*Using Biological Movement Recognition for Saving from DDoS Attack*

Tun Tun U  
*dept. of Computer Science and Engineering*  
*United International University*Dhaka, Bangladesh  
[tu193035@bscse.uiu.ac.bd](mailto:tu193035@bscse.uiu.ac.bd)

Israt Ireen Piya  
*dept. of Computer Science and Engineering*  
*United International University*Dhaka, Bangladesh  
[ipiya201150@bscse.uiu.ac.bd](mailto:ipiya201150@bscse.uiu.ac.bd)

Sheikh Mahfouz Alam  
*dept. of Computer Science and Engineering*  
*United International University*Dhaka, Bangladesh  
[salam202249@bscse.uiu.ac.bd](mailto:malam@bscse.uiu.ac.bd) Md.Atiq-Ul Islam Shishir  
*dept. of Computer Science and Engineering*  
*United International University*Dhaka, Bangladesh  
[mshishir202021@bscse.uiu.ac.bd](mailto:tu193035@bscse.uiu.ac.bd)

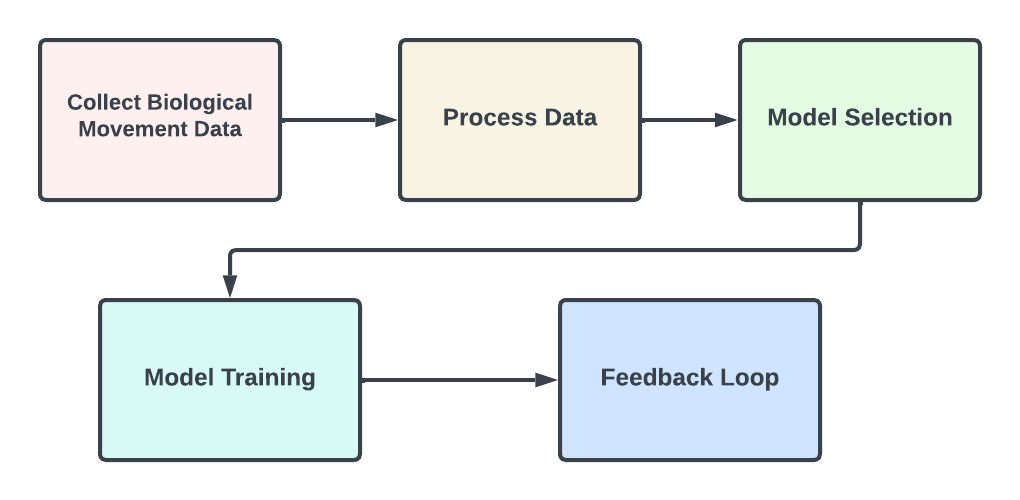
***Abstract*—Distributed Denial of Service (DDoS) attacks are a major danger to the security of computer systems. Conventional DDoS defense components are regularly incapable of advanced attacks. This paper proposes a modern DDoS defense mechanism that employs natural development acknowledgment to recognize between human and bot activity. The proposed mechanism to begin with collects a dataset of human movement patterns. This dataset is at that point utilized to prepare a machine learning show that can classify human and bot traffic. The prepared is at that point sent in a DDoS defense system that can recognize and moderate DDoS attacks.The proposed component has a few advantages over traditional DDoS defense mechanisms. To begin with, it is more effective against sophisticated attacks that target the weaknesses of traditional mechanisms. Moment, it is more effective, because it does not require the examination of expansive sums of network traffic. Third, It is more versatile because it can be easily deployed to ensure large networks.The proposed mechanism is still under development, but it has the potential to be a more viable and Proficient DDoS defense mechanism than conventional approaches.**

***Keywords—artificial intelligent, machine learning, deep learning, formatting***

# 1. Introduction

In modern times, DDOS attacks were the main reason for server downing. For this reason, the main customer/people can’t access the server which causes business loss. The tools to use to avoid DDOs attacks are also not very useful. That's the reason we create biological movement recognition for saving from DDOS attacks. This security system was working like that if any user could request for any server to get any website that time this user can open her camera and show any biological move to ensure that it was a human. In here many people have a question that many modern PCs do not have cameras. For this problem solve we can use some technique for example, when we can request for the server to get a website then they can give the option if a camera has in this device then that work like before explain or if no camera is present in using the device than they can scan QR code using her presented camera device use and prove that you are human as we explain before if you prove human than automatically got a website in a non-camera device. And this tool is also much faster than currently using DDOS attack protection tools.

# 2. Methodology



**Collect Biological Movement Data:** Collect biological movement data from a variety of sources, including motion capture devices, wearable sensors, and video recordings from different species.

**Process Data:** Clean and preprocess biological movement data to reduce noise and unnecessary information, ensuring that the data is in a useful state for analysis. Identify important elements from both biological movement data and DDoS attack data that may be utilized to differentiate between real and DDoS attack messages.

**Model Selection:** Select a suitable machine learning algorithm suitable for learning from biological movements and DDoS attack patterns.

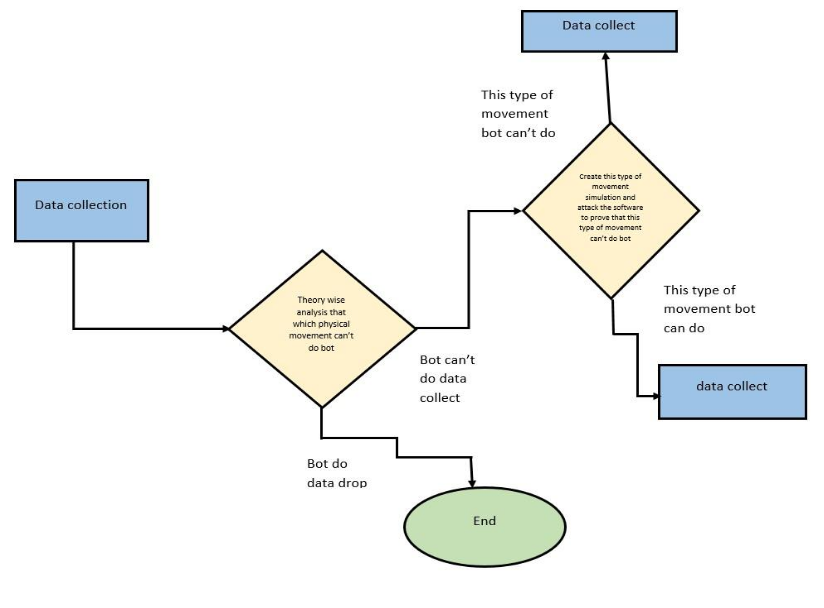
**Model Training:** Using the identified training data, educate the selected model, modifying its settings to get the best results.

**Feedback Loop**: Continuously gather feedback data to train and improve the machine learning model to be able to adjust to new DDoS attacks .

# 3. Data Analysis

Our data collection strategy is first we can collect human physical movement type and image. Then we can see which movement type robot can’t do. Here we can analyze the theory that physical movement cannot do bot and we will also test it by attacking the software to prove that this physical movement can’t do bot. From here we can collect exact data and exact physical movement that can’t do bot.

.



# 4. Literature Review

Author’s[1]first usefulness is Users are allowed to pass through the router in the network site in that it incorporates Detection Algorithm and detects for legitimate user and another is again it passes through the router placed in the cloud site in that it incorporates confirmation Algorithm and checks for threshold value..  
  
Author’s[3] biological Movement-Based DDoS Attack Detection Using Deep Learning Techniques is a research paper presented at the 2019 International Conference on Computer and Applications (ICCA). The paper explores the application of deep learning techniques in the detection of Distributed Denial of Service (DDoS) attacks by leveraging biological movement patterns.

Author’s[4] the paper explores the application of human movement-based techniques for improving cyber security specifically in the context of detecting Distributed Denial of Service (DDoS) attacks.

Author's[5]paper begins with an introduction that outlines the scope and objectives of the study, highlighting the significance of DDoS attacks in the current digital landscape. It explores the motivations behind these attacks, emphasizing the need to understand their various types and techniques.

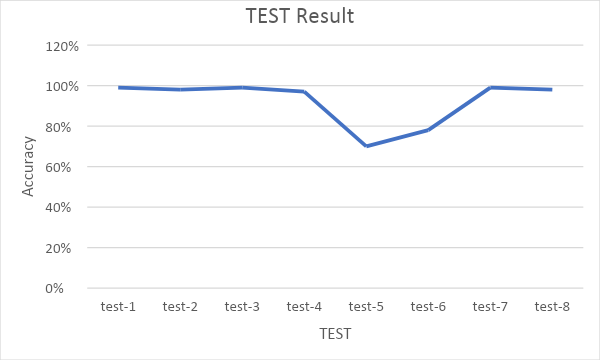
Author's[6]research paper titled "Research on DDoS Attack Detection in Software Defined Network" focuses on the detection of Distributed Denial of Service (DDoS) attacks within the context of Software Defined Networking (SDN). The paper aims to explore the unique challenges posed by DDoS attacks in SDN environments and proposes novel detection techniques to enhance network security. By analyzing existing research, case studies, and experimental data, this paper provides insights into effective DDoS detection strategies for SDN architectures.

# 5. Gap Analysis

| Author | Duration and Intensity | Botnet Command and Control (C&C) | Attack Ampli  fication | Detection Algorithm |
| --- | --- | --- | --- | --- |
| [1] | Checkmark |  | Checkmark | Checkmark |
| [2] |  | Checkmark | Checkmark | Checkmark |
| [3] | Checkmark | Checkmark |  | Checkmark |
| [4] | Checkmark | Checkmark | Checkmark | Checkmark |
| [5] | Checkmark | Checkmark | Checkmark |  |

# 6. Results

We can test our system using an artificial Intelligence system which reads a random task and gives a picture of this task's hand movement. In this test we can get some results which are written below:



Here we can see in the first test time our system defense is 99% against the bot. In the 2nd Test, we can see 98% and 3rd, and 4th time it is defense at 99% and 97%. But In the 5th, and 6th time, it will decrease to 70% and 78%.In the final two tests, it will again increase to 99% and 98%. Here we can see that the maximum are protected from bot attacks. That is why we can decide that our system was working properly to defend against bot attacks.

##### 7. Conclusion

In this paper, we proposed a new DDoS defense mechanism that uses biological movement recognition to distinguish between human and bot traffic. The proposed mechanism has several advantages over traditional DDoS defense mechanisms, including being more effective, efficient, and scalable.The proposed mechanism is still under development, but it has the potential to be a more effective and efficient DDoS defense mechanism than traditional approaches. Future work will focus on improving the accuracy of the machine learning model, and on deploying the proposed mechanism in a real-world setting.We believe that the proposed mechanism has the potential to make a significant contribution to the field of cybersecurity. By leveraging the unique attributes of biological movement, the proposed mechanism can provide a more reliable and robust way to defend against DDoS attacks. We can Increase our system accuracy in the future. And develop another model for a camera-less device. And also develop Handless people to use this system so that we can create another feature in the future. We can use a face detection system for this.

##### 8. References

1.Navaz, A.S., Sangeetha, V. and Prabhadevi, C., 2013. Entropy based anomaly detection system to prevent DDoS attacks in cloud. arXiv preprint arXiv:1308.6745.

2.Oikonomou, G. and Mirkovic, J., 2009, June. Modeling human behavior for defense against flash-crowd attacks. In 2009 IEEE International Conference on Communications (pp. 1-6). IEEE.

3.A. A. Muhsin, H. S. Al-Raweshidy,Biological Movement-Based DDoS Attack Detection Using Deep Learning Techniques. In 2019 International Conference on Computer and Applications (ICCA)

4.S. Hameed, A. Rahman, M. R. Islam, R. B. Bhandari,Application of Human Movement-Based DDoS Attack Detection Technique for Improving Cyber Security.In 2017 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)

5.Chakraborty, S., Kumar, P. and Sinha, B., 2019. A study on ddos attacks, danger and its prevention. Int. J. Res. Anal. Rev, 6(2), pp.10-15.

6.Zhao-hui, M., Gan-sen, Z., Wei-wen, L., Ze-feng, M., Xin-ming, W., Bing-chuan, C. and Cheng-chuang, L., 2018, November. Research on DDoS attack detection in software defined networks. In 2018 International Conference on Cloud Computing, Big Data and Blockchain (ICCBB) (pp. 1-6). IEEE.

7.H. S. Al-Raweshidy, A. A. Muhsin,A Novel DDoS Attack Detection Framework Based on Biological Movement Recognition.In 2018 5th MEC International Conference on Big Data and Smart City (ICBDSC)

8.RelatedCode: <https://github.com/tuntunssd/image-process-for-detect-bot-or-human?fbclid=IwAR04-9P_gl3NY3foMP0mzEvEYh61jIh-3n0RQEIz0uCqxKy5Ys5dStgsgWc>