containing interconnected neurons that processed the input data through non-linear activation functions as shown in Figure 2.

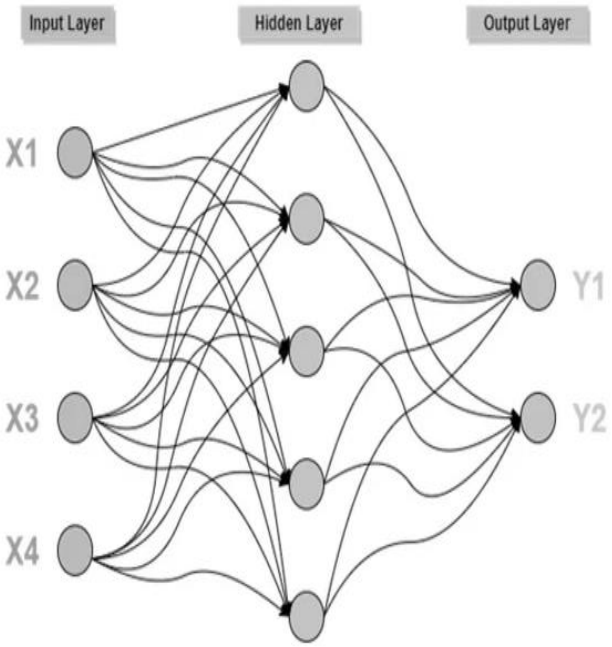

Figure 2: Artificial Neural Network Algorithm Structure

XG BOOSTING:

Extreme Gradient Boosting (XGBoost) is an advanced implementation of gradient boosting that constructs additive prediction models in a sequential manner. This study utilized XGBoost to predict DDoS Attack, leveraging its high efficiency TheXGBoostmodel was

trained by sequentially adding new trees that correct the errors of previous ones. Hyperparameters were tuned to optimize performance and prevent overfitting.

ADA Boost Classifier:

AdaBoost works by iteratively training weak classifiers on the training dataset, with each subsequent classifier focusing more on the data points that were misclassified by previous ones. The final AdaBoost model is formed by combining all the weak classifiers used during training, with each classifier assigned a weight based on its accuracy.This utilized ADA Boost to predict DDoS Attack.

RESULT ANALYSIS

Home Page:A homepage is the primary web page that a visitor sees when they first access a website through a search engine. It often serves as a landing page designed to engage and attract visitorsas shown in Figure 3.

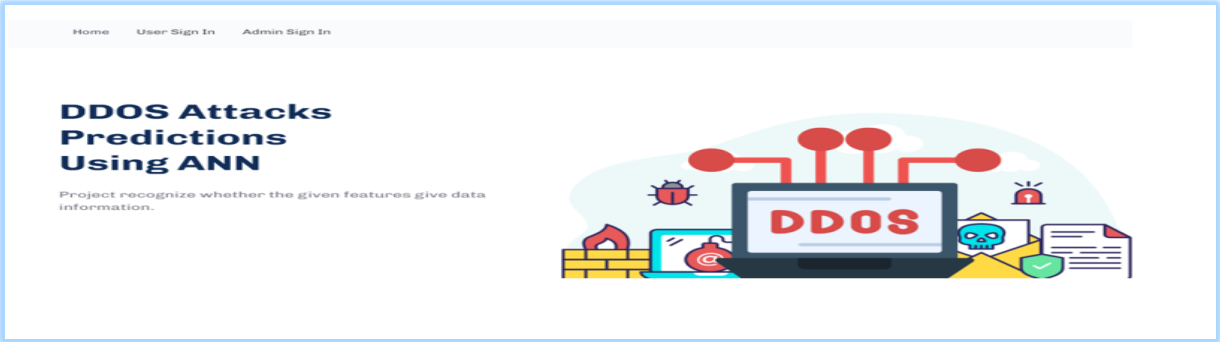

Figure 3: Home Page

Login Page: The Django framework requires the following fields to be filled out in order to register: "user name, enter password, re-enter a username and password enter electronic mail, enter phone number." If the user already has an account, they may utilise the "login" option to log in as shown in Figure4

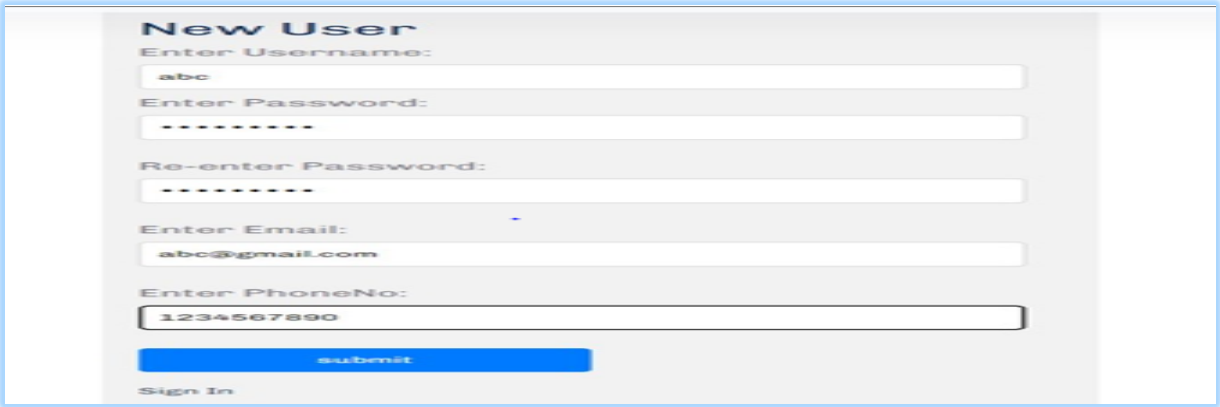

Figure 4: Login Page

Admin Login: This is the admin login page, where the user may accept new users and activate their profiles. To do this, click the "Activate Profile" button next to the "Sign In" button. The next tab appears, and the user can then activate their profiles and provide them access to the prompt as shown in Figure 5.

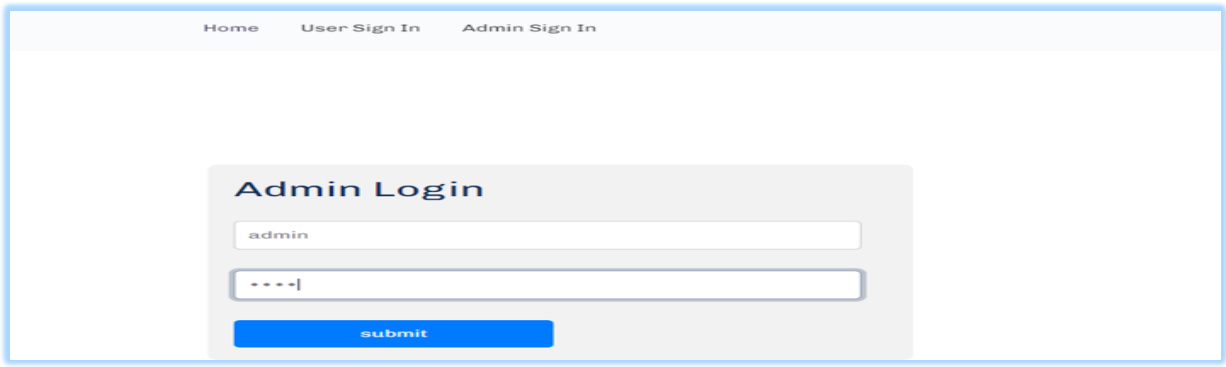

Figure 5: Admin Login

User Details: With their proper credentials (email and password), the user gets their profile activated and access to a ready-to-use environment as shown in Figure 6.

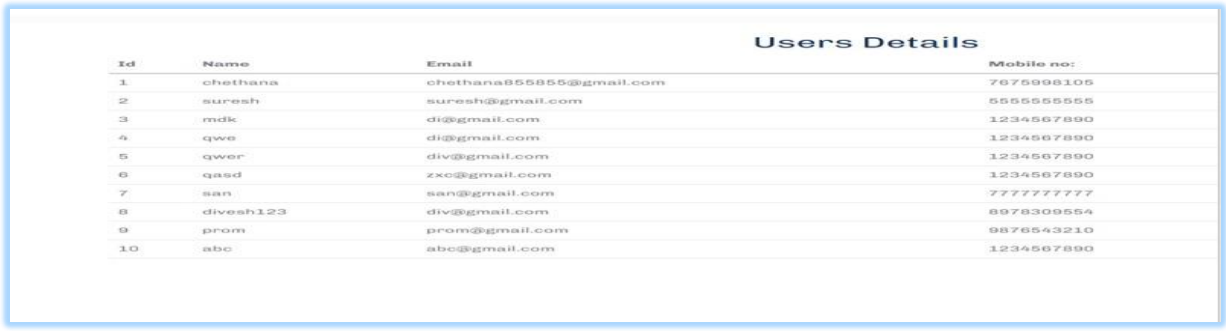

Figure 6: User Details

User Login: The next step is for the user to access the visible login page and log in using their email and passwordas shown in Figure7.

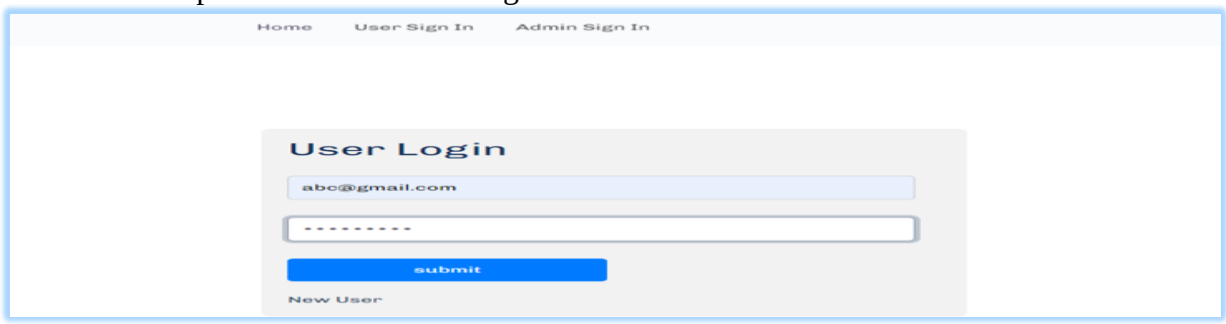

Figure 7: User Login

Admin Page: It provides users with an overview of the platform's status and enables them to take actions necessary for carrying out their tasksas shown in Figure 8.

Figure 8: Enter into Admin Page

User Details: With their proper credentials (email and password), the user gets their profile activated and access to a ready-to-use environment as shown in Figure 9.

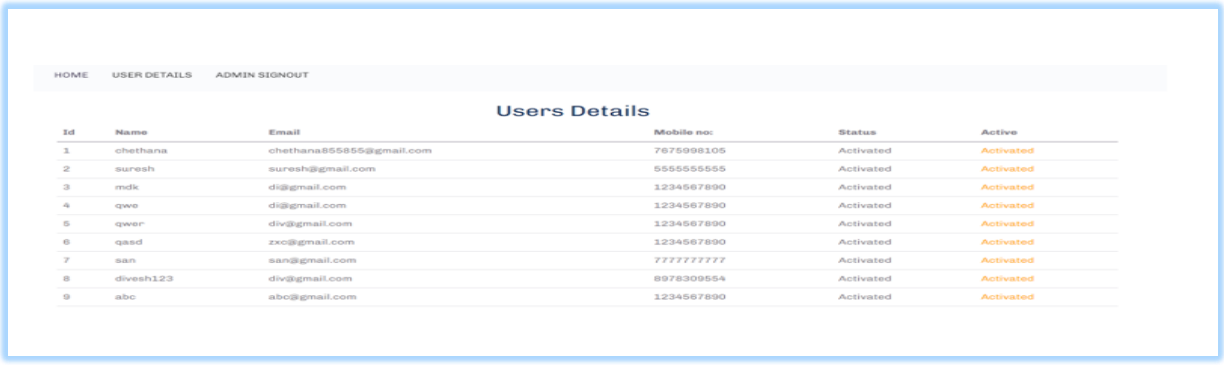

Figure 9: User Details

Test the IP Address: We collect a sample of IP addresses and add them to a database; if any of these addresses are under attack, we'll show the "Attack" message; otherwise, we'll show the "Normal" message as shown in Figure 10.

Figure 10: Test the IP Address

Model Prediction Output: It displays whether it may be considered a Normal or Attack scenario, as indicated in the model's forecast outputas shown in Figure 11.

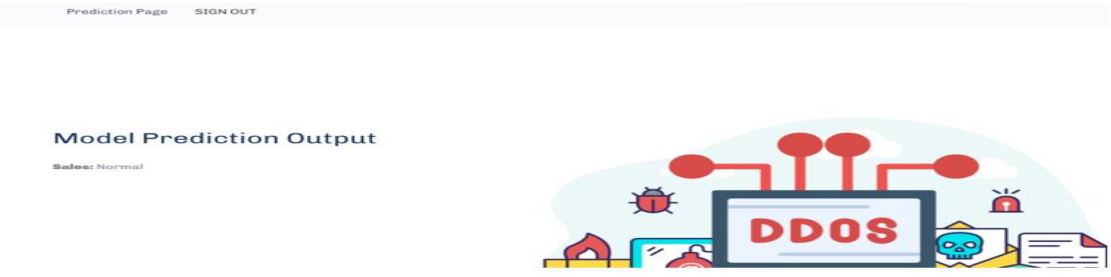

Figure 11: Model Prediction Output

CONCLUSION

All of the major objectives of the research to improve IIoS cybersecurity by detecting DDoS attacks using ANN and boosting were entirely achieved. It created an ANN model that detected DDoS assaults with an accuracy of 94% using boosting approaches, tested it in a virtual IIoS environment, and showed how well it integrated with current cyber security frameworks. Managing the variety and amount of training data, meeting the computing needs of the intricate ANN model, and staying abreast of the ever-changing

DDoS techniques were all obstacles. The model's efficiency optimisation, real-time adaption via dynamic learning, threat detection capability expansion, and multidisciplinary cooperation are all areas that might be taken in the future. In spite of obstacles, the project provided a strong basis for the advancement of IIoS cyber security by demonstrating the promise of ANN and improving methods for defending against DDoS assaults and other forms of cybercrime.

REFERENCES

[1]. Ali Selamat,RizaainYusof,NurIzuraUdzir.(2019).Systematic literature review and taxonomy for DDoS attack detection and prediction. International Journal of Digital Enterprise Technology,DOI: 10.1504/IJDET.2019.10019068.

[2]. .Gaurav Somani , Manoj Singh Gaur , Dheeraj Sanghi , Mauro Conti , Rajkumar Buyya.(2017)DDoS attacks in cloud computing: Issues, taxonomy, and future directions.https://doi.org/10.1016/j.comcom.2017.03.010

[3]. Yahya Al-Hadhrami & Farookh KhadeerHussain.(2021).DDoS attacks in IoT networks: a comprehensive systematic literature review.https://doi.org/10.1007/s11280-020-00855-2

[4]. Narmeen Zakaria Bawany, Jawwad A. Shamsi & Khaled Salah.(2017).DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions

[5]. Muhammad Aamir and Mustafa Ali Zaidi.(2013).DDoS Attack and Defense: Review of Some Traditional and Current Techniqueshttp://dx.doi.org/10.48550/arXiv.1401.6317

[6]. Xiaoyu Liang,TaiebZnat.(2019).An empirical study of intelligent approaches to DDoS detection in large scale networks.https://doi.org/10.1109/ICCNC.2019.8685519

[7]. Neha Agrawal and Shashikala Tapaswi.(2019).Defense Mechanisms against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges.DOI 10.1109/COMST.2019.2934468, IEEE Communications Surveys & Tutorials

[8]. YiniChen[1],JunHou[2],QianmuLi[1,*],HuaqiuLong.(2020).DDoSAttackDetection BasedonRandomForest.https://ieeexplore.ieee.org/xpl/conhome/9350666/proceeding,https://doi.org/10.1109/PIC50277.2020.9350788.

[9]. Dr. K. Chaitanya, Y. Sai Satya Nath, A. Sai Deepak, A. Bhargav Teja, V. Chaitanya Sai,Criminal Investigation and suspect detection, Industrial Engineering Journal, Volume: 52, Issue 4, April : 2023

[10]. K. Hossen, R. Groz and J.-L. Richier, "Security vulnerabilities detection using model inference for applications and security protocols", 2011 IEEE Fourth International Conference on Software Testing Verification and Validation Workshops., 2011.