Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

AI-Based Real-Time System Monitoring and Threat Analysis Using SLM

Gowri Sankar.R
Department of Computer Networking
PSG Polytechnic College
Coimbatore, India

Kavin Prasath
Department of Computer Networking
PSG Polytechnic College
Coimbatore, India

Abstract - Cybersecurity threats are increasing rapidly due to malicious software, hidden background processes, and unauthorized network communication in modern computer systems. Traditional security tools often consume high system resources and fail to provide understandable explanations about detected threats. This research proposes an AI based cybersecurity monitoring system using Small Language Models for real time process analysis and threat detection on Windows systems. The proposed system monitors running applications, startup services, CPU and memory usage, executable file locations, and network communication activities. Behavioral information collected from processes is analyzed using a lightweight Small Language Model to identify suspicious activities, malware behavior, and unauthorized data sharing attempts. The system also provides explainable security analysis by describing why a process is considered dangerous and suggesting possible solutions to the user. The proposed model is lightweight, cost effective, and capable of local offline execution, making it suitable for educational research, personal cybersecurity monitoring, and low resource systems. This research demonstrates the practical integration of Artificial Intelligence, Cybersecurity, Network Security, and Explainable AI into a real time threat detection framework using Small Language Models.

Keywords - Cybersecurity, Small Language Models, Threat Detection, Process Monitoring, Malware Detection, personal cybersecurity monitoring, Network Security, Artificial Intelligence.

I. INTRODUCTION

The rapid growth of digital technology and internet connectivity has significantly increased cybersecurity threats in modern computer systems. Malicious software, hidden background processes, spyware, ransomware, and unauthorized network communication have become major security concerns for both personal and organizational environments. Traditional antivirus software and monitoring systems mainly depend on predefined signatures and rule based detection techniques, which may fail to identify newly emerging or unknown threats. In addition, many existing security tools do not provide understandable explanations regarding why a process is considered suspicious, making it difficult for normal users to understand potential security risks.

Background processes running within an operating system can consume system resources, access sensitive information, and communicate with external servers without user awareness. Some malicious applications disguise themselves as legitimate system processes, making manual detection difficult. Monitoring such activities requires continuous analysis of process behavior, network communication patterns, executable file locations, CPU and memory usage, startup services, and system permissions.

Fig 1 : Network Security

Recent advancements in Artificial Intelligence and Natural Language Processing have introduced Small Language Models as lightweight and efficient alternatives to Large Language Models. Small Language Models require fewer computational resources and can operate locally on low resource systems while still providing intelligent reasoning and explanation capabilities. This makes them suitable for real time cybersecurity applications where low latency, privacy, and offline execution are important requirements.

This research proposes an AI Based Real Time System Monitoring and Threat Analysis framework using Small Language Models for Windows systems. The proposed system continuously monitors background processes and network activities, analyzes suspicious behavior patterns, detects possible malware activity, and provides explainable security recommendations to the user. Unlike traditional security

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

systems, the proposed model focuses on Explainable Artificial Intelligence by generating human readable explanations about detected threats and suggesting possible mitigation methods.

The objective of this research is to develop a lightweight, intelligent, and user friendly cybersecurity monitoring system capable of improving threat awareness and assisting users in identifying suspicious system activities in real time..

II. PROBLEMS AND CHALLENGES IN THE DIGITAL WORLD

The rapid growth of digital systems, internet connectivity, and online services has significantly increased cybersecurity challenges in modern computing environments. Individuals and organizations rely heavily on computer systems for communication, data storage, financial transactions, and business operations. However, this dependency has also created opportunities for cybercriminals to exploit system vulnerabilities through malicious software and unauthorized activities.

One of the major cybersecurity threats is malware, which includes harmful software designed to damage systems, steal information, or gain unauthorized access to devices. Malware can operate silently in the background without the user's knowledge, making detection difficult. Spyware is another serious threat that secretly monitors user activities, collects sensitive information, and transfers data to external servers. Similarly, ransomware attacks encrypt important user files and demand payment for recovery, causing severe financial and operational losses.

Hidden background processes present another major challenge in computer systems. Many malicious applications disguise themselves as legitimate system processes and continue running invisibly while consuming system resources, monitoring user behavior, or communicating with unauthorized remote servers. These processes may perform suspicious activities such as accessing sensitive files, modifying system settings, or continuously transmitting data over the network.

Unauthorized data sharing and suspicious network communication have become increasingly common in modern systems. Applications may exchange user information with unknown external servers without proper user awareness or permission. Detecting such communication manually is difficult because users generally lack technical knowledge about network traffic, IP addresses, and system level processes.

Another important issue is the lack of cybersecurity awareness among normal users. Many users are unable to identify whether a process running in the background is safe or dangerous. Traditional antivirus systems often provide technical warnings without proper explanations, making it difficult for users to understand the actual threat and take corrective actions.

Although traditional antivirus software and security monitoring tools provide protection against known threats, they have several limitations. Most conventional systems depend heavily on signature based detection methods, which may fail to identify newly emerging or unknown attacks. In addition, many security solutions consume high system resources and may not provide explainable analysis regarding why a process is considered suspicious.

These challenges highlight the need for an intelligent, lightweight, and explainable cybersecurity monitoring system capable of analyzing background processes, detecting suspicious activities, monitoring network communication, and providing understandable threat explanations in real time.

Fig 2 : Malware Threat

III. PROBLEM STATEMENT

Modern computer systems are increasingly vulnerable to cybersecurity threats such as malware, spyware, ransomware, hidden background processes, and unauthorized network communication. Many malicious applications operate silently within the system while consuming resources, accessing sensitive information, and transmitting data without user awareness. Detecting such activities manually is difficult because most users lack technical knowledge regarding system processes and network behavior.

Existing antivirus software and security monitoring tools mainly rely on signature based detection techniques, which are effective only for previously known threats. These traditional systems often fail to identify newly emerging attacks, suspicious behavioral patterns, and disguised malicious processes. In addition, many security tools consume high computational resources and provide technical warnings without proper explanations, making it difficult for users to understand the nature of detected threats and take corrective actions.

Another major limitation of existing security systems is the lack of Explainable Artificial Intelligence capabilities. Most tools can identify suspicious activity but cannot clearly explain why a process is considered dangerous, what risks are involved, or how the issue can be resolved. This creates a gap between threat detection and user understanding.

To address these challenges, there is a need for a lightweight, intelligent, and explainable cybersecurity monitoring system capable of real time background process analysis, network monitoring, suspicious activity detection, and human readable threat explanation. The proposed research aims to fill this gap

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

by integrating Small Language Models with process monitoring and network analysis techniques to create an AI based real time threat analysis framework for Windows systems.

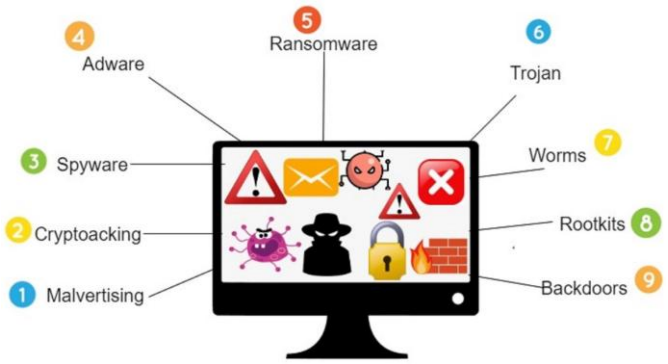

Fig 3 : Types of system Attack

IV. PROPOSED SOLUTION

To overcome the limitations of traditional cybersecurity monitoring systems, this research proposes an AI Based Real Time System Monitoring and Threat Analysis framework using Small Language Models for Windows operating systems. The proposed system is designed to continuously monitor background processes, analyze network communication activities, identify suspicious behavior patterns, and provide explainable security recommendations to users in real time.

The system integrates process monitoring techniques with Artificial Intelligence based threat analysis to create a lightweight and intelligent cybersecurity solution. Process monitoring is performed using system level monitoring libraries that collect information related to running applications, startup services, CPU and memory usage, executable file locations, active permissions, and process behavior. This allows the system to identify hidden or suspicious processes operating within the computer system.

In addition to process analysis, the proposed framework performs network monitoring to detect unauthorized communication between local applications and external servers. The system analyzes network traffic, connected IP addresses, data transfer behavior, and suspicious internet activity to identify possible data sharing attempts, spyware behavior, or malicious communication patterns.

A major component of the proposed solution is the integration of Small Language Models for intelligent threat reasoning and explanation generation. The Small Language Model analyzes the collected process and network information to determine whether a process is safe, suspicious, or potentially malicious. Unlike conventional antivirus systems, the proposed model provides Explainable Artificial Intelligence functionality by generating human readable explanations regarding detected threats, possible risks, and recommended mitigation steps.

The system also generates threat scores based on behavioral analysis and security indicators. Processes identified as suspicious are categorized according to their potential risk level, helping users understand the severity of detected threats. The proposed solution is lightweight, capable of local offline execution, and designed to operate efficiently on low resource systems without requiring large cloud based infrastructure.

By combining process monitoring, network analysis, Artificial Intelligence, and Explainable AI techniques, the proposed framework aims to improve cybersecurity awareness, real time threat detection capability, and user understanding of system level security threats.

Fig 4 : Hybrid AI

V. SYSTEM ARCHITECTURE

The proposed AI Based Real Time System Monitoring and Threat Analysis framework consists of multiple interconnected modules designed to monitor system activities, analyze suspicious behavior, and generate explainable cybersecurity reports. The architecture integrates process monitoring, network analysis, feature extraction, Small Language Model based reasoning, and threat reporting into a unified cybersecurity monitoring system.

The system continuously collects information from running processes and network communication channels within the Windows operating system. The collected information is processed and analyzed using Artificial Intelligence techniques to identify suspicious activities and possible security threats. The architecture is designed to operate in real time while maintaining low computational overhead and efficient local execution.

The overall workflow of the proposed system is shown below.

Windows Operating System
↓
Process Scanner
↓
Network Monitor
↓
Feature Extraction
↓
SLM Analyzer
↓
Threat Detection
↓

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Threat Scoring
↓
AI Security Report
↓
User Dashboard

Module Description

1. Process Scanner : The Process Scanner module continuously monitors running applications, startup services, CPU usage, memory consumption, executable file locations, and active system processes. This module identifies suspicious or hidden background activities within the operating system.

2. Network Monitor : The Network Monitor module analyzes active network communication, connected IP addresses, incoming and outgoing traffic, and unauthorized data transfer activities. This module helps detect suspicious internet communication and possible data sharing attempts.

3. Feature Extraction : The Feature Extraction module collects important behavioral information from processes and network activities, including resource usage, communication frequency, process location, permissions, and execution behavior. These features are prepared for AI based analysis.

4. SLM Analyzer : The Small Language Model Analyzer is responsible for intelligent threat reasoning and process evaluation. The SLM analyzes extracted behavioral features and determines whether a process is safe, suspicious.

5. Threat Detection and Scoring : This module classifies detected activities according to their threat level. Processes are assigned security risk scores such as Safe, Medium Risk, or Dangerous based on behavioral analysis and suspicious indicators.

6. AI Security Report and User Dashboard : The final module generates explainable security reports containing threat descriptions, possible risks, suspicious behavior explanations, and recommended mitigation steps. The User Dashboard displays monitoring results, threat scores, and real time security alerts in a user friendly interface.

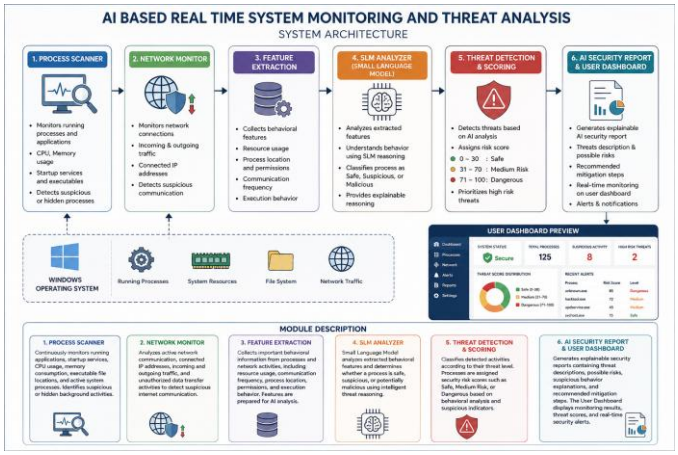

Fig 5 : Architecture

VI. METHODOLOGY

The proposed AI Based Real Time System Monitoring and Threat Analysis framework operates through multiple stages including process scanning, network monitoring, feature extraction, Small Language Model based threat reasoning, threat scoring, and report generation. The methodology is designed to continuously monitor system activities, identify suspicious behavior patterns, and provide explainable cybersecurity analysis in real time.

Initially, the system performs continuous process scanning within the Windows operating system. The process scanning module collects information regarding active applications, hidden background services, startup programs, CPU usage, memory consumption, executable file locations, and system permissions. This monitoring process helps identify abnormal or suspicious process behavior that may indicate malware activity.

Simultaneously, the network monitoring module analyzes incoming and outgoing network communication associated with running processes. The module monitors connected IP addresses, network ports, internet traffic frequency, and unauthorized data transfer activities. Suspicious communication with unknown external servers is treated as a potential security indicator.

After collecting process and network information, the Feature Extraction module processes the gathered data and extracts important behavioral attributes required for Artificial Intelligence based analysis. The extracted features include resource consumption patterns, execution behavior, file path location, startup activity, communication frequency, process privileges, and network interaction patterns.

The extracted features are then provided to the Small Language Model Analyzer. The Small Language Model performs intelligent reasoning on the collected behavioral data to determine whether a process is safe, suspicious, or potentially malicious. Unlike traditional rule based systems, the SLM can analyze multiple behavioral indicators simultaneously and generate human readable explanations regarding detected threats.

Following the analysis stage, the Threat Scoring module assigns security risk levels based on the severity of suspicious activities. Processes are categorized into different risk levels such as Safe, Medium Risk, or Dangerous. Threat scoring is determined using behavioral indicators including unusual resource usage, hidden execution patterns, suspicious network communication, unknown publishers, and unauthorized access attempts.

Finally, the Report Generation module creates explainable security reports for the user. The generated report contains process details, detected suspicious activities, possible security risks, and recommended mitigation steps. The results are displayed through a user friendly dashboard that provides real time monitoring information and threat alerts.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

The proposed methodology combines Cybersecurity, Artificial Intelligence, Network Monitoring, and Explainable AI techniques to provide an intelligent and lightweight threat detection framework suitable for modern computer systems.

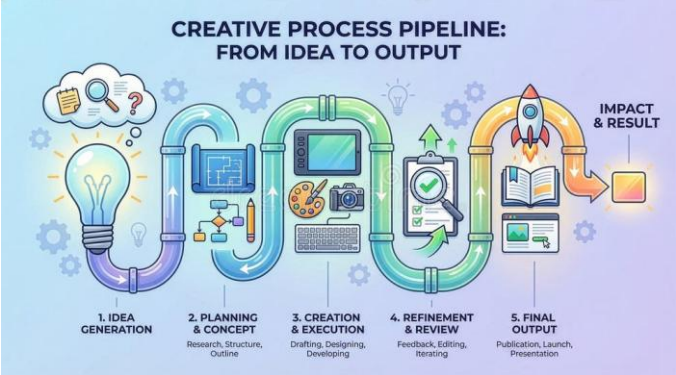

Fig 6 : Methodology Pipeline

VII. RESULTS AND ANALYSIS

The proposed AI Based Real Time System Monitoring and Threat Analysis system was tested on a Windows operating system environment to evaluate its ability to monitor background processes, analyze suspicious activities, and generate explainable security reports. The system successfully monitored running applications, detected abnormal process behavior, analyzed network communication patterns, and generated threat scores based on behavioral analysis.
During testing, the Process Scanner module continuously monitored active system processes including CPU usage, memory consumption, executable file locations, startup activities, and process permissions. The system successfully identified unknown background processes running from suspicious file locations such as temporary directories and unauthorized startup folders.

The Network Monitoring module analyzed incoming and outgoing communication associated with running processes. The system detected suspicious network activities including repeated communication with unknown IP addresses, continuous background data transfer, and unauthorized internet access attempts. These activities were treated as possible indicators of spyware or malware behavior.

The Small Language Model Analyzer successfully generated explainable threat analysis reports by interpreting collected behavioral information. Instead of providing only technical warnings, the system produced human readable explanations describing why a process was considered suspicious, possible risks involved, and recommended mitigation methods. This improved user understanding of detected cybersecurity threats.

Threat scoring was implemented to classify processes according to their security risk level. Processes were categorized as Safe, Medium Risk, or Dangerous based on behavioral indicators such as unusual resource consumption, hidden execution behavior, suspicious network communication, unknown publishers, and unauthorized access attempts.

Experimental observations showed that the proposed system operated efficiently with low resource consumption while maintaining real time monitoring capability. The lightweight Small Language Model architecture enabled local offline execution without requiring high computational infrastructure. The system demonstrated effective integration of Artificial Intelligence, Explainable AI, and Cybersecurity monitoring techniques for practical threat analysis.

Process Name	Suspicious Activity	Threat Score	Risk Level
chrome.exe	Normal browsing	10%	Safe
unknown.exe	Hidden execution	85%	Dangerous
mailmind.exe	External connection	70%	Medium Risk
system32.exe	High CPU usage	5%	Safe

TABLE I. PROCESS THREAT ANALYSIS RESULTS

Fig 7 : AI Monitoring

VIII. ADVANTAGES OF THE PROPOSED SYSTEM

The proposed AI Based Real Time System Monitoring and Threat Analysis framework provides several advantages compared to traditional cybersecurity monitoring systems. The integration of Small Language Models with process monitoring and network analysis techniques improves threat detection capability while maintaining lightweight system performance.

One of the major advantages of the proposed system is its lightweight architecture. Unlike large scale cloud based security systems, the proposed framework is designed to operate efficiently on low resource systems with minimal computational requirements. This makes the system suitable for personal computers, educational environments, and low configuration devices.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

The proposed system also supports local offline execution. Since the Small Language Model can operate locally without depending entirely on cloud infrastructure, the framework improves user privacy and reduces dependency on continuous internet connectivity. Offline execution also minimizes external data exposure during cybersecurity analysis.

Another important advantage is real time monitoring capability. The system continuously monitors background processes, startup services, CPU and memory usage, executable files, and network communication activities. This allows early detection of suspicious behavior and improves response time against potential threats.

The integration of Explainable Artificial Intelligence improves user understanding of cybersecurity threats. Instead of displaying only technical warnings, the proposed system generates human readable explanations describing why a process is considered suspicious, possible risks involved, and recommended mitigation steps. This increases cybersecurity awareness among users with limited technical knowledge.

The system also provides intelligent threat scoring based on behavioral analysis. Processes are categorized into different risk levels such as Safe, Medium Risk, and Dangerous, helping users quickly identify high risk activities within the system.

Another advantage of the proposed framework is its ability to combine multiple cybersecurity functions within a single platform. The system integrates process monitoring, network analysis, Artificial Intelligence based reasoning, threat scoring, and security report generation into one unified monitoring environment.

Overall, the proposed system offers a cost effective, explainable, lightweight, and intelligent cybersecurity monitoring solution capable of improving real time threat detection and user awareness in modern computer systems.

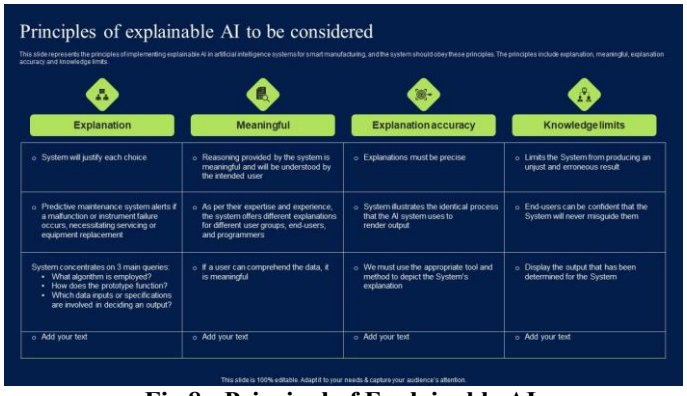

Fig 8 : Principal of Explainable AI

IX. FUTURE SCOPE

The proposed AI Based Real Time System Monitoring and Threat Analysis framework can be further enhanced with several advanced features and technologies in future developments. Although the current system focuses on lightweight real time monitoring and explainable threat analysis, future improvements can significantly increase its scalability, intelligence, and enterprise level security capabilities.

One possible enhancement is cloud integration for centralized cybersecurity monitoring and threat intelligence sharing. Cloud connectivity can allow the system to access real time malware databases, security updates, and global threat information for improved detection accuracy. Cloud based storage can also support centralized log management and remote security analysis.

Another important future improvement is automatic threat blocking and response capability. The current system mainly focuses on threat detection and explainable analysis, but future versions can automatically terminate suspicious processes, block unauthorized network communication, quarantine harmful files, and restrict malicious applications without requiring manual user intervention.

Mobile platform support can also be added in future implementations. The proposed framework may be extended to Android and mobile operating systems to monitor background applications, suspicious permissions, unauthorized data sharing, and abnormal mobile device behavior. This can improve cybersecurity protection across multiple platforms.

Fig 9 : Future Scope

Advanced malware detection techniques using Machine Learning and Deep Learning algorithms may further improve the system's ability to identify unknown and zero day attacks. Future models can incorporate behavioral learning, anomaly detection, and adaptive threat intelligence for more accurate cybersecurity analysis.

Another major future enhancement is integration with enterprise Security Operations Center environments. The proposed system can be expanded into a larger scale enterprise cybersecurity platform capable of centralized monitoring, real time alert management, incident response support, and AI assisted security analysis for organizational networks.

Future research may also focus on improving Explainable Artificial Intelligence capabilities by generating more detailed threat explanations, attack pattern visualization, and intelligent

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

cybersecurity recommendations for both technical and non technical users.

Overall, the proposed framework has significant future potential in the fields of Artificial Intelligence, Cybersecurity, Network Security, and intelligent threat analysis systems.

X. CONCLUSION

This research proposed an AI Based Real Time System Monitoring and Threat Analysis framework using Small Language Models for cybersecurity monitoring in Windows systems. The study addressed major cybersecurity challenges including hidden background processes, malware activity, unauthorized data sharing, suspicious network communication, and the limitations of traditional antivirus systems.

The system combines monitoring mechanisms with AI-driven analysis to improve threat detection and user understanding techniques to create a lightweight and intelligent cybersecurity monitoring solution. By continuously analyzing running processes, system behavior, and network activities, the system was able to identify suspicious behavior patterns and generate real time threat analysis reports.

Small Language Models played an important role in improving intelligent threat reasoning and explainable cybersecurity analysis. Unlike traditional security tools that provide only technical warnings, the proposed system generated human readable explanations describing detected threats, possible risks, and recommended mitigation methods. This improved user understanding and cybersecurity awareness.

The proposed system also demonstrated several advantages including lightweight architecture, offline execution capability, low resource consumption, real time monitoring, intelligent threat scoring, and explainable security reporting. These features make the framework suitable for educational research, personal cybersecurity monitoring, and low resource computing environments.

Fig 10 : Secured Digital Space

Future improvements such as cloud integration, automatic threat blocking, advanced malware detection, mobile platform support, and enterprise Security Operations Center integration can further enhance the capabilities of the system. Overall, the proposed research demonstrates the practical application of Small Language Models in modern cybersecurity systems and highlights their future potential in intelligent threat detection and explainable AI based security monitoring.

ACKNOWLEDGMENT

The authors express their sincere gratitude to Mrs. T.Rajashwari , Department of Computer Networking, PSG Polytechnic College, Coimbatore, for valuable guidance, encouragement, and continuous support throughout many research work. The authors also thank the department faculty members and friends for their support and suggestions.

REFERENCES

BOOKS :

[1] A. Vaswani et al., “Attention is all you need,” Advances in Neural Information Processing Systems, vol. 30, 2017.

[2] T. Brown et al., “Language Models are Few Shot Learners,” Advances in Neural Information Processing Systems, vol. 33, pp. 1877-1901, 2020.

[3] Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,” Nature, vol. 521, no. 7553, pp. 436-444, 2015.
[4] M. Ring, D. Landes, D. Wunderlich, and A. Hotho, “Flow based network traffic generation using Generative Adversarial Networks,” Computers and Security, vol. 82, pp. 156-172, 2019.

JOURNAL ARTICLES AND RESEARCH PAPERS:

[1] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA: MIT Press, 2016.

[2] W. Stallings, Network Security Essentials: Applications and Standards, 6th ed. Pearson Education, 2017.

[3] C. Bishop, Pattern Recognition and Machine Learning. Springer, 2006.

[4] O. Chapelle, B. Scholkopf, and A. Zien, Semi-Supervised Learning. MIT Press, 2010.

[5] S. Russell and P. Norvig, Artificial Intelligence: A Modern Approach, 4th ed. Pearson, 2020.

OFFICIAL WEBSITES AND DOCUMENTATION :

[1] Microsoft Corporation, “Windows Security and Threat Protection,” Available: https://learn.microsoft.com/

[2] Python Software Foundation, “Python Documentation,” Available: https://docs.python.org/3/

[2] Psutil Developers, “Psutil Documentation,” Available: https://psutil.readthedocs.io/

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

[3] Scapy Project, "Scapy Packet Manipulation Tool," Available: https://scapy.net/

[4] Meta AI, "LLaMA and Small Language Models," Available: https://ai.meta.com/

[5] Google AI, "Gemma Open Models," Available: https://ai.google.dev/gemma

[6] Microsoft Research, "Phi Language Models," Available: https://www.microsoft.com/en-us/research/

[7] National Institute of Standards and Technology, "Cybersecurity Framework," Available: https://www.nist.gov/cyberframework

[8] OWASP Foundation, "OWASP Top 10 Web Application Security Risks," Available: https://owasp.org/

[9] Ollama, "Running Language Models Locally," Available: https://ollama.com/