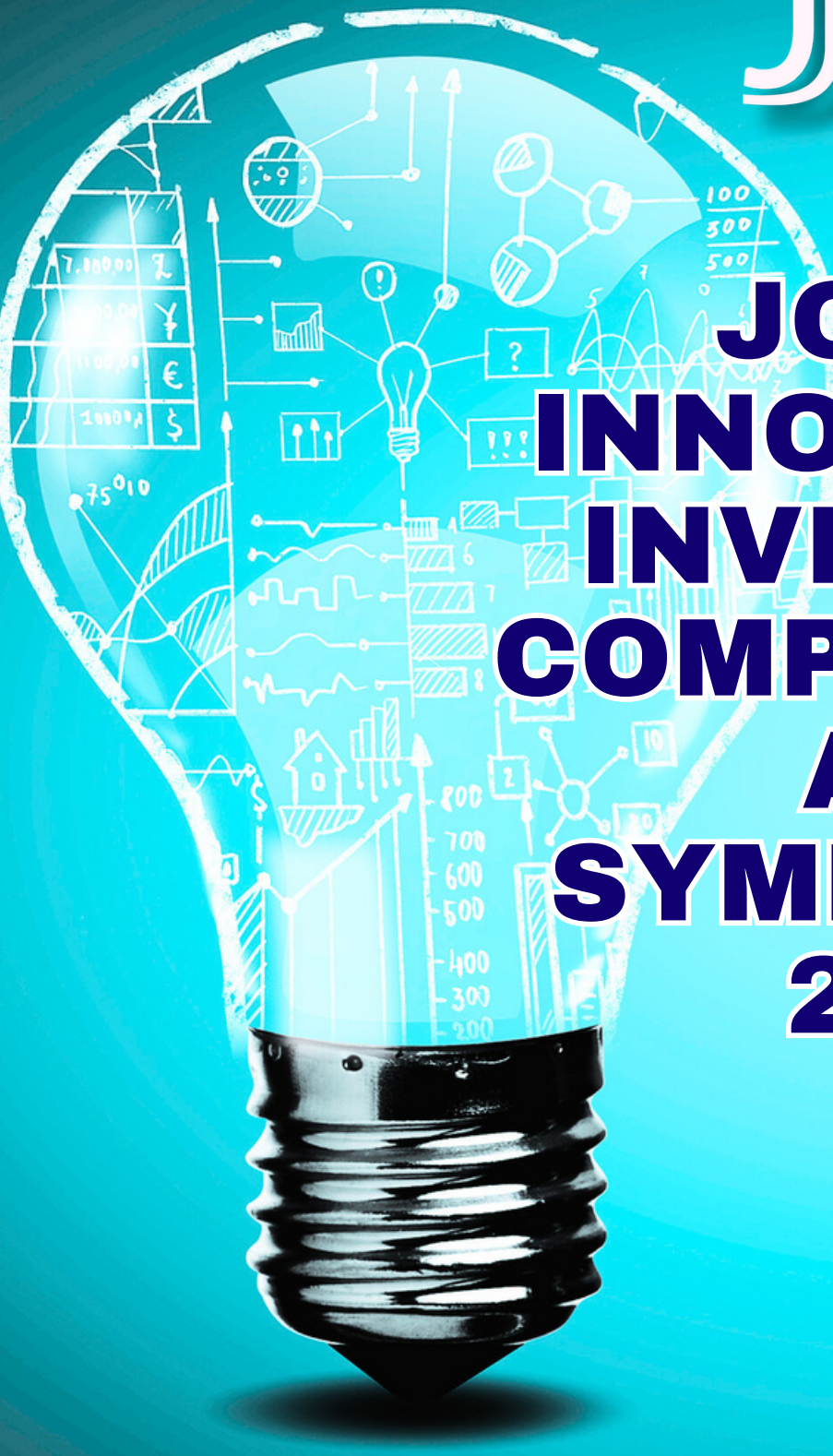
UNIVERSITI TEKNOLOGI MARA

2023

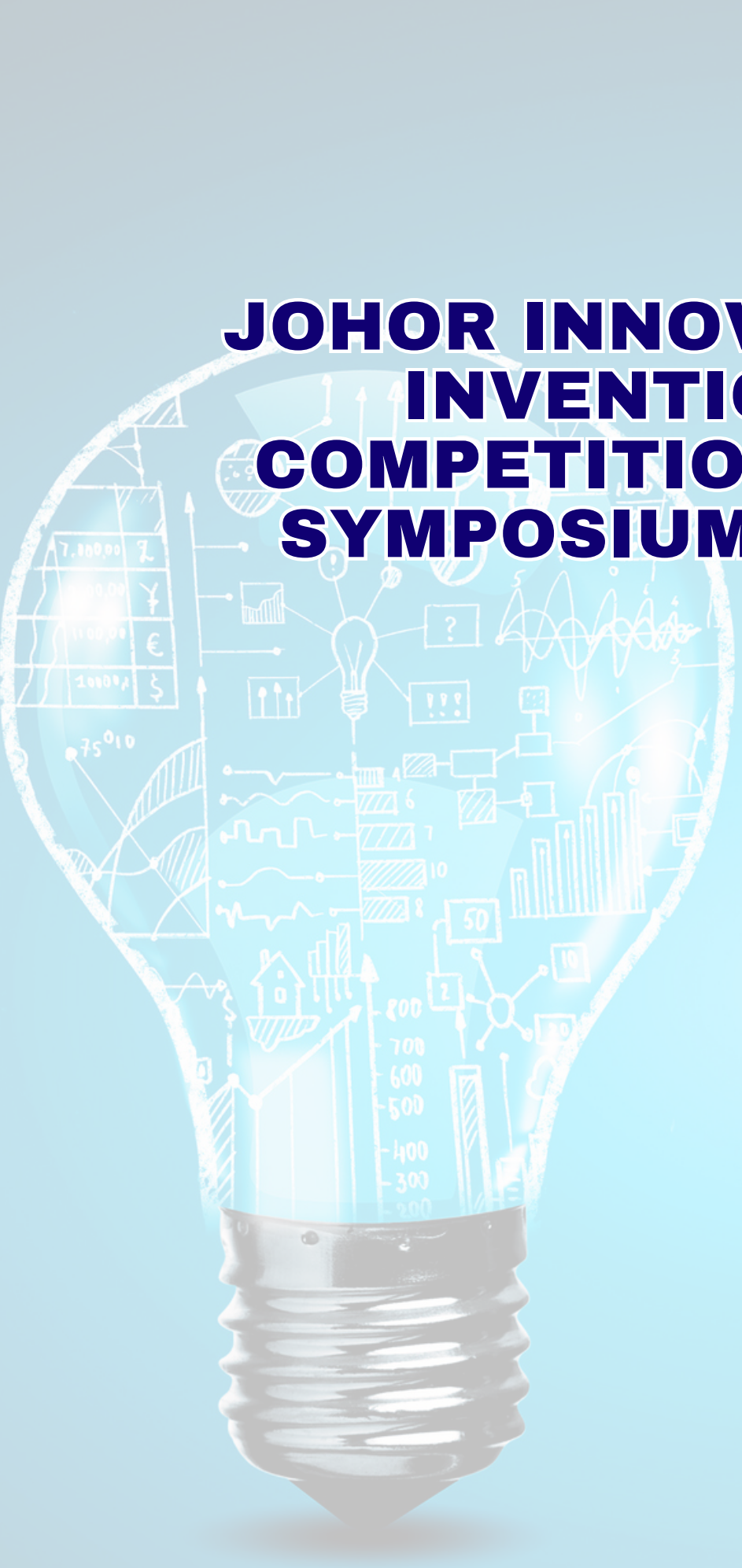
JIICaS



JOHOR INNOVATION INVENTION COMPETITION AND SYMPOSIUM 2023

" Innovation Inspires a Society to be Critical and Creative"

JOHOR INNOVATION INVENTION COMPETITION AND SYMPOSIUM 2023



JOHOR INNOVATION INVENTION COMPETITION AND SYMPOSIUM 2023

" Innovation Inspires a Society to be Critical and Creative"

Editors-in-Chief

AHMAD KHUDZAIRI KHALID

NUR INTAN SYAFINAZ AHMAD

UNIVERSITI TEKNOLOGI MARA

Cawangan Johor

Kampus Pasir Gudang

2023

First Edition 2023

e ISBN: 978-967-0033-17-4

Editors-in-Chief: AHMAD KHUDZAIRI KHALID & NUR INTAN SYAFINAZ AHMAD

Art & Cover Designer: DR. WAN MUNIRAH WAN MOHAMAD & DR. NUR IDAYU ALIMON

Published in Malaysia by
Universiti Teknologi MARA Cawangan Johor
Kampus Pasir Gudang
81750 Masai

Preface

In the name of Allah, the Almighty who gives us the enlightenment, the truth, the knowledge and with regards to Prophet Muhammad (peace be upon him) for guiding us to the straight path. We thank to Allah for giving us guidance and strength to write this e-book.

This e-book compiles the extended abstracts that submitted to Johor Innovation Invention Competition and Symposium 2023 (JIICaS2023), where JIICaS2023 is a virtual platform for all creative minds to share and present their invention and innovation. The extended abstracts are divided into two categories, which are Category A (Higher Educational Student/ Any Recognized Institutional Students in Malaysia) and Category B (Primary/ Secondary School Students / Special Education School Students in Johor). Each abstract gives a brief background on the innovation or project.

We hope that this e-book will help the readers to get to know the innovation done by the students from both categories and get some ideas to develop future innovation products.

A105

Rogue Access Point Detection and Tracking System Using Trilateration Algorithm

Lee Chiew Min[1], Ang Boon Keat[1], Kok Ser Leen[1],
Dr. Abdulrahman Aminu Ghali[1], Ms. Nor 'Afifah Binti Sabri[1]

[1]Faculty of Information and Communication Technology (FICT),
Universiti Tunku Abdul Rahman, Kampar, Petaling Jaya 31900, Malaysia.

victor84@1utar.my (Lee Chiew Min)
keat.qwerty@1utar.my (Ang Boon Keat)
alankok02@1utar.my (Kok Ser Leen)
aminu@utar.edu.my (Dr. Abdulrahman Aminu Ghali)
afifahs@utar.edu.my (Ms. Nor 'Afifah binti Sabri)

ABSTRACT

In the current digital era, network security is an essential concern, especially in the growing usage of wireless networks. Network security is vulnerable to rogue access points, and unauthorized wireless access points lead to security threats. The rapid growth of wireless technology has led to an increased demand for wireless networks in numerous sectors, including educational institutions. However, the widespread use of wireless networks has also introduced new security challenges, particularly the threat of rogue access points (RAPs). A rogue access point is an unauthorized wireless access point that has been installed on a network without the knowledge or approval of the network administrator. This project aims to evaluate and implement the most effective method for detecting RAPs in tertiary institutions. Besides, that the project introduces a robust method called trilateration algorithm. Therefore, the proposed trilateration algorithm if implemented will detect and reduce the risk of unauthorized network access in tertiary institutions and save the danger of financial loss. In addition, a preliminary study will be conducted to identify potential network security vulnerabilities and a literature review will be carried out to analyze the latest research on rogue access points to compare with our proposed trilateration algorithm. On this basis, the concept of mitigating the threat of rogue access point attacks using the proposed approach may be considered when designing a framework to mitigate the rogue access point in tertiary institutions.

Keywords: Wireless Networks, Network Security, Rogue Access Points (RAPs), Trilateration Algorithm.

1.0 INTRODUCTION

In the modern digital age, wireless network communication has become an indispensable and important part of human society as it has revolutionized the way humans connect and communicate. As wireless connectivity has brought us the convenience and flexibility of browsing the internet from anywhere at any time, it also brought forth a critical security concern which is the emergence of rogue access points where unauthorized individuals perform within the network without any authorization, making more potential entry points for performing various malicious activities. In the academic environment, like many other public spaces RAPs can be set up easily by both insiders and outsiders. Once the RAP is successfully installed, it can initiate an attack on the network it targeted which will cause security breaches including

compromising data confidentiality, stealing network resources, and even sniffing out the packet through the network using Man-in-the-Middle (MITM and DoS attacks [1][2], where this attack performs a sniffing attack in between the servers and clients to gain unauthorized access to sensitive data.

2.0 OBJECTIVE

The first objective of this project includes the development of a new dedicated Rogue Access Point Detection and Tracking System specifically designed to detect the RAP effectively and efficiently within the tertiary institution network environment. The second objective of this project is to design a system that is expected to perform two main features which are precise detection of the RAP by scanning the network around the campus. After it has successfully detected the RAP, it will be able to track the movement or location of the RAP in real time. Lastly, to improve the security of the network around the campus of the tertiary institution in terms of preventing potential security breaches and ensuring the confidentiality and integrity of sensitive data.

3.0 DESCRIPTION OF INNOVATION / METHODOLOGY

In this section, the proposed methodology was divided into two sections. These are hardware and software. The details of the explanation of the methodology are described below.

3.1 Hardware

The hardware involved in this project is a laptop and wireless USB adapter. The laptop in this project plays a crucial role, as most of the research and development are using a laptop to perform their experiments. The specification of the implementation of the project is identified in Table 1.1. while the Wireless USB adapter specification is also shown in Table 1.2. The overall features of the USB adapter are described in Table 1.3.

Table 1.1 Laptop Specifications

Description	**Specifications**
Model	S340-14IWL Laptop (Ideapad) - Type 81N7
Processor	Intel(R) Core (TM) i5-8265U CPU @ 1.60GHz, 1800 Mhz, 4 Core(s), 8 Logical Processor(s)
Operating System	Microsoft Windows 11 Home Single Language
Graphic	Intel(R) UHD Graphics 620
Memory	8GB
Storage	Window SSD 236GB

Table 1.2 Wireless USB Adapter Specifications

Description	**Specifications**
Interface	USB 2.0
Button	WPS button
Dimensions (W x D x H)	3.7 x 1.0 x 0.4 in. (93.5 x 26 x 11mm)
Antenna Type	Detachable Omni Directional (RP-SMA)
Antenna Gain	4dBi

Table 3.3 Wireless features of wireless USB adapter

Description	**Specifications**
Wireless Standards	IEEE 802.11n, IEEE 802.11g, IEEE 802.11b
Frequency	2.400-2.4835GHz
Signal Rate	11n: Up to 150Mbps(dynamic) 11g: Up to 54Mbps(dynamic) 11b: Up to 11Mbps(dynamic)
Reception Sensitivity	130M: -68dBm@10% PER 108M: -68dBm@10% PER 54M: -68dBm@10% PER 11M: -85dBm@8% PER 6M: -88dBm@10% PER 1M: -90dBm@8% PER
Transmit Power	<20dBm
Wireless Modes	Ad-Hoc / Infrastructure mode
Wireless Security	Support 64/128 bit WEP, WPA-PSK/WPA2-PSK
Modulation Technology	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM

3.2 Software

In this project, several tools are integrated into the research and development: Oracle VM Virtual Box, Kali-Linux virtual machine, and Python programming language. Oracle VM virtual machine as a platform running the virtual machine within an isolated environment to eliminate the physical host. Thus, it allows the utilization of virtual machines like Kali-Linux to perform penetration testing. Moreover, Kali-Linux can be a robust cybersecurity-oriented system, offering extensive features and capabilities for ethical hacking and research activities. Thus, using Kali Linux as the operating system will enhance the performance and overall environment. While the Python programming language facilitates the development of the system's algorithm components. Section 1.1 describes the proposed framework of the RAP Detection and Tracking System.

3.3 Proposed Framework of RAP Detection and Tracking System

In this project, the proposed RAP Detection and Tracking System is illustrated to describe the details of the proposed project. Figure 1.1 illustrates the framework.

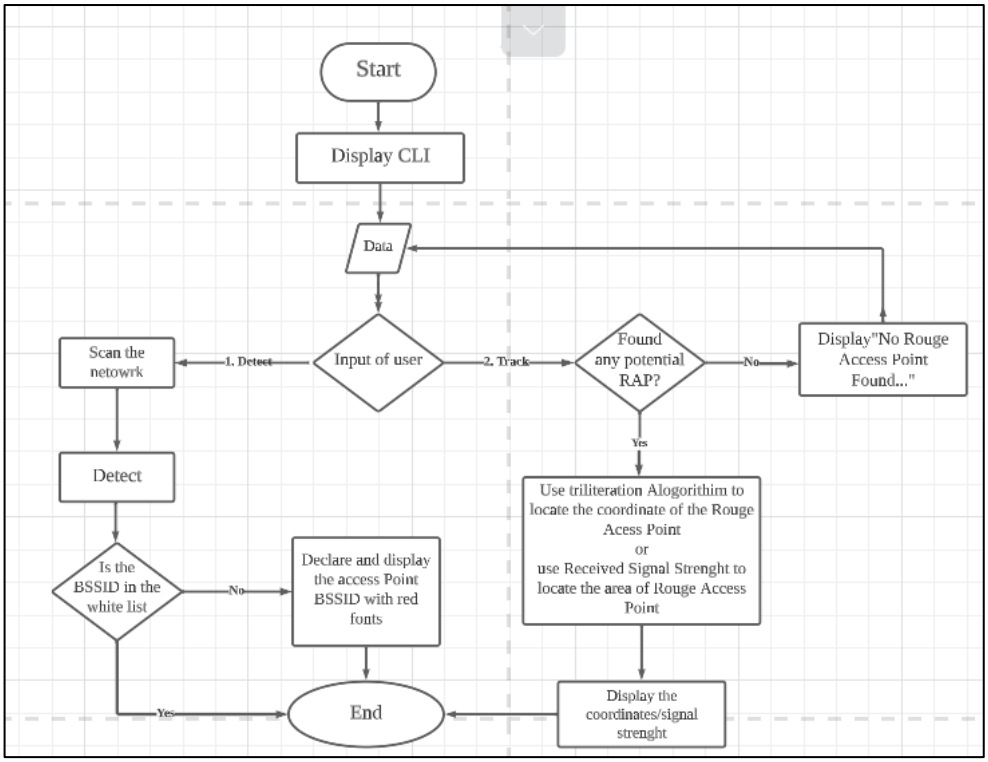


Figure 1.1: Flow chart of the RAP Detection and Tracking System

Figure 1.1 shows the project's flow chart of the RAP Detection and Tracking System. At the beginning of the system, it will display CLI to the users, and users will choose the functions they want to use for the detection, tracking, and exit. If the user chooses detection, it will indicate the surroundings available for the network to determine any potential Rogue Access Point. Whereas if yes, it will display the potential Rouge access point with red font and display BSSID, SSID, and other relevant information, while if no it will show no Rouge Access Point found. Therefore, if the user chooses to track, it will proceed to a condition where it checks whether the system has found any potential RAPs. If found, then it will use a trilateration algorithm to locate the coordinate of the RAP and further receive a signal strength to locate the area of the RAP to the user. Thus, Figure 1.2 displays the use of a case diagram.

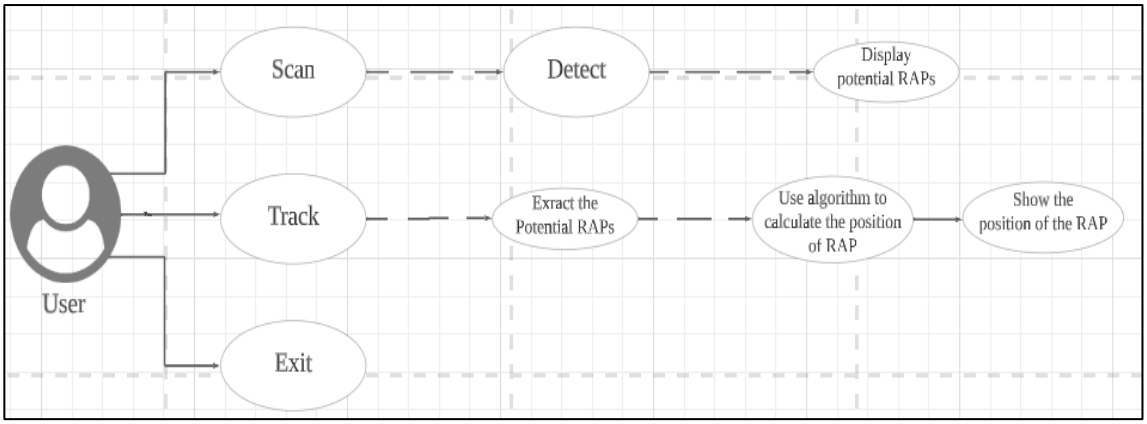


Figure 1.2: Use Case Diagram

Figure 1.2 shows a Use Case Diagram to indicate the function of the system provided on how it goes, and the result that will be shown to the users. In this case, the system has two main

functions. These are detection and tracking which will serve the function of displaying information to the user. While, if the user wants to end the session the system also allows it.

4.0 ADVANTAGE / IMPACT / RESULTS / NOVELTY

In this section, the advantages, impact, result, and novelty of the project will be described as enhancing security, incident response, reducing the risk of security incidents, enhancing IT management, mitigating unauthorized access points within the organization, IoT device detection, enhanced reporting, and visualization, wireless intrusion prevention and continues monitoring.

5.0 CONCLUSION

In conclusion, the novel features and methodologies describe how RAP Detection and Tracking Systems have evolved in tackling cybersecurity threats and the increasing complexity of modern networks. In addition, if the method is implemented will provide organizations with more robust tools and strategies to proactively identify and mitigate the risks associated with rogue access points.

References

[1] Ghali, A. A., Ahmad, R., & Alhussian, H. (2021). A framework for mitigating DDoS and DOS attacks in IoT environment using hybrid approach. Electronics, 10(11), 1282.

[2] Aminu Ghali, A., Ahmad, R., & Alhussian, H. S. A. (2020). Comparative analysis of DoS and DDoS attacks in Internet of Things environment. In Artificial Intelligence and Bioinspired Computational Methods: Proceedings of the 9th Computer Science On-line Conference 2020, Vol. 2 9 (pp. 183-194). Springer International Publishing.