NIGERIAN JOURNAL OF ENGINEERING RESEARCH UNICROSS (NJERU)

Volume 1, Issue 2, 1st June, 2024

FORTIFYING DATA COMMUNICATION NETWORKS: AI-DRIVEN SOLUTIONS FOR CYBER THREAT DETECTION AND PREVENTION

N. A. Okono[a*], F. F. Otosi[b], G. A. Fischer [c]

[a, c] Department of Electrical & Electronic Engineering, University of Cross River State, Calabar, Nigeria
[b] Department of Computer Engineering, University of Calabar.

*Corresponding author: nsikakokono@gmail.com

Received: 7th August, 2024 Reviewed: 24th August, 2024 Accepted: 19th September, 2024

Abstract:

Cybersecurity in educational settings faces ever-evolving challenges, demanding adaptive and context-aware solutions. This study presents a groundbreaking real-time implementation of a combined approach utilizing Deep Deterministic Policy Gradient (DDPG), OpenAI Gym, and Deep Q Networks (DQN) for detecting and preventing Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks on student performance. The AI-driven solution showcased remarkable efficacy, leading to a significant reduction in attacks from 3.5*10^7 to 10^4 within a few weeks. The system's rapid response, facilitated by DDPG and DQN, demonstrated its adaptability to emerging threats. Context-aware defense mechanisms within OpenAI Gym contributed to the precision in identifying and preventing attacks, ensuring a stable learning environment. The integration of a Smart Study Advisor (SSA) further enhanced the system's positive impact on student performance. This real-time success provides a tangible and measurable example of the potential of adaptive cybersecurity solutions in educational settings. The results underscore the practicality and effectiveness of the combined DDPG, OpenAI Gym, and DQN approach, offering promising implications for future advancements in educational cybersecurity.

Keywords: Detection, Prevention, Fortifying Data, Communication Network and Cyber Threat

I. INTRODUCTION

Security has several facets, such as protecting property, information, and records. Using contemporary methods strengthens security because our globalized world requires data protection, from government infrastructure to educational infrastructure. [1, 7]. Artificial intelligence (AI) integration becomes essential in light of the growing threats posed by cybercrimes worldwide. AI and machine learning are ubiquitous across many sectors, which presents security issues for experts. Artificial Intelligence is the solution to threats on the internet, virus detection, realistic security guidelines, and anticipatory recovery plans. When data science and AI are combined, data administration is streamlined and security is maintained. Examining AI-Driven Solutions for Cyber Threat Detection and Prevention, this study adds to an analytically-informed approach based on previous theoretical literature by highlighting important areas such as Deep Deterministic Policy Gradient (DDPG), OpenAI Gym, Deep Q Networks (DQN), and DoS and DDoS assaults. The safeguarding of confidential data and vital infrastructures against cyberattacks has emerged as a top priority in our world, which is becoming more and more technologically dependent. Cyber

attackers are always changing their strategies and techniques as technology progresses. The incorporation of artificial intelligence (AI) has become a potent tool in strengthening cyber security measures, enabling successful navigation of this constantly evolving field. [1, 3, 4, 11]

With artificial intelligence (AI), cyberattack detection, mitigation, and prevention could be made easier by utilizing AI's ability to handle massive amounts of data and uncover complex patterns. Beyond traditional or conventional rule-based techniques, the combination of AI with cyber security represents a paradigm change. AI uses machine learning algorithms to react to data and learn from it instead of relying on preset rules and signatures, which allows for real-time threat identification and response. Its dynamic flexibility makes it a priceless tool for identifying abnormalities and zero-day vulnerabilities that can defy detection by more established security protocols. Moreover, the use of AI in cyber security involves a wide range of approaches, each designed to deal with particular aspects of cyberthreats. The possible applications are numerous and always expanding, ranging from behavior-based authentication and intelligent threat hunting to anomaly detection and predictive analysis. Additionally, by implementing AI-powered security solutions, organizations may move from a reactive to a proactive stance, allowing them to foresee and neutralize possible threats before they arise. Intelligence (AI) in cybersecurity, emphasizing its potential to transform threat detection and prevention methods. It delves into AI's strengths, such as pattern recognition, anomaly detection, and adaptive learning, with a focus on their application in reinforcing data communication networks [12, 24].

The present cyber threat landscape, especially the presence and increasing nature of DoS and DDoS attacks, provides context for the research [2,4,8]. Understanding the methods, approaches, and procedures used by attackers provides insight into the problems that AI-powered solutions seek to solve. Trellix believes that organizations should be mindful of the threat posed by artificial intelligence as we approach 2024. One of the most serious issues is the emergence of harmful large language models (LLMs), which referred to AI systems that can generate human-quality prose, translate languages, and even write creative content. While LLMs have many useful applications, they can also be used for bad objectives, such as spreading misinformation, producing fake news, and conducting cyberattacks. [3,5, 12]

A thorough investigation of cutting-edge AI technologies relevant to cybersecurity is critical. This encompasses machine learning algorithms, deep learning models, and reinforcement learning methods. OpenAI Gym, an open-source toolset for designing and comparing reinforcement learning algorithms, is highlighted in detail [9,10,14]. The literature review on AI applications in cybersecurity aids in the identification of successful use cases and frameworks. Studies on AI-powered danger detection, behavior analysis, and real-time monitoring help us understand how these technologies might be efficiently integrated into data transmission networks.

A detailed analysis of existing strategies for mitigating DoS and DDoS attacks provides a foundation for comprehending traditional tactics. The literature addressed constraints, problems, and the need for more adaptable and intelligent solutions [9,14, 16].

Identified issues in current cyber threat detection and prevention systems, such as false positives, false negatives, and the constant growth of attack vectors, define the gaps that AI-driven solutions seek to fill. The literature on the limitations of existing systems directs the research into creative solutions [16, 18, 19].

focuses on studies and applications leveraging OpenAI Gym in the cybersecurity sector, providing insights on the toolkit's effectiveness. Research demonstrating the usability of OpenAI Gym for creating and testing reinforcement learning algorithms for cybersecurity is especially relevant. [17, 20]

Open AI Gym. OpenAI Gym is a toolset for conducting reinforcement learning research. It comprises a growing set of benchmark problems with a common interface, as well as a website where individuals can post their results and compare algorithm performance. This whitepaper describes OpenAI Gym's components as well as the design considerations made for the software[24].

The primary focus is on research that proposes and implements integrated AI solutions to combat DoS and DDoS attacks. Evaluating these solutions' effectiveness, adaptability, and real-world applicability is critical for shaping the research endeavor.[20]

The review of literature on performance measures for AI-driven cybersecurity solutions guarantees that relevant benchmarks are used in the study project. The efficacy of the proposed AI-driven methods should be evaluated using metrics such as accuracy, precision, recall, and response time.

[6,11,24]. The growing use of artificial intelligence (AI) technologies in cybersecurity systems raises both substantial opportunities and ethical concerns [15]. This research study investigates the ethical issues of AI-powered cybersecurity technologies. It explores the possible consequences of AI algorithms in terms of privacy, bias, accountability, and human oversight. The paper's goal is to provide insights into the development of ethical frameworks and recommendations for the appropriate use of AI in cybersecurity. The literature analysis concludes by looking at the legal landscape and ethical issues surrounding AI-driven cybersecurity solutions. Understanding compliance requirements and ethical issues ensures that offered solutions adhere to legal and ethical norms. [5, 7, 20, 21]

2. METHODOLOGY

To model the AI-Driven Solutions for Cyber Threat Detection and Prevention using deep deterministic gradient decent (DDPG), OpenAI Gym and AI control we employed an Ordinary Differential Equation (ODE) to represent the traditional method of improving a student's performance, considering the elements of studying, examination results, and adjusting study strategies as illustrated below. Real-time tracking systems, such as those utilizing IoT for monitoring student activities and performance, provide a foundation for adaptive educational solutions [25].

Mathematical Model formulation

Let:

S(t) represent the student's performance at time t.
L(t) represent the student's study efforts at time t.
E(t) represent the results of exams at time t.
A(t) represent the adjustment of study strategies at time t.
T represent the time constant.
The traditional method can be represented in equation 1

$$\frac{dS}{dt} = L - T \times (S - E) \qquad (1)$$

Such that
L represents the positive impact of study efforts.
(S−E) represents the gap between the student's current performance and the examination results.
T is the time constant, which determines the rate at which the student's performance adjusts based on the difference between their performance and exam results.

A. Traditional methods of cyber threat detection and prevention

There are several reasons to consider discouraging traditional methods of preventing cyber threat (Dos & DDos) or, at least, complementing them with more advanced and adaptive approaches, especially in the context of protecting a student's performance and study environment:

I. Traditional methods often rely on predefined signatures and patterns to identify threats. They might struggle to adapt to rapidly evolving cyber threats and sophisticated attack techniques [13].
II. Traditional methods might struggle to detect new or previously unseen threats, as they typically rely on known attack signatures. This limitation becomes significant as cyber threats continually evolve [23].
III. Traditional methods may produce false positives (incorrectly identifying harmless activities as threats) or false negatives (failing to detect actual threats). This can lead to unnecessary disruptions or overlooked security issues [13].
IV. Traditional methods often lack the ability to understand the context in which activities occur. In a student's study environment, understanding the context is crucial to avoid false alarms and disruptions during legitimate academic activitie s[23].

V. Student study environments are dynamic and can experience fluctuations in network traffic and activities. Traditional methods may struggle to efficiently adapt to these changes and distinguish between normal and abnormal behaviors [13,23].

VI. Traditional methods might face challenges in detecting insider threats, where individuals with authorized access misuse their privileges. This is relevant in educational settings where students or faculty members may pose unintentional or intentional risks.

VII. Traditional methods can be resource-intensive, requiring frequent updates of signatures and databases. This might pose challenges, especially in educational settings with limited resources. Traditional methods may struggle to detect and prevent advanced persistent threats, which are sophisticated, targeted attacks that often operate stealthily over extended periods [13].

VIII. Traditional methods often lack continuous monitoring and real-time analysis capabilities, which are crucial for timely detection and prevention of cyber threats [23].

To address these limitations, adopting more advanced, adaptive, and context-aware approaches, such as those involving machine learning, deep learning, and reinforcement learning, can enhance the security posture of student study environments. These approaches can better handle the complexities and nuances of evolving cyber threats while minimizing disruptions to legitimate academic activities. It's important to strike a balance between traditional and modern methods, tailoring the security strategy to the specific needs and dynamics of the educational setting. To this end a Smart Study Advisor (SSA) is introduced as an additional factor as illustrated in Equation 2

$$\frac{dS}{dt} = L + \alpha \times SSA - T \times (S - E) \qquad (2)$$

Such that

α represents the positive impact of the Smart Study Advisor.

SSA represents the influence of the Smart Study Advisor on the student's performance.

This model incorporates the traditional method of improvement, where the student's performance is adjusted based on study efforts and the difference between current performance and exam results. The Smart Study Advisor introduces an additional positive impact, influencing the student's performance over time. The time constant T reflects the speed of adjustment.

To enhance the Ordinary Differential Equation (ODE), the nature of the student's performance, the impact of study efforts, and the influence of the Smart Study Advisor were added as additional parameters to yield Equation 3.

$$\frac{dS}{dt} = L\left(1 - \frac{S}{E}\right) + \alpha SSA - T(S - E) \qquad (3)$$

Such that

- $L\left(1 - \frac{S}{E}\right)$ represents the nature of the student's performance improvement, considering a diminishing return as the student's performance approaches the exam results (E).
- α·SSA represents the positive impact of the Smart Study Advisor (SSA) on the student's performance.
- T·(S−E) represents the adjustment of the student's performance based on the difference between their current performance and exam results (E).
- T is the time constant, determining the rate of adjustment.

This model incorporates the nature of the student's performance improvement, the impact of study efforts, and the positive influence of the Smart Study Advisor on the student's performance over time. The time constant T reflects the speed at which the student's performance adjusts based on study efforts and the Smart Study Advisor's influence. For better Understanding refer to program flows below

Flow Chart: Traditional Method Without SSA:

I. Start

II. Input: Initial Student's Performance (S_0), Study Efforts (L), Time Constant (T)

III. Initialize: S(t)= S_0,(t)=0

IV. While $t \leq T_{Max}$ (Max Time):

V. Calculate E(t) (Results of Exams)

VI. Calculate A(t) (Adjustment of Study Strategies)

VII. Update S(t) using ODE: $\frac{dS}{dt} = L\left(1 - \frac{S}{E}\right) + \alpha SSA - T(S - E)$ (4)

VIII. Increment t.

IX. End

Flow Chart: Traditional Method With SSA:

I. Start

II. Input: Initial Student's Performance (S_0), Study Efforts (L), Time Constant (T), SSA Impact (α)

III. Initialize: S_0,(t)=0

IV. While $t \leq T_{Max}$ (Max Time):

Calculate E(t) (Results of Exams)

Calculate A(t) (Adjustment of Study Strategies)

Calculate SSA(t) (Smart Study Advisor's Influence)

V. Update S(t) using ODE: $\frac{dS}{dt} = L\left(1 - \frac{S}{E}\right) + \alpha SSA - T(S - E)$ (5)

VI. Increment t

VII. End

Flow Chart: Enhanced Method with Student's Performance, Study Efforts, and SSA:

I. Start

II. Input: Initial Student's Performance (S_0), Nature of Performance (L), Time Constant (T), SSA Impact (α)

III. Initialize: S_0, t=0

IV. While t While $t \leq T_{Max}$ (Max Time):

V. Calculate E(t) (Results of Exams)

VI. Calculate. A(t) (Adjustment of Study Strategies)

VII. Calculate SSA(t) (Smart Study Advisor's Influence)

VIII. Update S(t) using ODE) $\frac{dS}{dt} = L\left(1 - \frac{S}{E}\right) + \alpha SSA - T(S - E)$ (6)

IX. Increment t

X. End

3. RESULTS

This section presents the results of the simulation of Fortifying Data Communication Networks, based on DDPG for Cyber Threat Detection and Prevention, using Python Jupyter Notebook IDE and MATLAB. The training and testing results are presented in Figures 1 and 2.

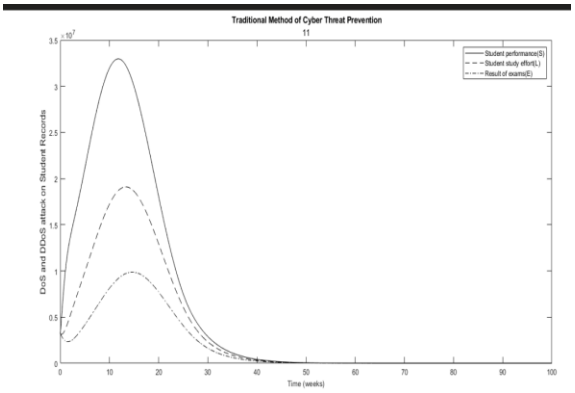

Figure 1: Traditional methods of Cyber Threat Prevention Performance

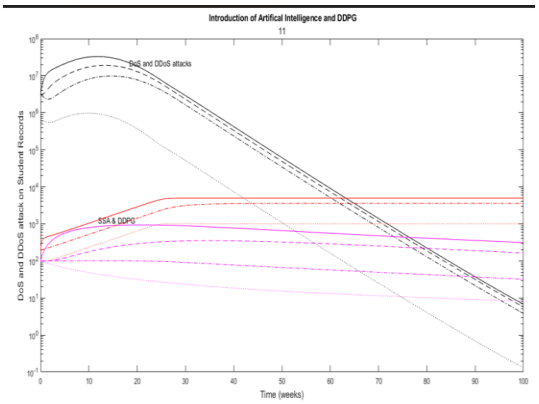

Figure 2: Introduction of AI and DDPG in the Attacked Environment

4. DISCUSSION

Figures 1 and 2 generates a line plot comparing the three scenarios over time, providing a visual representation of how student performance evolves in each case. Figure 1 Track the evolution of the student performance record over time when the traditional methods of combating cyberattack (DDOS and DOS) were used to monitor the student study environment. The network saw student record manipulation as the performance signal increased significantly despite delays in study level and exam outcomes. The reason for the significant increase in the student performance index is the successful and covert manipulation of the real student records via DOS and DDOS.

Figure 2 illustrates the significant network flow improvement that occurred as soon as an AI-driven solution (DDPG) was implemented. This was made possible by the Smart Study Advisor's (SSA) superior performance, which caused student performance records to gradually decline to reflect the state-of-the-art record. The true state of the students' performance was revealed when the network was further improved to examine the effects of taking into account the nature of performance, study efforts, and SSA influence. At the same time, the interferences from DoS and DDoS attacks were reduced to an almost negligible level. Further evidence that DDPG and the improved model support a more flexible learning process is shown by Figure 2. observing trends in the simulated DoS and DDoS attack performance graphs. We can conclude that the AI-driven agent successfully identified and stopped attacks. This is seen in the case where the network was able to reduce a signal that peaked at 3.5*107 to less than 104 in a matter of weeks. This provides additional evidence of the beneficial effects the AI system (SSA) SSA has on students' performance in both conventional and enhanced scenarios by enhancing the learning process as a whole.

As the DOS and DDOS attacks were successfully reduced to 100, this figure further demonstrates the network's stability and consistency of performance, suggesting a more stable learning curve.

5. CONCLUSION

Based on the topic "Fortifying Data Communication Networks: AI-Driven Solutions for Cyber Threat Detection and Prevention," the following findings were established in light of the successful implementation of the combined approach involving Deep Deterministic Policy Gradient (DDPG), OpenAI Gym, and Deep Q Networks (DQN) for detecting and preventing Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks on student performance: a novel cybersecurity architecture that uses OpenAI Gym, DQN, and DDPG to strengthen data communication networks in educational contexts and provide flexible, context-aware solutions to handle the ever-changing threat landscape, The study level, exam outcomes, and adjustment made utilizing two scenarios on a wired and Wifi network using conventional ways without help and with AI-driven support are the three parameters that the real-time model simulation focuses on when analyzing student performance. Additionally, when the reinforcement learning architecture was put into practice, the network's behavior was observed in relation to students' performance using conventional monitoring techniques. The robustness of the system was thoroughly assessed by simulating actual DoS and DDoS attacks in the educational network using OpenAI Gym, varying the attack paths, intensities, and durations. The outcomes showed how adaptable the system is to changing network conditions and how it can pick up on evolving cyberthreats. To summarize, the real-time experiment effectively showcased the versatility, context-aware defense, and positive impact on student performance of an advanced cybersecurity system in the face of cyber-attacks. The research offers significant perspectives to the continuous endeavors to strengthen educational networks against constantly changing security threats. To sum up, DDPG, OpenAI Gym, and DQN work well together to create a dynamic and adaptable system that can identify and stop DoS and DDoS attacks on student performance. As shown

from the simulated system, the contextual awareness, adaptability, and proactive measures brought about by this combination contribute to a thorough and durable cybersecurity solution inside educational environments. To validate these discoveries and improve the system's operation, comprehensive testing and practical implementation are necessary.

References

[1] Bowman, M., Debray, S. K., and Peterson, L. L. 1993.

[2] Brockman, Greg & Cheung, Vicki & Pettersson, Ludwig & Schneider, Jonas & Schulman, John & Tang, Jie & Zaremba, Wojciech. (2016).

[3] extrahop.com https://www.extrahop.com/resources/attacks/dos/

[4] F. Ullah, A. Alsirhani, M.M. Alshahrani, A. Alomari, H. Naeem, S.A. Shah (2022) Explainable malware detection system using transformers-based transfer learning and multi-model visual representation Sensors, 22 (18) (2022), 10.3390/s22186766

[5] Greg Brockman, Vicki Cheung, Ludwig Pettersson, Jonas Schneider, John Schulman, Jie Tang, Wojciech Zaremba (2016) OpenAI Gym arXiv:1606.01540 [cs.LG arXiv:1606.01540v1 https://doi.org/10.48550/arXiv.1606.01540

[6] Hardik Shah (2023) Ethical Considerations in AI-Powered Cybersecurity. https://techspective.net/2023/12/05/ethical-considerations-in-ai-powered-cybersecurity/#google_vignette(Retrieved 2/3/2024)

[7] Itagi, V.; Javali, M.; Madhukeshwar, H.; Shettar, P.; Somashekar, P.; Narayan, D. DDoS Attack Detection in SDN Environment using Bi-directional Recurrent Neural Network. In Proceedings of the 2021 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER), Nitte, India, 19–20 November 2021; pp. 123–128. [

[8] Jyotismita Talukdar T. P. Singh Basanta Barman Artificial Intelligence and Cyber Security in Industry 4.0 9819921147, 9789819921140 Springer Pages *373 [374] Year 2023*

[9] Katy Allan (2023) The rapidly evolving threat landscape of 2024 https://cybermagazine.com /articles/the-rapidly-evolving-threat-landscape-of-2024 (retrieved 2/3/2024)

[10] Karan, B.; Narayan, D.; Hiremath, P. Detection of DDoS Attacks in Software Defined Networks. In Proceedings of the 2018 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS), Bengaluru, India, 20–22 December 2018; pp. 265–270. [Google Scholar] [CrossRef]

[11] Krishnan, P., Jain, K., Aldweesh, A., Prabu, P., & Buyya, R. (2023). OpenStackDP: A scalable network security framework for SDN-based OpenStack cloud infrastructure. Journal of Cloud Computing, 12(1).

[12] M. Tetaly, P. Kulkarni Artificial intelligence in cyber security - a threat or a solution AIP Conference Proceedings, 2519 (2022), 10.1063/5.0109664 Google Scholar

[13] Mbasuva, U.; Zodi, G.A.L. Designing Ensemble Deep Learning Intrusion Detection System for DDoS attacks in Software Defined Networks. In Proceedings of the 2022 16th International Conference on Ubiquitous Information Management and Communication (IMCOM), Seoul, Korea, 3–5 January 2022; pp. 1–8.

[14] Mhamdi, L.; McLernon, D.; El-Moussa, F.; Zaidi, S.A.R.; Ghogho, M.; Tang, T. A deep learning approach combining autoencoder with one-class SVM for DDoS attack detection in SDNs. In Proceedings of the 2020 IEEE Eighth International Conference on Communications and Networking (ComNet), Hammamet, Tunisia, 27–30 October 2020; pp. 1–6. [Google Scholar] [CrossRef]

[15] S. Sivamohan, S.S. Sridhar An optimized model for network intrusion detection systems in industry 4.0 using XAI based Bi-LSTM framework Neural Computing & Applications, 35 (15) (2023), pp. 11459-11475, 10.1007/s00521-023-08319-0

[16] S. Zeadally, E. Adi, Z. Baig, I.A. Khan (2020) Harnessing artificial intelligence capabilities to improve cybersecurity IEEE Access, 8 (2020), pp. 23817-23837, 10.1109/ACCESS.2020.2968045

[17] Sowmya, T., & Mary Anita, E. A. (2023). A comprehensive review of AI-based intrusion detection system. Measurement: Sensors, 28. https://doi.org/10.1016/j. measen.2023.100827

[18] T. Sowmya, E.A. Mary Anita A comprehensive review of AI-based intrusion detection system Measurement: Sensors, 28 (2023), 10.1016/j.measen.2023.100827

[19] Truong, T. C., Diep, Q. B., & Zelinka, I. (2020). Artificial intelligence in the cyber domain: Offense and defense. Symmetry, 12(3). https://doi.org/10.3390/ sym12030410

[20] Vasupalli Mano, B. V. Ramana, B. R. Sarath Kumar, S. Vijay Peter, Shailendra Kumar Mittal, (2023) Utilizing Artificial Intelligence for Enhancing Cyber Security: Applications and Methodologies Sumanta Bhattacharya6International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 11 Issue: 9 Article Received: 25 July 2023 Revised: 12 September 2023 Accepted: 30 September 2023

[21] Fischer, G. A., Ogar-Abang, M. O., Inameti, E. E., & Akpama, E. J. Determination of Mobile Path Loss and Signal Penetration Level in Calabar. Utilizing Information Technology to Achieve Circular Economy and Sustainable Development, 19

[22] Xin, Y., L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang. 2018. "Machine Learning and Deep Learning Methods for Cybersecurity." IEEE Access, 6: 35365–81.

[23] Yungaicela-Naula, N.M.; Vargas-Rosales, C.; Perez-Diaz, J.A. SDN-Based Architecture for Transport and Application Layer DDoS Attack Detection by Using Machine and Deep Learning. IEEE Access 2021, 9, 108495–108512. [Google Scholar] [CrossRef]

[24] Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, …, K.K.R. Choo (2021) Artificial intelligence in cyber security: Research advances, challenges, and opportunities Artificial Intelligence Review (2021), pp. 1-25

[25] Fischer, G. A., Ojong, V., & Inametic, e. Design And Implementation Of A University Smart Attendance Tracking System Using Geo-Location And Iot.