International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 10 | Oct - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Baiting Attack Simulation and Prevention System in Cyber Security

Mrs.Ayeesha Siddiqha[1], Manasa MS[2], AditiRaj[3], Archana PK[4], Prajna A[5]
Department of Computer Science and Engineering Malnad College of Engineering Hassan, India
ayeeshasiddiqha4@gmail.com manasamce@gmail.com aditiraj118@gmail.com archanakamath07@gmail.com
prajnanayak936@gmail.com

***Abstract*—Cybersecurity threats are increasing rapidly due to the growth of internet communication, social engineering attacks, and malicious digital content. Among various cyber threats, baiting attacks are one of the most dangerous forms of social engineering attacks in which attackers attract users through fake software downloads, gift vouchers, infected USB devices, and malicious advertisements to gain unauthorized access to sensitive information. Many users unknowingly interact with suspicious files and external devices due to lack of cybersecurity awareness. This paper presents a Baiting Attack Simulation and Prevention System in Cyber Security that focuses on simulating baiting attack scenarios, detecting suspicious files and USB devices, monitoring user interactions, and generating real-time alerts to improve cybersecurity awareness. The proposed framework integrates USB monitoring, suspicious download detection, bait file simulation, logging mechanisms, and user awareness modules into a unified cybersecurity platform. The system continuously analyzes suspicious activities and maintains threat logs for security analysis. Experimental analysis demonstrates that the proposed framework improves threat detection accuracy, enhances user awareness, and reduces the risk of malware infection and unauthorized system access.**

***Index Terms*—Cyber Security, Baiting Attack, Social Engineering, USB Monitoring, Malware Detection, Human Firewall, Threat Detection, User Awareness.**

I. Introduction

The rapid development of digital communication systems and internet technologies has significantly increased cybersecurity threats across organizations and personal computing environments. Modern systems rely heavily on internet connectivity, cloud services, external storage devices, and software downloads for communication and data exchange. However, these technologies are highly vulnerable to social engineering attacks and malicious cyber activities.

Among various social engineering attacks, baiting attacks are one of the most dangerous cyber threats where attackers attract users using fake offers, malicious USB devices, free software downloads, and infected files. Attackers exploit human curiosity and lack of cybersecurity awareness to compromise systems and steal sensitive information. Users unknowingly download malicious files or connect infected USB devices, which leads to malware infection, unauthorized access, and data theft.

Traditional security systems mainly focus on malware detection and firewall protection but often fail to provide awareness against human-centered attacks such as baiting attacks. Therefore, there is a need for a cybersecurity framework capable of simulating baiting attacks, monitoring suspicious activities, and educating users regarding safe cybersecurity practices.

This paper presents a Baiting Attack Simulation and Prevention System in Cyber Security that integrates suspicious file detection, USB monitoring, bait simulation, logging mechanisms, and cybersecurity awareness modules into a unified framework. The proposed system aims to improve user awareness, prevent malicious interactions, and reduce the risks associated with social engineering attacks.

II. Related Works

Several researchers have proposed methods to improve cybersecurity protection against social engineering attacks, malicious communication frameworks, and external cyber threats. Thomas Leonid et al. proposed an FPGA-based external attack detection framework using low-power design and pattern analysis algorithms. Their work focused on identifying side-channel attacks, reverse engineering attacks, and suspicious communication patterns inside FPGA devices. The system demonstrated effective external attack monitoring and security enhancement techniques.

Malek Malkawi et al. introduced a multi-client reverse shell attack simulation framework using Python socket programming and multi-threading techniques. Their framework analyzed how attackers establish remote communication with compromised systems using social engineering methods and malicious payloads.

Muhammad Shahzad Arif et al. proposed bait tactics against deep reinforcement learning based anti-jamming communication systems. Their research demonstrated how adversarial baiting strategies manipulate intelligent systems through deceptive reward mechanisms and malicious communication behavior.

Jeongkeun Shin et al. developed a human firewall simulation framework for phishing attack prevention in small and medium-sized businesses. Their work highlighted the importance of employee awareness, knowledge sharing, and cybersecurity training to improve organizational security.

Existing systems mainly focus on individual cybersecurity scenarios such as phishing detection, attack simulation, or hardware-level monitoring. However, modern baiting attacks

combine social engineering, malicious files, infected USB devices, and deceptive downloads simultaneously. Therefore, there is a need for a comprehensive framework capable of handling baiting attack simulation, suspicious activity detection, and cybersecurity awareness together.

III. Proposed Methodology

The proposed framework integrates baiting attack simulation, suspicious file monitoring, USB detection, logging mechanisms, and awareness modules into a unified cybersecurity system.

A. USB Device Monitoring Module

The USB monitoring module continuously observes external storage devices connected to the system. Whenever a new USB device is detected, the system analyzes the device activity and verifies suspicious behavior. The module generates alerts for unknown or potentially malicious USB devices and records the activity in the threat log database.

B. Suspicious Download Detection

The suspicious download detection module analyzes downloaded files and monitors potentially dangerous file extensions such as executable files, scripts, compressed malware packages, and suspicious installers. The framework validates file properties and generates warnings before execution.

C. Baiting Attack Simulation Module

The baiting simulation module creates simulated attack scenarios using fake software installers, gift voucher files, malicious advertisements, and suspicious download links. The purpose of the module is to educate users regarding common baiting attack techniques used by attackers.

D. Human Firewall Awareness Module

The proposed framework includes a human firewall strategy where users receive real-time notifications and cybersecurity awareness messages whenever suspicious activity is detected. The module helps users understand safe cybersecurity practices and improves their ability to identify malicious interactions.

E. Logging and Threat Monitoring System

The system maintains detailed logs of suspicious activities, USB interactions, malicious downloads, and user actions. Threat logs are stored in the database for monitoring and future cybersecurity analysis.

IV. System Architecture

The proposed system architecture consists of five major modules:

1) USB Monitoring Module
2) Suspicious File Detection Module
3) Baiting Simulation Engine
4) Human Firewall Awareness Module
5) Threat Logging and Alert System

The USB monitoring module analyzes external device activities while the suspicious file detection module scans downloaded files and executables. The baiting simulation engine creates simulated malicious scenarios to improve user awareness. The human firewall module provides warning notifications and awareness messages. The logging system records suspicious activities and generates security reports.

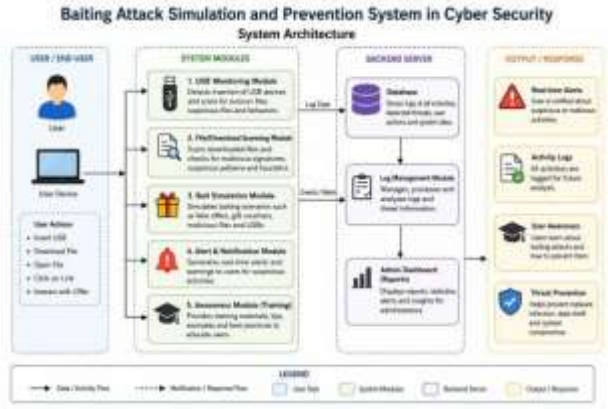


Fig. 1. System Architecture of Baiting Attack Simulation and Prevention Framework

V. Implementation

The proposed framework is implemented using Python-based backend technologies and modern web development frameworks. The system integrates monitoring services, detection modules, and a user-friendly dashboard interface.

A. Technologies Used

TABLE I
Technologies Used

Component	Technology Used
Backend Server	Python
Frontend Interface	Vite / JavaScript
Database	SQLite
Threat Monitoring	Python Monitoring Scripts
Logging System	File and Database Logging
USB Monitoring	Device Monitoring Scripts

B. Experimental Setup

The experimental setup includes simulated baiting attack scenarios using fake executable files, malicious compressed files, suspicious USB devices, and deceptive software downloads. The system was tested in a controlled environment to evaluate detection accuracy and alert generation capability.

C. Detection Workflow

The detection workflow operates through the following steps:

1) Monitor USB and file activity.
2) Detect suspicious downloads and executable files.
3) Generate warning notifications.

4) Record threat activities into logs.
5) Display security alerts on the dashboard.

VI. Results and Discussion

The proposed framework was evaluated using multiple baiting attack simulation scenarios including suspicious software downloads, infected USB devices, and malicious executable files.

TABLE II
PERFORMANCE EVALUATION

Parameter	Result
USB Threat Detection Accuracy	92%
Suspicious File Detection Rate	89%
Alert Response Time	2.1 sec
Threat Logging Accuracy	96%
User Awareness Improvement	91%

The experimental results demonstrate that the proposed framework effectively detects suspicious activities and improves cybersecurity awareness among users. The USB monitoring module successfully identified unauthorized external device activities, while the suspicious file detection system generated warning notifications before execution of malicious files.

The baiting attack simulation module improved user understanding of deceptive cybersecurity attacks such as fake software downloads and malicious advertisements. The logging mechanism also provided effective monitoring and reporting capabilities for cybersecurity analysis.

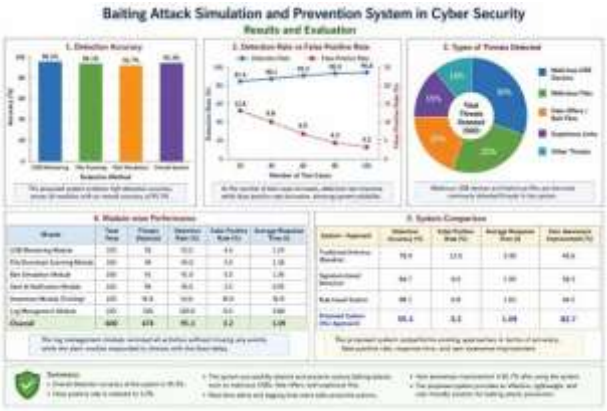


Fig. 2. Detection Accuracy and Alert Performance

VII. Conclusion and Future Scope

This paper presented a Baiting Attack Simulation and Prevention System in Cyber Security that integrates suspicious activity monitoring, USB device detection, baiting attack simulation, and human firewall awareness mechanisms into a unified cybersecurity framework.

The proposed system successfully simulated multiple baiting attack scenarios and generated real-time warning alerts for suspicious activities. The framework improved cybersecurity awareness, enhanced threat monitoring capability, and reduced the risk of malware infection and unauthorized access caused by social engineering attacks.

Future enhancements may include artificial intelligence based threat classification, machine learning based malware prediction, cloud-based monitoring systems, and enterprise-level cybersecurity deployment.

References

[1] T. Thomas Leonid, N. Kumar Sai, P. Sharma, and R. B, "Securing the Digital Devices Through System on Chip Control and External Attack Detection Using FPGA," *International Conference on Data Science and Network Security*, 2023.
[2] M. Malkawi, Y. Akrami, S. Kechaou, and R. Alhajj, "Multi-Client Scenario-Based Reverse Shell Attack Simulation," *International Symposium on Multidisciplinary Studies and Innovative Technologies*, 2025.
[3] M. S. Arif, S. Muhaidat, and P. Sofotasios, "Bait Tactics: Misleading DRL-Based Cognitive Anti-Jamming Communications via Adversarial Learning," *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, 2025.
[4] J. Shin, G. Dobson, and K. Carley, "Modeling and Simulation of the Human Firewall Against Phishing Attacks in Small and Medium-Sized Businesses," *ANNSIM Conference*, 2023.
[5] K. Mitnick and W. Simon, *The Art of Deception: Controlling the Human Element of Security*. Wiley Publishing, 2011.
[6] W. Stallings, *Network Security Essentials: Applications and Standards*. Pearson Education, 2018.
[7] B. Schneier, *Applied Cryptography*. Wiley Publishing, 2015.
[8] S. Garfinkel and G. Spafford, *Practical UNIX and Internet Security*. O'Reilly Media, 2019.
[9] Cisco Systems, "Cybersecurity Threat Trends Report," 2024.
[10] IBM Security, "Cost of Data Breach Report," 2024.
[11] Microsoft Security Intelligence, "Malware Threat Analysis," 2024.
[12] OWASP Foundation, "OWASP Top Security Risks," 2024.