International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 02 | Feb - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

An Adaptive Decoy-Based Security Framework Using Dynamic Honeypots and Fake Operating Environment

Isha P. Charjan
Diploma
Dept. Of Computer Engineering
Dr. PDGP, Amravati

Nidhi P. Wankhade
Diploma
Dept. Of Computer Engineering
Dr. PDGP, Amravati

Saket R. Bobade
Assistant Professor
Dept. Of Computer Engineering
Dr. PDGP, Amravati

Sumit M. Dhopte
H.O.D
Dept. Of Computer Engineering
Dr. PDGP, Amravati

Abstract — Traditional cybersecurity systems such as firewalls, antivirus software, and intrusion detection systems are mainly designed to block or detect attacks. However, in today's digital world, attackers use advanced techniques like ransomware, zero-day exploits, and advanced persistent threats that can bypass these traditional defenses. Honeypots were introduced as decoy systems to attract attackers and study their behavior without harming real systems. Although honeypots are useful, most of them are static and can be easily identified by experienced attackers. In this paper, an Adaptive Decoy-Based Security Framework is proposed that improves traditional honeypot systems by making them dynamic and behavior-based. The proposed system includes a Dynamic Fake Operating Environment (DFOE) that can change operating system fingerprints, services, and system behavior depending on how the attacker interacts with it. A Behavioral Deception Engine is used to analyze attacker activities and generate realistic responses. In addition, a Psychological Delay Mechanism is introduced to intentionally increase the attacker's time and effort. The main objective of this framework is not only to detect intrusions but also to mislead attackers, protect real infrastructure, and collect useful threat intelligence. This approach helps in transforming cybersecurity from passive defense to active deception.

Keywords: Honeypot, Deception Security, Dynamic Fake Environment, Adaptive Cybersecurity, Intrusion Detection.

1.INTRODUCTION

In today's digital era, cybersecurity has become one of the biggest concerns for organizations, businesses, and individuals. As technology continues to grow rapidly, cyber attackers are also becoming more advanced and intelligent. Attacks such as ransomware, phishing, data breaches, zero-day exploits, and advanced persistent threats (APTs) are increasing day by day. Traditional security systems like firewalls, antivirus software, and intrusion detection systems are mainly designed to block or detect known threats. However, these systems often fail when attackers use new or unknown techniques to bypass security mechanisms. To improve cybersecurity, researchers introduced the concept of deception technology. Instead of only protecting real systems, deception-based security creates fake systems or services that attract attackers. Honeypots are one of the most common examples of deception systems. A honeypot is a decoy system that appears vulnerable and attracts attackers so that their activities can be monitored and analyzed safely. This helps security teams understand attacker behavior without exposing real infrastructure.

Although honeypots are useful, most existing honeypot systems are static in nature. They use fixed configurations, fixed operating system fingerprints, and predefined responses. Skilled attackers can detect these honeypots by analyzing system behavior, network responses, or fingerprint inconsistencies. Once identified, attackers may avoid interacting with them, which reduces their effectiveness. To overcome these limitations, there is a need for a more intelligent and adaptive deception system.

This paper proposes an Adaptive Decoy-Based Security Framework that combines adaptive honeypots with a Dynamic Fake Operating Environment. The proposed system can modify operating system characteristics, simulated services, and system responses based on attacker interaction. It also introduces a Behavioral Deception Engine to analyze attacker activities and a Psychological Delay Mechanism to increase attacker effort and engagement time. The main objective of this research is to transform cybersecurity from passive protection into active deception. By intelligently misleading attackers and collecting valuable threat intelligence, the proposed framework aims to enhance overall system security while protecting real infrastructure from direct exposure.

2. RELATED WORK

Over the years, many cybersecurity techniques have been developed to protect systems from cyberattacks. Traditional security mechanisms such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and antivirus software are widely used to detect and block malicious activities. These systems mainly depend on predefined rules, signatures, or known attack patterns. Although they are effective against known threats, they often fail to detect new or advanced attacks such as zero-day exploits and advanced persistent threats.

To improve security, researchers introduced honeypots as deception-based systems. Honeypots are designed to attract attackers by appearing as real and vulnerable systems. They allow security teams to monitor attacker behavior without risking actual data or infrastructure. Honeypots are generally classified into low-interaction and high-interaction types. Low-interaction honeypots simulate limited services and are easier to manage, while high-interaction honeypots provide a more realistic environment but require more resources and monitoring.

With technological advancement, virtual honeypots and cloud-based honeypot systems were developed to improve scalability and flexibility. Some recent research has also focused on integrating machine learning techniques to analyze attacker behavior and classify threats more efficiently. Deception technology has also evolved to include fake databases, decoy credentials, and simulated network environments.

However, most existing honeypot systems are static and predictable. They use fixed configurations and do not change their behavior according to attacker actions. Skilled attackers can detect these honeypots by analyzing system fingerprints, response timing, or unrealistic service behavior. Many systems also focus only on logging attacker activities instead of actively adapting or misleading them. Therefore, there is a need for a more intelligent and adaptive deception-based security system that not only monitors attackers but also dynamically modifies the environment to increase realism and reduce detectability. The proposed framework aims to address this gap by introducing adaptive honeypots combined with a Dynamic Fake Operating Environment and behavioral analysis mechanisms.

3. PROPOSED FRAMEWORK

The proposed Adaptive Decoy-Based Security Framework is designed to improve cybersecurity by actively misleading attackers instead of only blocking them. The main idea of this framework is to redirect suspicious users into a controlled fake environment where their activities can be monitored safely without affecting the real system.

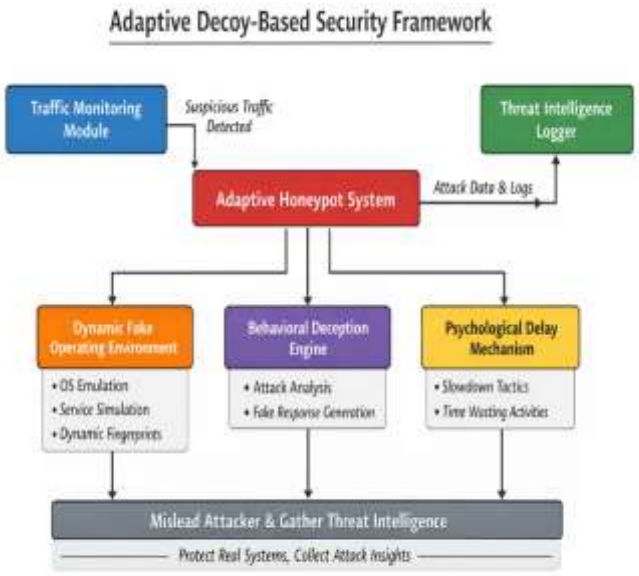
The framework consists of several important components. First, a Traffic Monitoring Module continuously observes incoming network traffic. This module analyzes user requests and identifies whether the traffic is normal or suspicious. If the traffic is legitimate, it is directed to the real server. However, if suspicious behavior is detected, the system redirects the user to an adaptive honeypot.

Once the attacker enters the honeypot, the Dynamic Fake Operating Environment (DFOE) becomes active. This environment simulates a real operating system such as Windows or Linux. It generates realistic system files, background processes, services, and vulnerabilities. Unlike traditional honeypots, this fake environment is not fixed. It can change its operating system fingerprint, open ports, and service responses based on how the attacker interacts with the system. This makes detection more difficult for skilled attackers.

Another important component of the framework is the Behavioral Deception Engine. This engine analyzes attacker activities such as scanning behavior, command usage, typing patterns, and exploit attempts. Based on this analysis, the system generates customized fake responses and simulated vulnerabilities. This helps in increasing realism and keeps the attacker engaged for a longer time.

The framework also includes a Psychological Delay Mechanism. This mechanism intentionally slows down certain operations, simulates large data transfers, or shows fake progress indicators. The purpose of this feature is to increase the attacker's time and effort, making the attack less efficient and more costly. All attacker activities inside the fake environment are recorded by the Threat Intelligence Logger. The collected information can later be used to improve firewall rules, update security policies, and understand new attack techniques.

Figure 1: - Decoy Security Model



4. SECURITY ANALYSIS

The proposed Adaptive Decoy-Based Security Framework improves system protection by shifting the focus from only blocking attacks to actively engaging and misleading attackers. In this model, suspicious traffic is redirected to a controlled honeypot environment, which ensures that the real server and actual data remain isolated and protected. Even if an attacker successfully gains access to the decoy system, no sensitive information or real services are exposed.

One of the main security advantages of this framework is the Dynamic Fake Operating Environment (DFOE). Traditional honeypots often use fixed configurations, which makes them easier to detect through fingerprint analysis or response pattern testing. In contrast, the proposed system dynamically changes operating system characteristics, service behavior, and vulnerability exposure based on attacker interaction. This reduces the possibility of honeypot detection and increases realism.

The Behavioral Deception Engine further enhances security by analyzing attacker activities in real time. By studying scanning patterns, command execution behavior, and exploit attempts, the system generates customized fake responses. This adaptive behavior makes the environment appear more genuine and prevents automated tools from quickly identifying it as a decoy.

The Psychological Delay Mechanism also plays an important role in strengthening security. By intentionally slowing down certain operations or simulating large amounts of fake data, the system increases the time and effort required by the attacker. This reduces the efficiency of the attack and discourages prolonged interaction.

However, the framework also has certain limitations. Since it involves dynamic simulation and behavioral analysis, it may require higher computational resources and proper system monitoring. Additionally, strong isolation mechanisms such as sandboxing and virtualization must be implemented to prevent attackers from escaping the fake environment.

Overall, the proposed framework provides stronger resilience against modern cyber threats compared to static honeypot systems. By combining adaptability, deception, and behavioral analysis, it enhances protection while safely collecting valuable threat intelligence.

5. CONCLUSION

In this paper, an Adaptive Decoy-Based Security Framework has been proposed to improve traditional cybersecurity mechanisms. Unlike conventional security systems that mainly focus on blocking or detecting attacks, the proposed approach actively engages and misleads attackers using adaptive honeypots and a Dynamic Fake Operating Environment. By continuously modifying system behavior, operating system fingerprints, and simulated services, the framework reduces the chances of honeypot detection.

The introduction of the Behavioral Deception Engine allows the system to analyze attacker activities and generate realistic responses, which increases authenticity and engagement time. In addition, the Psychological Delay Mechanism increases the attacker's effort and operational cost by intentionally slowing down certain actions. This makes the overall defense strategy more effective against modern cyber threats.

The proposed framework not only protects real infrastructure but also collects valuable threat intelligence that can be used to improve future security strategies. Although the system may require proper monitoring and computational resources, it provides a promising approach toward transforming cybersecurity from passive defense to active deception. With further development and real-world implementation, this model can contribute to stronger and more intelligent cyber defense systems.

6. REFERENCES

[1] L. Spitzner, *Honeypots: Tracking Hackers*, Addison-Wesley, 2003.

[2] N. Provos and T. Holz, *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*, Addison-Wesley, 2007.

[3] F. Cohen, "The Use of Deception Techniques in Computer Security," *Computers & Security*, vol. 17, no. 8, pp. 699–708, 1998.

[4] M. Bishop, *Computer Security: Art and Science*, Addison-Wesley, 2003.

[5] K. Seifert and J. Steenson, "A Taxonomy of Honeypots," in *Proceedings of the 2006 Workshop on Information Assurance*, 2006.

[6] S. M. Bellovin, "Security Problems in the TCP/IP Protocol Suite," *ACM Computer Communication Review*, vol. 19, no. 2, pp. 32–48, 1989.

[7] R. Mitchell and I. R. Chen, "A Survey of Intrusion Detection Techniques for Cyber-Physical Systems," *ACM Computing Surveys*, vol. 46, no. 4, 2014.

[8] The SANS Institute, "Deception Technology: The Next Generation of Cyber Defense," SANS White Paper, 2022.