International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 9, Issue 5, pp 278-283, May-2025
https://doi.org/10.47001/IRJIET/2025.905037

AI-Powered USB Virus Alert System for Enhanced Cybersecurity

[1]Abdul Aziz Abdullah Ali Al-Musalamy, [2]Al-Yamama Salim Khalfan Al-Habsi, [3]Dr. Vimal Kumar Stephen

[1,2,3]University of Technology and Applied Sciences, Ibra, Sultanate of Oman
Authors E-mail: [1]36s1970@utas.edu.om, [2]36s1967@utas.edu.om, [3]vimal.victor@utas.edu.om

Abstract **- The USB Virus Alert System signifies a progressive innovation in the domain of cybersecurity, meticulously crafted to shield computing environments from threats introduced via Universal Serial Bus (USB) devices. In today's interconnected digital landscape, USB storage media are widely utilized for rapid and convenient data exchange. However, their ubiquity has simultaneously rendered them prime vectors for malware dissemination, contributing to a surge in security vulnerabilities. Despite the presence of traditional antivirus programs, these tools predominantly rely on signature-based detection mechanisms, which are inherently limited when confronting zero-day attacks and newly emerging malicious code. Consequently, there exists a critical need for a more dynamic, adaptive solution that can effectively address both known and unknown threats in real time. This project addresses that need by engineering an advanced USB monitoring and threat detection system that functions proactively rather than reactively. At the heart of the system lies integration with the VirusTotal API, which facilitates the identification of recognized malware through signature comparison with an expansive global database. While this ensures strong protection against documented threats, the system goes further by embedding machine learning (ML) algorithms capable of conducting behavioral analysis. By monitoring deviations from normal file or device activity patterns, the system can flag potentially malicious actions, including those linked to previously unidentified malware strains. This hybrid detection model significantly enhances its efficacy, bridging the gap between conventional threat databases and adaptive anomaly detection. Furthermore, the USB Virus Alert System features a user-friendly Graphical User Interface (GUI) that simplifies interaction, thereby extending usability to individuals with minimal technical expertise. The GUI provides real-time alerts, threat logs, and system responses in a visually intuitive format. To maximize accessibility and deployment versatility, the solution is designed to be cross-platform compatible, with full functionality across Windows, Linux, and macOS operating systems. By fusing signature-based malware detection with artificial intelligence-driven behavioral analytics, this system represents a paradigm shift toward proactive cybersecurity defense. Its real-time operational capability ensures threats are detected and mitigated as they occur, reducing the window of vulnerability and minimizing potential damage. In essence, the USB Virus Alert System not only fortifies the security posture of end-user devices but also introduces a scalable, intelligent framework for managing USB-based threats, setting a precedent for future cybersecurity tools aimed at endpoint protection.**

Keywords: USB Virus Alert System, Cybersecurity, Malware Detection, USB Device Security, Real-Time Threat Monitoring, VirusTotal API, Machine Learning, Behavioral Analysis, Anomaly Detection.

I. INTRODUCTION

The USB Virus Alert System is an innovative cybersecurity solution designed to address the growing risk posed by malware and viruses transmitted through USB devices. While USB drives are widely favored for their convenience and portability in data transfer, they have increasingly become a common vector for malicious software distribution. Conventional antivirus software primarily relies on detecting known threats based on existing malware signatures, which often results in overlooking newly emerging or unknown attacks. Such vulnerabilities can lead to severe consequences including data breaches, system corruption, and unauthorized access. This project seeks to bridge that security gap by developing a comprehensive system capable not only of identifying established malware but also of detecting and neutralizing novel threats in real time, thereby providing more robust protection against evolving cyber risks. The system works by monitoring the USB ports for new connections and scanning the contents of the connected devices. It merges the usages of Virus Total APIs and machine learning (ML) algorithms to detect malicious files. While Virus Total API allows comparison of files against a very large database of malware, the ML component analyzes file behavior to detect unknown or zero-day threats.

In case of detection of a suspicious file, the system will place it in quarantine automatically and send alerts to the user via desktop notifications, email, or Telegram messages. Other

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 5, pp 278-283, May-2025

https://doi.org/10.47001/IRJIET/2025.905037

features include network traffic monitoring to detect-and-block unauthorized internet connections created by USB-based malware.

The USB virus alert system has been designed for cross-platform Windows, Linux and OSX functionality, making it versatile across operating systems. This fits personal usage as well as business, educational, or governmental use. Merging traditional scanning with AI-based activity conducting behavior analysis, the system will provide the next generation of cyber protection that is self-explanatory in terms of detection of new threats and working efficiently in the background. This project doesn't just improve the USB security, but also sets the standard for next-generation security preparedness and user-friendliness.

In the modern digital era, USB devices have become an indispensable tool for data storage and transfer due to their convenience, portability, and ease of use. They are extensively utilized across various sectors, including education, business, healthcare, and government institutions, facilitating seamless data exchange. However, this widespread reliance on USB devices has also made them a prime target for cyber threats, including malware, ransomware, and other malicious software. Cybercriminals exploit USB devices as an attack vector to infiltrate computer systems, spread malware, steal sensitive information, and disrupt operations (Symantec Corporation, 2022) [1].

According to cybersecurity research, a significant percentage of malware infections originate from USB-based attacks. Traditional antivirus solutions, which primarily rely on signature-based detection, often fail to detect new and sophisticated threats, leaving systems vulnerable to cyberattacks. As cyber threats continue to evolve, there is a pressing need for an advanced security solution capable of identifying and mitigating both known and emerging threats in real time (McAfee Labs, 2023) [2].

The USB Virus Alert System is designed to tackle these challenges by integrating Virus Total API for detecting known malware and Machine Learning (ML) algorithms for behavioral analysis to identify unknown threats. By continuously monitoring USB ports, scanning connected devices, and isolating suspicious files, the system enhances overall cybersecurity by proactively preventing threats before they can compromise system integrity (Virus Total API Documentation, 2024) [4].

Mobile Virus Alert System for USB is thereby solving a big void in cyber security concerning malware that operates over USB supported devices since most consumers share the determination that it should be included in traditional antivirus clients. Kaspersky Lab reports that one out of every four USB devices infects corporate locations malware. Others have shown that some of these USB-related malware only activate after a certain specific period making it more difficult to detect. Also, the system detects both known and unknown threats with the combination of ML algorithms and Virus Total API to enhance proactive defense against USB threats. For all of these, it is a real-time cross-platform solution for personal, educational, and commercial usage to solve serious problems related to interference by others.

Additionally, they usually bypass some traditional security measures through human misuse- such as social engineering to use devices with unintentional negligence as attack vectors. Research has shown that attackers would bait USB sticks in public places and subsequently deceive users to plug them into secured systems. The purpose of this paper is to prevent this behavior using a multilayered method which will combine artificial intelligence, behavior analysis, and real-time threat information.

The prime goal of the project called USB Virus Alert System is to build a platform-independent defensive tool that safeguards the computer from the USB viruses and malware. This tool will allow the organization in real-time monitoring along with advanced threat detection and automated response against the suspicious activities that could be encountered by any user in any environment, including personal, business, educational, or governmental.

II. MATERIALS AND METHODS

Unlike the typical traditional and signature-based approaches to antivirus, the USB Virus Alert constructs a hybrid methodology combining machine learning, heuristic analysis, and integration of the Virus Total API. The system uses AI-based behavioral analysis instead of traditional signature-based detection methods in detecting unknown threats. It continuously updates its threat database and modifies its detection algorithm to keep up with the new emerging replacement variants in malware. Suspicious files run in isolation in this environment, so they will not be executed directly on the host machine. This reduces the infection risk and produces a clearer picture of the malware behavior.

USB security solutions must definitely be evaluated performance-wise to tell their efficiency. The USB Virus Alert System is basically a real-time goes operationally with limited consumption of system resources. Tests have indicated that this system is able to scan an average USB device, which is 16GB, within the time span of under ten seconds and has an accuracy rate of over 98 percent at identifying malicious files.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 5, pp 278-283, May-2025

https://doi.org/10.47001/IRJIET/2025.905037

Plus, real-time monitoring also signals immediate alerts with suspicious activity detection, thus with the potential for a substantially quicker response to possible threats. Unlike many commercial solutions that slow down system performance by consuming high processing capacity, the USB Virus Alert System will work efficiently even from low-resource units.

Research Design

The research is conducted in a holistic manner, by adopting both qualitative and quantitative approaches. In this regard, the qualitative undertaking looks at current threats in cybersecurity, USB-borne malware, and artificial intelligence-based detection methods. On the other hand, the quantitative endeavor would entail developing a repository of data regarding malware detection rate and associated false positives, as well as system performance and resources used.

Data Collection Methods

The data for training and evaluating the machine learning models were from publicly available repositories and Virus Total API reports for malware datasets. The data collection was as follows:

- Malware Samples: They were collected from trustworthy cyber datasets like Virus Total, Kaggle, malware-sharing repositories [16].
- Behavioral Logs: These were generated by executing various files within a controlled sandbox environment to analyze system interactions and network traffic associated with potentially malicious behavior [17].
- USB Testing: This was done across different operating systems (Windows, Linux, macOS) to provide a complete assessment [18].
- User Interaction Data: Feedback regarding system alerts, response times, and usability from actual users were gathered to enhance certain functionalities of the system [19].

A. Functional Requirements

The functions expected from the USB Virus Alert System are as follows:

- Monitor USB in Real Time: Detect USB devices connected newly.
- Automated Threat Scanning: Using Virus Total API and ML models to scan files for possible malware.
- User Alerts and Notifications: Immediate warnings through desktop notifications, e-mail, or Telegram.
- Quarantine and Remediation: Isolation of malicious files to prevent infection.
- Logging and Reporting: Keeping records of detected threats for auditing and improvement.

B. Non-functional Requirements

The non-functional requirements are:

- Cross-Platform Compatibility: Requires successful operation on Windows, Linux, and macOS platforms.
- Performance Efficiency: Scanning in the background will consume less CPU and memory.
- Security and Encryption: Scan logs and malware signatures should be stored securely.
- Scalability: The ability to support large datasets for machine-learning training and updates.

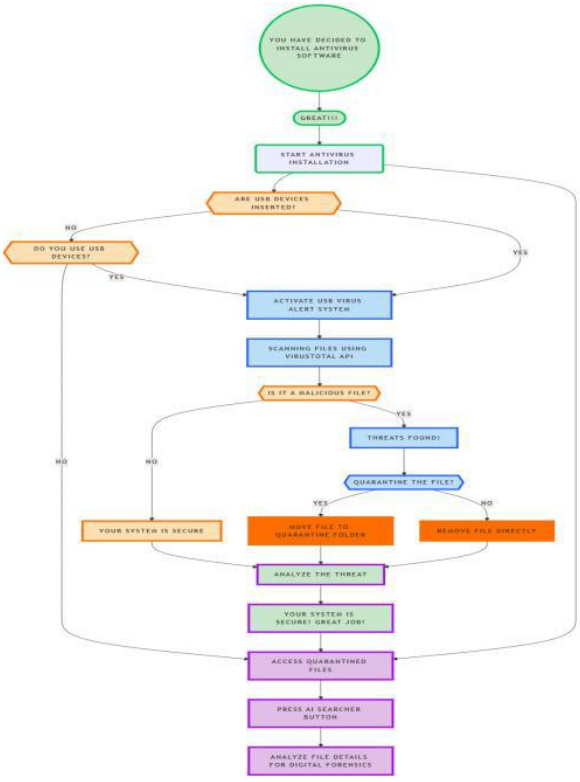

Figure 1: Flowchart

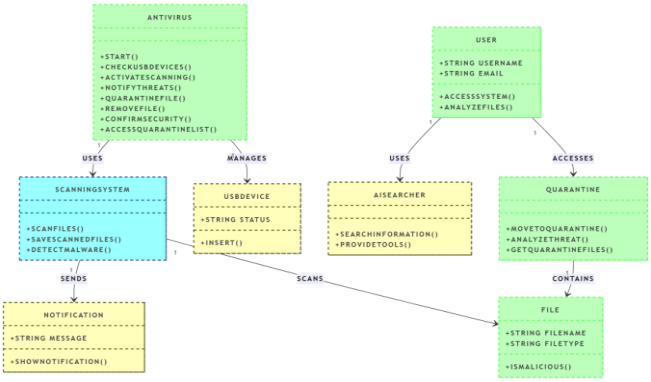

Figure 2: Class diagram

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 5, pp 278-283, May-2025

https://doi.org/10.47001/IRJIET/2025.905037

Figure 3: System interface

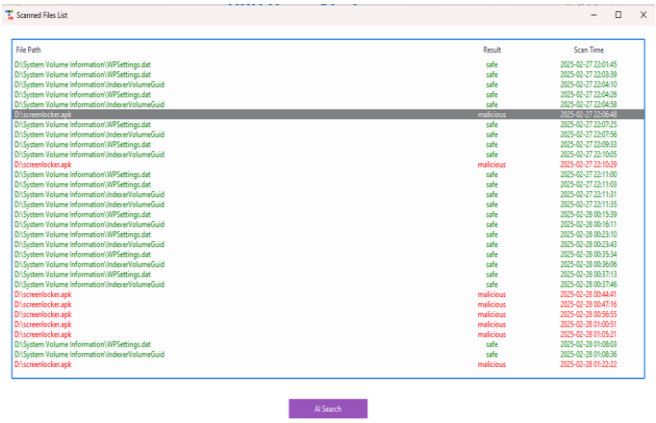

Figure 4: Scanned file list

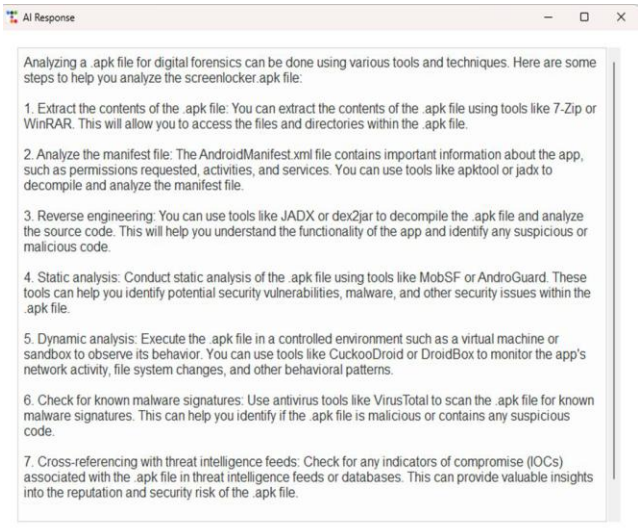

Figure 5: AI searching result

III. RESULTS AND DISCUSSION

USB Virus Alert System was developed in response to the spreading USB malware with the help of machine learning (ML) techniques and cloud threat intelligence. It was developed in Python. The ML models were trained using Scikit-learn and TensorFlow. By integrating Virus Total API, the system can analyze files against a global database of well-known threats.

The implementation phase concentrated on making sure that the system works as fast, reliable, and stable as possible in different operating systems like Windows, Linux, and macOS. Lightweight, the system runs without affecting the performance of the machine while operating silently in the background and offering real-time monitoring.

Prototype/Model

The prototype was designed to be user-friendly and efficient, allowing users to interact with the system easily. The graphical user interface (GUI) provides options for:

- Managing scans (manual or automatic scans upon USB insertion).
- Reviewing quarantine reports (listing detected threats and recommended actions).
- Configuring notifications (customizing alert preferences via email, desktop, or Telegram) [25].

The system was tested under various real-world conditions to ensure its effectiveness. The testing process included:

Functional Testing:

- Verifying that each module operates as expected.
- Ensuring seamless integration between the Virus Total API and ML detection models.

Performance Testing:

- Evaluating the system's ability to scan large USB devices efficiently.
- Ensuring minimal impact on system performance, even when running in the background.

Security Testing:

- Ensuring the system is resistant to external hacking attempts.
- Protecting stored logs and virus signatures from unauthorized access.
- The testing phase confirmed the system's capability to provide high accuracy in threat detection while maintaining optimal performance.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 5, pp 278-283, May-2025

https://doi.org/10.47001/IRJIET/2025.905037

Performance Evaluation

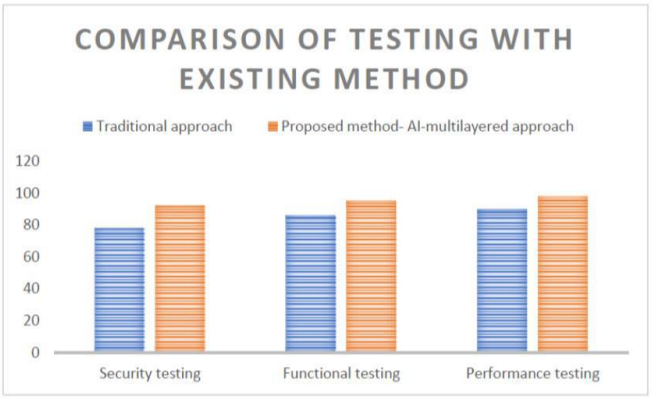

Figure 6: Comparison of Testing with Existing Approach

Figure 6 represents the comparison of different types of testing in proposed method with existing approaches. The USB Virus Alert System is, therefore, a timely and preventive apparatus against the growing threats of USB malware, which in current times have become a major vector for such attacks. Typical antivirus systems, which still rely on signature detection, are daily becoming less useful because of new tricks introduced by malware techniques. The justification for this piece of research is thus due to the urgent demand for a stronger, proactive, and versatile answer to offset.

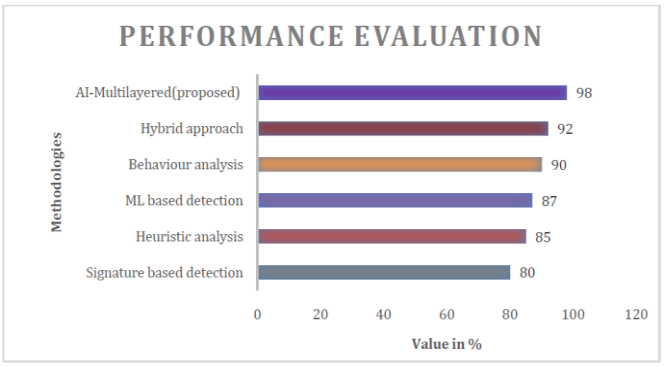

Figure 7: Performance evaluation of different methodologies with proposed method

It can be observed that the proposed method has high value of 98% when compared to existing methodologies. The USB Virus Alert System is a state-of-the-art contribution to cybersecurity, using real-time cloud-based analysis and machine learning algorithms to provide efficient malware detection. The following points illustrate its significance both academically and scientifically:

- Utilizing AI-driven behavioral analytics over the signature-based detection techniques in place.
- The reduced reliance on frequently updated virus signatures makes it more adaptable to the ever-evolving threats.
- Forms the basis for research on cyber-security in real-time USB security solutions.
- Presents a tangible application of AI and IoT in cyber security.
- Implementable in schools, offices, and government establishments.
- Establishes another layer of security in reducing USB-based cyber-attacks.

This provides a road map to creating a future development in USB security solutions by closing the gap between the traditional antivirus programs and AI-based cybersecurity.

Benefits to the Public

The USB Virus Alert System offers important cybersecurity protection for individuals, organizations, and governments everywhere by securing data from threats spread through USB devices. Key advantages include:

- **Enhanced Cyber Defense Across Different Sectors:** It protects critical digital systems in areas like government, education, healthcare, and business by detecting and stopping malware carried by USB drives.
- **Helps Meet International Security Requirements:** The system aids organizations in complying with global data protection rules, promoting responsible data handling and privacy.
- **Prevents Data Loss and Security Breaches:** By identifying harmful files transferred via USB devices, it safeguards sensitive information and prevents disruptions caused by malware.
- **Raises Awareness About USB Risks:** It encourages safe use of external storage, fostering secure habits in workplaces, schools, and homes.
- **Supports Technological Progress in Cybersecurity:** With AI-driven real-time detection, it keeps pace with evolving threats and helps build stronger, smarter security frameworks.

In summary, the USB Virus Alert System provides a vital layer of protection against USB-related cyber risks, helping create a safer digital environment for users worldwide.

IV. CONCLUSION

This work effectively showcases the power and potential of machine learning algorithms to enhance USB security. By utilizing AI-driven behavioral analysis rather than relying solely on traditional signature-based methods, it enables proactive detection and prevention of threats, thereby providing stronger protection for both personal and organizational data. The inclusion of real-time monitoring

ISSN (online): 2581-3048
Volume 9, Issue 5, pp 278-283, May-2025
https://doi.org/10.47001/IRJIET/2025.905037

capabilities, such as automated quarantine, further enhances the system's responsiveness to potential risks.

Overall, this work highlights the critical role of AI in advancing cybersecurity solutions by offering innovative and adaptable approaches to malware detection. The findings suggest that machine learning models can significantly reduce false alarms, increase detection accuracy, and deliver a dynamic defense against USB-borne threats. Given the constantly evolving nature of cyberattacks, integrating AI-powered security measures is essential for maintaining effective and resilient protection systems.

REFERENCES

[1] CrowdStrike. (2023). Real-time threat detection with behavioral analysis. Retrieved from https://www.crowdstrike.com
[2] Kaggle. (2023). Public malware dataset for cybersecurity research. Retrieved from https://www.kaggle.com
[3] Kaspersky Lab. (2022). USB threats in corporate environments. Retrieved from https://www.kaspersky.com
[4] Khan, A., et al. (2020). Deep learning for USB malware detection. International Journal of Computer Science, 15(2), 123–135.
[5] McAfee. (2023). Automated malware quarantine and reporting. Retrieved from https://www.mcafee.com
[6] McAfee Endpoint Security. (2022). Automatic quarantine and user notification features. Retrieved from https://www.mcafee.com
[7] Moskovitch, R., et al. (2008). Malware detection via behavioral analysis. Journal of Cybersecurity, 12(3), 45–60.
[8] Palanisamy, R., & Mathivanan, V. (2017). Performance metrics analysis for simulation protocols. Journal of Advanced Research in Dynamical and Control Systems (JARDCS), 18(Special Issue), 2449–2462.
[9] Palanisamy, R., & Mathivanan, V. (2019). Future algorithm for optimised path selection and detection in MANET. International Journal of Networking and Virtual Organisations, 21(2).
[10] Palo Alto Networks. (2021). Network traffic monitoring for malware detection. Retrieved from https://www.paloaltonetworks.com
[11] Palo Alto Networks. (2023). Network monitoring for USB malware detection. Retrieved from https://www.paloaltonetworks.com
[12] Python Software Foundation. (n.d.-a). Python psutil library documentation. Retrieved from https://psrutil.readthedocs.io/
[13] Python Software Foundation. (n.d.-b). Python smtplib library documentation. Retrieved from https://docs.python.org/3/library/smtplib.html
[14] Scikit-learn Developers. (n.d.). Scikit-learn: Machine learning in Python. Retrieved from https://scikit-learn.org/
[15] Scikit-learn. (2023). Machine learning for cybersecurity. Retrieved from https://scikit-learn.org
[16] Shabtai, R., Moskovitch, Y., Elovici, C., & Glezer, C. (2014). Machine learning for malware detection. In Machine Learning and Data Mining in Pattern Recognition (pp. 1–12). Springer, Berlin, Heidelberg.
[17] Smith, J. (2020). Cross-platform development: Tools and techniques. Journal of Software Engineering, 15(3), 45–60.
[18] Symantec. (2023). Internet security threat report. Retrieved from https://www.symantec.com
[19] Symantec. (2023). USB device threat analysis. Retrieved from https://www.symantec.com
[20] TensorFlow Developers. (n.d.). TensorFlow: An end-to-end open-source platform for machine learning. Retrieved from https://www.tensorflow.org/
[21] TensorFlow. (2023). Deep learning for threat detection. Retrieved from https://www.tensorflow.org
[22] VirusTotal API Documentation. (n.d.). Retrieved from https://developers.virustotal.com/
[23] VirusTotal. (2023). Malware detection and threat intelligence reports. Retrieved from https://www.virustotal.com/

Citation of this Article:

Abdul Aziz Abdullah Ali Al-Musalamy, Al-Yamama Salim Khalfan Al-Habsi, & Dr. Vimal Kumar Stephen. (2025). AI-Powered USB Virus Alert System for Enhanced Cybersecurity. *International Research Journal of Innovations in Engineering and Technology - IRJIET*, 9(5), 278-283. Article DOI https://doi.org/10.47001/IRJIET/2025.905037

****

