IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

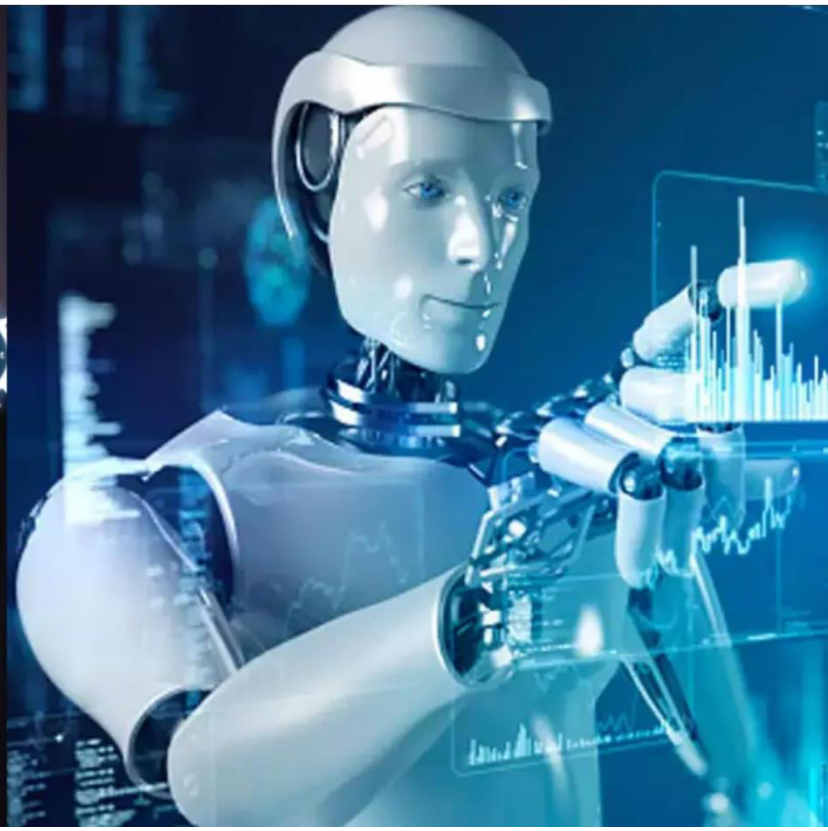
ISSN(O): 2319-8753
ISSN(P): 2347-6710



International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)





Impact Factor: 9.935

Volume 15, Issue 10, October 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 10, October 2026

|DOI: 10.15680/IJIRSET.2026.1510087|

AI Powered Adaptive Honeypot for Intelligent Cyber Attack Detection

Sakshi Pawade, Vijaya Shinde, Divya Badhe, Prof. Suryawanshi J. S

U.G. Student, Department of Computer Engineering, Samarth College of Engineering and Management, Belhe, Maharashtra, India

Associate Professor, Department of Computer Engineering, Samarth College of Engineering and Management, Belhe, Maharashtra, India

ABSTRACT: The increasing frequency and complexity of cyberattacks have become significant challenges for modern digital infrastructure, including computer networks, web applications, and cloud-based systems. Traditional intrusion detection mechanisms primarily rely on predefined rules and known attack signatures, which may limit their effectiveness in identifying previously unseen threats and evolving attack patterns. To address these limitations, this paper proposes an AI Powered Adaptive Honeypot for Intelligent Cyber Attack Detection, a defensive cybersecurity framework that integrates honeypot technology, machine learning-based behavioral analysis, and adaptive deception mechanisms. The proposed system deploys a controlled honeypot environment to simulate selected services and collect security-related information, including connection attempts, authentication failures, suspicious requests, source IP addresses, and interaction logs. The collected data is preprocessed, and relevant behavioral features are extracted for identifying anomalous activities and classifying potential cyber threats. An adaptive response mechanism modifies selected simulated service responses and monitoring strategies according to observed interactions and predefined security policies. Furthermore, a centralized web-based dashboard supports event visualization, threat classification, historical log analysis, and automated alert generation. The system aims to improve threat visibility, support the early identification of suspicious activities, and reduce dependence on manual security-log analysis. Its performance can be evaluated using metrics such as accuracy, precision, recall, false-positive rate, and detection time. The proposed framework is intended for controlled cybersecurity research environments, educational institutions, and organizational security monitoring. By combining intelligent behavioral analysis with adaptive deception, the system provides a foundation for developing more flexible and informative cyber threat detection solutions.

KEYWORDS: Adaptive Honeypot, Artificial Intelligence, Machine Learning, Cyber Attack Detection, Anomaly Detection, Intrusion Detection System, Threat Intelligence, Behavioral Analysis, Cybersecurity, Deception Technology.

I. INTRODUCTION

Cybersecurity has become a critical concern with the rapid growth of internet-based applications, cloud computing, digital services, and interconnected computer networks. Organizations increasingly depend on digital infrastructure to store and process sensitive information, making these systems potential targets for cyberattacks. Common threats include unauthorized access attempts, automated network scanning, credential attacks, malicious requests, and exploitation of vulnerable services. Traditional security mechanisms, such as firewalls and signature-based intrusion detection systems, play an important role in protecting digital assets. However, their dependence on predefined rules and known attack patterns can limit their ability to identify unfamiliar or continuously evolving threats.

Honeypot technology provides an additional approach to cybersecurity by creating controlled, simulated environments that attract and record suspicious interactions. These environments allow security researchers to observe potential attackers, collect relevant activity logs, and analyze their behavior without intentionally exposing critical production resources. Conventional honeypots, however, may rely on static configurations and basic logging mechanisms, which can restrict their ability to adapt to changing attack behavior or perform intelligent analysis of collected events.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 10, October 2026

|DOI: 10.15680/IJIRSET.2026.1510087|

To address these limitations, this paper proposes an **AI Powered Adaptive Honeypot for Intelligent Cyber Attack Detection**. The proposed framework integrates honeypot technology with artificial intelligence and machine learning techniques to improve the analysis of suspicious activities. The system collects security-related information, including source IP addresses, connection requests, authentication failures, suspicious commands, and service interaction logs. The collected information is then validated, preprocessed, and transformed into relevant behavioral features for identifying anomalous activities and classifying potential cyber threats. This approach aims to support the detection of suspicious behavior that may not be easily identified through conventional signature-based methods.

An important feature of the proposed framework is its adaptive response mechanism. Instead of relying entirely on fixed honeypot behavior, the system can modify selected simulated service responses and monitoring strategies according to observed interactions and predefined defensive policies. This allows the honeypot to collect more relevant information about potential attack patterns while maintaining controlled and isolated operating conditions. The system also incorporates automated alert generation, event storage, and a centralized web-based dashboard to support real-time monitoring and security analysis.

The proposed framework aims to provide security analysts with improved visibility into suspicious activities, reduce dependence on manual log examination, and support the investigation of emerging cyber threats. Its effectiveness can be assessed using performance measures such as accuracy, precision, recall, false-positive rate, and detection time. Proper isolation, access control, and responsible handling of collected security data remain essential for safe deployment.

The main contribution of this work is the integration of controlled honeypot-based event collection, machine learning-driven behavioral analysis, adaptive deception, and centralized threat visualization within a unified defensive cybersecurity framework. The system is intended for cybersecurity research laboratories, educational institutions, and organizations seeking to enhance their security monitoring capabilities. It is designed to complement existing security mechanisms rather than replace firewalls, intrusion prevention systems, or established incident response procedures.

II. LITERATURE SURVEY

Cybersecurity research has increasingly focused on improving the detection of sophisticated and previously unknown cyberattacks. Traditional intrusion detection systems primarily use predefined signatures and rules to identify known threats. Although these methods are effective for recognized attack patterns, they may struggle to detect new attack techniques and changing malicious behavior. Researchers have therefore explored honeypot technology, machine learning-based intrusion detection, anomaly detection, and adaptive deception as complementary approaches to improving cyber threat monitoring.

A. Traditional Intrusion Detection Systems

Traditional intrusion detection systems identify suspicious activities by comparing network traffic and system events against predefined rules or known attack signatures. These systems are useful for detecting established threats and generating security alerts. However, their effectiveness depends on regularly updated signatures and accurately configured detection rules. Unknown attacks and modified attack patterns may remain undetected, motivating the development of more adaptive detection approaches.

B. Honeypot-Based Cyber Threat Detection

Honeypots are controlled decoy environments designed to attract suspicious interactions and collect information about potential attackers. They provide opportunities to observe connection attempts, unauthorized access requests, authentication failures, and other security-related activities. Unlike conventional monitoring mechanisms, honeypots can collect information about interactions directed toward simulated services. However, traditional honeypots may use static configurations and basic logging techniques, limiting their ability to analyze complex behavioral patterns or adjust their responses dynamically.

C. Machine Learning for Cyber Attack Detection

Machine learning has become an important approach for analyzing network traffic and identifying suspicious activities. Classification algorithms can learn patterns from labeled security datasets, while anomaly detection techniques can identify deviations from expected behavior. These methods can support the identification of unusual

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 10, October 2026

|DOI: 10.15680/IJIRSET.2026.1510087|

connection patterns, repeated authentication failures, and potentially malicious requests. Nevertheless, detection performance depends on the quality of training data, feature selection, model configuration, and evaluation methods. Inaccurate classification can also produce false-positive alerts.

D. Adaptive Honeypot and Deception Techniques

Adaptive honeypot systems extend conventional honeypot functionality by modifying selected configurations, simulated responses, or monitoring strategies according to observed interactions. Such adaptation can help collect additional information about attacker behavior and improve the flexibility of defensive monitoring. However, adaptive mechanisms require carefully designed policies, controlled execution, and strong isolation to prevent unintended effects on legitimate systems or external networks.

E. Integrated AI-Based Threat Monitoring

Integrating machine learning with honeypot technology provides an opportunity to combine controlled threat observation with automated behavioral analysis. A unified system can collect interaction logs, preprocess security events, classify suspicious activities, generate alerts, and present threat information through a centralized dashboard. Such integration can reduce dependence on manual log examination and improve visibility into recurring attack patterns. However, the practical effectiveness of an integrated framework must be established through controlled experiments and comparison with appropriate baseline detection methods.

F. Research Gap

The reviewed approaches highlight the need for a defensive cybersecurity framework that combines honeypot-based event collection, machine learning-driven behavioral analysis, adaptive response mechanisms, and centralized monitoring. Traditional detection systems may be limited by predefined signatures, while basic honeypots may lack intelligent analysis and dynamic behavior. The proposed AI Powered Adaptive Honeypot for Intelligent Cyber Attack Detection addresses this research gap by integrating these capabilities within a controlled environment. Its performance can be evaluated using accuracy, precision, recall, false-positive rate, and detection time to determine its effectiveness in identifying suspicious activities.

III. METHODOLOGY

The proposed AI Powered Adaptive Honeypot for Intelligent Cyber Attack Detection follows a systematic methodology that combines controlled honeypot deployment, security event collection, data preprocessing, machine learning-based threat detection, adaptive response selection, and centralized monitoring. The methodology is designed to identify suspicious activities, analyze potential attack patterns, and provide useful threat intelligence while maintaining a secure and isolated environment.

A. Honeypot Environment Configuration

The first stage involves configuring a controlled honeypot environment with simulated services that can attract and record suspicious interactions. The environment is designed to observe incoming connections, authentication attempts, service requests, and other security-related activities. Isolation and access-control mechanisms are maintained to prevent the honeypot from affecting production systems or external networks.

B. Security Event Collection

The honeypot records relevant information generated during interactions with its simulated services. The collected data includes source IP addresses, connection attempts, authentication failures, suspicious requests, command interactions, timestamps, and network activity logs. These events are stored for further analysis and historical investigation.

C. Data Preprocessing and Feature Extraction

The collected event data is validated and preprocessed before being passed to the detection module. This stage involves handling incomplete records, removing duplicate entries where appropriate, normalizing data fields, and organizing events into a consistent format. Relevant behavioral features, such as connection frequency, repeated authentication failures, request patterns, and interaction sequences, are extracted to support threat analysis.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 10, October 2026

|DOI: 10.15680/IJIRSET.2026.1510087|

D. AI-Based Threat Detection

The processed data is analyzed using suitable machine learning techniques to identify abnormal behavior and classify potential cyber threats. The detection module examines the extracted features to identify suspicious patterns that may indicate unauthorized access attempts, automated scanning, or other potentially malicious activities. The classification results are treated as indicators for further investigation rather than definitive proof of malicious intent.

E. Event Risk Scoring and Adaptive Response

After threat analysis, detected events can be assigned risk levels according to their characteristics and predefined security policies. Based on the observed behavior and assigned risk level, the adaptive response module can modify selected simulated service responses or monitoring strategies. This process aims to improve the collection of relevant threat information while ensuring that responses remain controlled, reversible, and isolated.

F. Alert Generation and Event Storage

When an event satisfies the configured threat-detection criteria, the system generates an alert containing relevant event information and its classification. The associated records and analysis results are stored for later investigation, reporting, and performance evaluation. This process supports timely identification of potentially significant security events and reduces dependence on exclusively manual log analysis.

G. Web-Based Monitoring Dashboard

A centralized web-based dashboard presents collected events, detected threat categories, risk levels, historical activity, and security alerts. The dashboard enables authorized users to monitor system activity, examine suspicious interactions, and review changes in observed attack patterns. Visual summaries support the interpretation of detection results and facilitate security analysis.

H. Performance Evaluation

The proposed system can be evaluated through controlled experiments using suitable security datasets and authorized test scenarios. Its performance is assessed using detection accuracy, precision, recall, false-positive rate, and detection time. The results can be compared with an appropriate baseline detection method to determine whether integrating machine learning and adaptive honeypot techniques provides measurable improvements. Experimental values must be obtained from actual testing rather than assumed in advance.

Overall, the methodology integrates event collection, intelligent behavioral analysis, adaptive deception, automated alerting, and centralized visualization into a unified defensive cybersecurity framework. The effectiveness of the system depends on the quality of collected data, the suitability of the selected machine learning model, the reliability of adaptive policies, and the security of the deployment environment.

IV. PROBLEM DEFINITION AND OBJECTIVES

A. Problem Definition

The continuous growth of cyberattacks has created significant challenges for existing cybersecurity systems. Traditional intrusion detection mechanisms primarily depend on predefined rules and known attack signatures, which may limit their ability to identify previously unseen threats and evolving attack patterns. Additionally, conventional honeypot systems often focus on collecting security logs without providing advanced behavioral analysis or adapting their responses according to observed interactions. Manual examination of large volumes of security events can further delay threat identification and investigation.

Therefore, there is a need for an intelligent and adaptive cybersecurity framework that integrates honeypot technology, machine learning-based threat detection, behavioral analysis, and automated alert generation. The proposed AI Powered Adaptive Honeypot for Intelligent Cyber Attack Detection aims to address these challenges by collecting suspicious interaction data, identifying abnormal behavior, classifying potential cyber threats, and adapting selected simulated service responses according to predefined security policies. A centralized monitoring dashboard provides event visualization and historical analysis to support security investigation while maintaining a controlled and isolated environment.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 10, October 2026

|DOI: 10.15680/IJIRSET.2026.1510087|

B. Objectives

The primary objective of this research is to develop an AI-powered adaptive honeypot framework for intelligent cyberattack detection and defensive security monitoring.

The specific objectives are as follows:

1. To design a controlled honeypot environment that simulates selected services for observing suspicious cyber activities.
2. To collect and store security-related information, including connection attempts, authentication failures, suspicious requests, and interaction logs.
3. To preprocess collected event data and extract relevant behavioral features for intelligent threat analysis.
4. To apply suitable machine learning techniques for detecting anomalous activities and classifying potential cyber threats.
5. To implement an adaptive response mechanism that modifies selected honeypot responses based on observed behavior and predefined defensive policies.
6. To generate automated security alerts and maintain historical records for further investigation.
7. To develop a centralized web-based dashboard for monitoring suspicious events, threat classifications, risk levels, and attack trends.
8. To evaluate system performance using accuracy, precision, recall, false-positive rate, and detection time.
9. To maintain secure deployment through appropriate isolation, access control, and responsible handling of collected security data.

The proposed system aims to combine intelligent threat analysis with adaptive deception to improve security-event visibility and support the early identification of suspicious activities. Its effectiveness will be determined through controlled testing and comparison with suitable baseline detection methods.

V. SYSTEM ARCHITECTURE

The proposed system architecture consists of multiple interconnected layers that work together to capture suspicious network activity, analyze potential cyber threats using artificial intelligence and machine learning, and perform adaptive security responses. The architecture includes the network layer, honeypot layer, data processing layer, detection and analysis layer, response management layer, data storage layer, notification layer, and administrator interface.

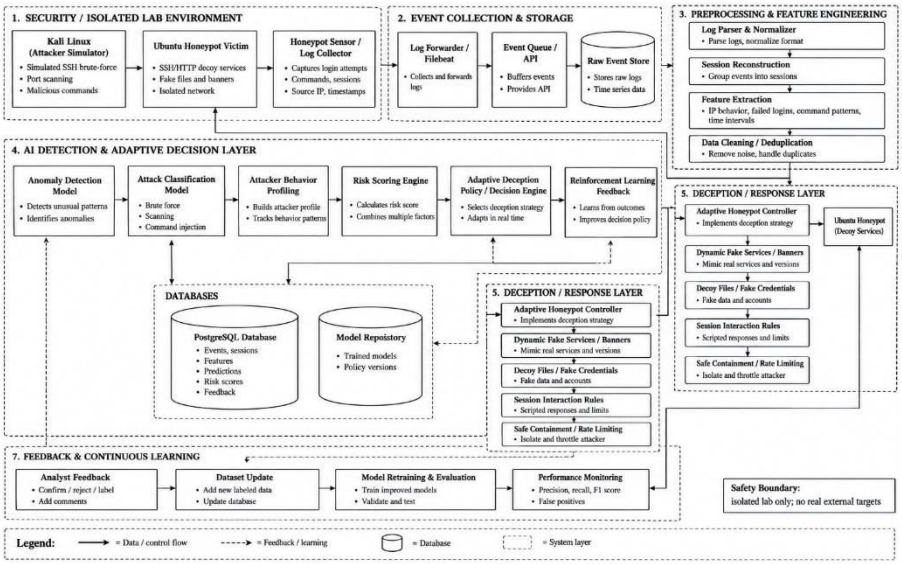


Figure 5.1: Overall System Architecture of AI-Powered Adaptive Honeypot

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 10, October 2026

|DOI: 10.15680/IJIRSET.2026.1510087|

1. External Users / Attackers

- This layer represents external users or potential attackers who interact with the network. Their activities may include port scanning, exploitation attempts, brute-force attacks, and suspicious network traffic. These interactions provide the initial input for the system. The honeypot is designed to observe such activities in a controlled environment without intentionally exposing actual production services.

2. Network Layer

- The network layer manages incoming traffic between external users and the honeypot environment. It consists of the internet connection and a firewall that filters network traffic according to configured security rules. The firewall helps restrict unwanted connections and controls which traffic can reach the honeypot server.

3. Honeypot Layer (Decoy Environment)

- The honeypot layer contains the honeypot server and multiple simulated services, including:
- Web honeypot
- SSH honeypot
- FTP honeypot
- Database honeypot
- Custom honeypot
- These services are designed to attract and record suspicious interactions. The honeypot server captures information about connection attempts, authentication failures, requests, and other activities. The collected event data is forwarded to the data processing layer for further analysis.

4. Data Processing Layer

- This layer prepares collected event data for machine learning-based analysis. It consists of three main components:
- Data Collector: Receives and organizes event information captured by the honeypot.
- Preprocessing Module: Performs data cleaning, filtering, feature extraction, and normalization.
- Feature Vector: Represents the processed event information in a structured format suitable for the detection model.
- The resulting feature vectors are transferred to the detection and analysis layer.

5. Detection and Analysis Layer (AI/ML)

- This is the main intelligence component of the proposed system. It analyzes processed security events to identify abnormal activities and classify potential threats.
- The layer includes the following modules:
- Historical Data: Provides previously collected or prepared training data for developing the machine learning model.
- Model Training: Trains the model, supports model updates, and stores the trained model.
- Trained Model: Supplies the learned patterns used for threat analysis.
- Real-Time Threat Analysis: Examines incoming feature vectors, predicts potential threat types, calculates risk scores, and supports anomaly detection.
- Threat Classification: Categorizes detected activities as normal, suspicious, or malicious.
- Risk Scoring: Assigns low, medium, or high risk levels to help prioritize security events.
- The detection results are forwarded to the response management layer. Logs and results can also be stored for future analysis, while model updates can use suitable historical data and validated results.

6. Response Management Layer

- This layer determines the actions to be taken based on the detection results. It contains three main modules.
- Adaptive Response: Performs configured defensive actions, such as blocking a source IP address, deploying additional decoy services, or updating honeypot configurations. These actions must be authorized, carefully controlled, and reversible.
- Alert Generation: Generates security alerts, notifies administrators, and records potential incidents for investigation.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 10, October 2026

|DOI: 10.15680/IJIRSET.2026.1510087|

- Rule Update: Updates configured security rules and supports adaptive learning based on validated observations and approved policies.
- This layer helps the system respond to suspicious activities while maintaining control over the honeypot environment.

7. Data Storage Layer

- The data storage layer maintains information required for detection, monitoring, and historical analysis. It contains three databases.
- Event Log Database: Stores captured traffic information, event logs, and system logs.
- Model Database: Stores trained models, model parameters, and model history.
- Threat Intelligence Database: Stores information about known threats, attack signatures, and IP reputation data.
- These databases support event investigation, model management, and threat analysis. Historical records can also help evaluate system performance and improve future model versions.

8. Notification Layer

- The notification layer communicates important security events to administrators and security analysts. It supports three notification mechanisms:
- Email Notification: Sends security alerts and event summaries through email.
- SMS Notification: Delivers important alerts through text messages.
- Push Notification: Provides alerts through supported applications or notification services.
- The notification layer receives alert details from the response management process and forwards relevant notifications and reports to the administrator interface.

9. Administrator / Security Analyst

- The administrator or security analyst interacts with the system through the monitoring interface. The main responsibilities include:
- Viewing generated security alerts.
- Analyzing captured attack logs.
- Monitoring honeypot status.
- Managing honeypot configurations.
- Reviewing and updating security rules and machine learning models.
- Examining notifications, reports, and historical threat information.
- This layer provides human oversight, enabling administrators to investigate detection results and verify whether further defensive action is required.

Overall working of the system

The complete workflow follows these steps:

1. External users generate network traffic that reaches the configured network security controls.
2. The firewall filters traffic according to its configured rules and permits relevant traffic to reach the honeypot environment.
3. The honeypot services capture suspicious interactions and generate event logs.
4. The data collector receives the logs, and the preprocessing module cleans the data and extracts relevant features.
5. The trained AI/ML model analyzes the feature vectors and identifies potential threats.
6. The threat classification module categorizes events, and the risk-scoring module assigns a risk level.
7. The response management layer selects configured adaptive responses, generates alerts, and records incidents.
8. Event records, model information, and threat intelligence are stored in their respective databases.
9. The notification layer sends relevant alerts and reports to the administrator or security analyst.
10. The administrator reviews the results and may approve configuration changes or model updates based on the available evidence.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 10, October 2026

|DOI: 10.15680/IJIRSET.2026.1510087|

VI. DATA PREPROCESSING

Data preprocessing is an essential stage in the proposed AI Powered Adaptive Honeypot for Intelligent Cyber Attack Detection. The primary purpose of this stage is to transform raw security events collected from honeypot services into a structured and consistent format suitable for machine learning-based threat detection. The collected data may contain incomplete records, duplicate events, inconsistent values, and irrelevant information that can affect the accuracy of threat analysis. Therefore, appropriate preprocessing techniques are applied before the data is passed to the detection and analysis layer.

A. Data Collection

The system collects security-related information from the honeypot environment, including source IP addresses, timestamps, connection attempts, authentication failures, suspicious requests, service interactions, and event logs. These records provide information about the behavior of users interacting with simulated web, SSH, FTP, database, and custom services.

B. Data Cleaning and Validation

The collected event records are checked for missing values, invalid fields, inconsistent formats, and duplicate entries. Incomplete records are handled according to predefined validation rules, while duplicate events are removed when appropriate. Data validation ensures that only records meeting the required quality criteria are forwarded for further processing.

C. Data Filtering

The filtering process removes irrelevant information and selects event records useful for cybersecurity analysis. Events can be grouped according to service type, connection patterns, authentication failures, and suspicious request characteristics. This step helps reduce unnecessary information and focuses the analysis on relevant security activities.

D. Feature Extraction

Feature extraction converts raw event logs into meaningful attributes that can be analyzed by the machine learning model. The selected features may include connection frequency, number of failed authentication attempts, request patterns, event duration, source information, and repeated interactions with honeypot services. These features help the detection engine identify deviations from expected behavior and recognize potential attack patterns.

E. Data Normalization and Encoding

Numerical features may have different ranges, which can affect certain machine learning algorithms. Normalization or standardization can therefore be applied where appropriate. Categorical attributes, such as service type and event category, may be converted into numerical representations required by the selected model. The preprocessing approach depends on the algorithm and the characteristics of the collected dataset.

F. Feature Vector Generation

After cleaning, filtering, feature extraction, and transformation, the processed information is represented as feature vectors. Each feature vector describes relevant characteristics of a recorded security event and serves as input to the AI/ML detection engine. These vectors are used to identify anomalous behavior, classify potential threats, and calculate event risk levels.

G. Dataset Preparation and Storage

Where supervised machine learning is used, labeled data is prepared to support model training and evaluation. The dataset can be divided into training, validation, and testing subsets to assess model performance. Data leakage must be avoided by ensuring that information from the test set does not influence training or preprocessing decisions. Processed event records, extracted features, and relevant metadata can be stored for historical analysis and model evaluation.

Overall, the data preprocessing stage improves the consistency and usability of security event data before machine learning analysis. By applying data cleaning, filtering, feature extraction, normalization, and feature vector generation, the proposed system prepares relevant information for intelligent cyber threat detection. The quality of this stage directly influences the reliability of subsequent threat classification, risk scoring, and adaptive response decisions.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 10, October 2026

|DOI: 10.15680/IJIRSET.2026.1510087|

VII. CONCLUSION

The proposed AI Powered Adaptive Honeypot for Intelligent Cyber Attack Detection presents an integrated approach to improving cybersecurity monitoring through honeypot technology, artificial intelligence, and machine learning. The system is designed to capture suspicious interactions within a controlled environment, preprocess collected security events, identify abnormal behavior, and classify potential cyber threats. By incorporating risk scoring, adaptive response mechanisms, automated alert generation, and centralized monitoring, the framework aims to provide better visibility into suspicious activities and support timely security investigation.

The integration of machine learning-based behavioral analysis with adaptive honeypot techniques offers a flexible approach to observing changing attack patterns. The web-based dashboard and event storage components further support historical analysis, threat monitoring, and security reporting. However, the reliability of the proposed system depends on the quality of collected data, the suitability of the selected machine learning model, and the effectiveness of the implemented security policies. Appropriate isolation, access controls, and responsible handling of security information are also essential for safe operation.

Future work can focus on evaluating the framework using real-world or publicly available cybersecurity datasets, comparing different machine learning algorithms, reducing false-positive detections, and improving the adaptability of simulated services. Integration with security information and event management (SIEM) platforms and additional threat intelligence sources could further enhance its capabilities. Overall, the proposed framework provides a foundation for developing intelligent and adaptive defensive cybersecurity solutions, with its practical effectiveness to be established through systematic testing and experimental evaluation.

REFERENCES

[1] W. Fan, F. Du, Z. Wang, Q. Cao, L. Liu, K. Chang, and S.-Y. Chang, “HoneyLLMd: A Large Language Model-Powered Adaptive Honeypot System,” *IEEE Transactions on Network Science and Engineering*, vol. 13, pp. 8646–8665, 2026, doi: 10.1109/TNSE.2026.3683862.

[2] N. Moukafih, A. P. R. Sabapathy, A. Murillo, and S. Motoyoshi, “Adaptive Agentic Honeypots: Decoupling Simulation from Reasoning for Robust Cyber Deception,” in *Proc. IEEE 50th Annual Computers, Software, and Applications Conference (COMPSAC)*, 2026, pp. 635–640, doi: 10.1109/COMPSAC69091.2026.00089.

[3] N. Ahmed, K. Uddin, J. Son, and D. Kim, “A Stability Testing Framework for Machine Learning in Honeypot Traffic Classification,” in *Proc. IEEE 12th Conference on Big Data Security on Cloud (BigDataSecurity)*, 2026, pp. 66–71, doi: 10.1109/BigDataSecurity69476.2026.00017.

[4] “Cloud-Deployed Adaptive SSH Honeypot with Reinforcement Learning and LLM-based Dynamic Response Generation,” in *Proc. International Conference on Secure Information Systems and Technologies (ICSIST)*, 2026, doi: 10.1109/ICSIST70215.2026.11705925.

[5] “Learning-Based Internet of Things Honeypots for Cyber Deception,” *IEEE Security & Privacy*, 2025, pp. 2–10, doi: 10.1109/MSEC.2025.3601986.

[6] “Smart Grid Intrusion Detection for IEC 60870-5-104 With Feature Optimization, Privacy Protection, and Honeypot-Firewall Integration,” *IEEE Access*, vol. 13, pp. 128938–128958, 2025, doi: 10.1109/ACCESS.2025.3590151.

[7] “Leveraging Artificial Intelligence for Enhancing Real-Time Honeypot Security,” in *Proc. 4th International Conference on Computing and Information Technology (ICCIT)*, 2025, doi: 10.1109/ICCIT63348.2025.10989357.

[8] “Beekeeper: Accelerating Honeypot Analysis With LLM-Driven Feedback,” *IEEE Access*, vol. 13, pp. 168034–168054, 2025, doi: 10.1109/ACCESS.2025.3613118.



INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details