International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

A Conceptual Framework for Leveraging Artificial Intelligence in Proactive Threat Detection in Cybersecurity

Mohammed Awad Mohammed Ataelfadiel*

Submitted: 16/08/2022 **Accepted:** 22/11/2022

Abstract*:* A conceptual framework is introduced, leveraging artificial intelligence (AI) techniques, including machine learning (ML) and behavioral analysis, to enable proactive threat detection in cybersecurity. This framework addresses the increasing complexity of modern cyber threats by integrating critical components such as anomaly detection, threat intelligence, user behavior analysis, and automated response systems. These components are designed to function collaboratively, providing an adaptive and resilient defense mechanism capable of detecting and mitigating a wide spectrum of cyber threats in real time.

Although the primary focus of this research is the theoretical development of the framework, it highlights the pivotal role of real-time threat intelligence integration in enhancing the system's capacity to respond to emerging threats. This integration facilitates the creation of a dynamic and proactive defense strategy, positioning the framework as a viable solution for organizations aiming to enhance their cybersecurity posture in the face of an evolving threat landscape.

Future research will involve empirical validation of the framework in real-world environments, such as smart cities and enterprise networks, to assess its effectiveness and scalability. Key areas of investigation will include the efficiency of data processing, resilience to adversarial attacks, and the scalability of the model. This framework serves as a foundation for advancing AI-driven cybersecurity solutions, providing organizations with a robust mechanism to counter sophisticated and continuously evolving cyber threats.

Keywords: *Cybersecurity, Machine Learning, Deep Learning, Anomaly Detection, Threat Intelligence, Proactive Defense, AI*

1. Introduction

The increasing complexity and frequency of cyber threats have driven the need for advanced cybersecurity measures. Traditional defense mechanisms, particularly signature-based detection systems, are often inadequate against sophisticated attacks such as zero-day exploits and advanced persistent threats (APTs). These methods, which rely on predefined attack signatures, struggle to keep pace with the rapid evolution of cyber threats, leaving systems vulnerable to breaches and compromises[1].

Artificial Intelligence (AI), particularly machine learning (ML) and deep learning (DL), offers a promising solution to these challenges. AI-based systems can analyze vast amounts of data, identify patterns, and detect anomalies that may indicate malicious activities. By learning from historical data and continuously adapting to new threats, AI provides dynamic and proactive defense mechanisms[2], [3].

This research proposes a comprehensive AI-based proactive threat detection framework to enhance cybersecurity. The framework integrates several key components: anomaly detection, threat intelligence integration, user behavior analysis, and automated response systems. Each component leverages advanced ML and DL techniques to provide a robust and adaptive defense against a wide range of cyber threats.

Anomaly detection is a fundamental aspect of the framework, focusing on identifying deviations from normal behavior that may indicate potential threats. This is achieved through the use of ML models trained on extensive datasets of network traffic and user activities[4]. Threat intelligence integration complements anomaly detection by incorporating real-time threat intelligence feeds, providing valuable insights into the latest attack vectors and allowing the system to adapt quickly to emerging threats[5].

User behavior analysis further strengthens the system by monitoring actions and interactions of users. Behavioral analysis helps detect insider threats and sophisticated attacks that do not exhibit traditional malicious signatures[6]. The automated response system is designed to implement swift countermeasures when threats are detected, such as isolating compromised systems, blocking malicious traffic, and alerting security analysts [7].

This AI-driven approach addresses the limitations of traditional cybersecurity measures by providing a proactive, adaptive defense. By integrating multiple AI-based components, the framework offers a comprehensive solution to the growing complexity of cyberattacks, equipping organizations to protect against both known and evolving threats [8].

2. Literature Review

Artificial Intelligence (AI) is playing an increasingly critical role in modern cybersecurity, revolutionizing the way threats are detected and mitigated. The integration of AI techniques, such as Machine Learning (ML) and Deep Learning (DL), has enabled cybersecurity systems to process vast amounts of historical data, recognize patterns, and identify anomalies indicative of malicious activities. These AI-driven methods are particularly adept at handling sophisticated cyber threats, including zero-day attacks

A Applied college, King Faisal University
Al-Ahsa, KSA, melfadiel@kfu.edu.sa
ORCID No: 0009-0000-1497-4381

and Advanced Persistent Threats (APTs) [9].

Several studies have highlighted the potential of AI to enhance cybersecurity. Buczak and Guven [10] provide a comprehensive survey of ML techniques, showcasing their ability to detect complex and evolving threats. They emphasize that traditional security solutions, such as signature-based detection systems, are increasingly ineffective against advanced, polymorphic threats. In contrast, ML algorithms have demonstrated superior adaptability in identifying threats that do not follow predefined patterns. Tang et al. [8] and Meidan et al. [11] extend this discussion by exploring the use of deep learning models—specifically Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs)—to detect malware and identify anomalies in network traffic. These models excel in their ability to learn complex patterns in large datasets, making them invaluable in a field where new attack vectors constantly emerge.

In addition to anomaly detection, behavioral analysis has emerged as a critical component in cybersecurity frameworks. By monitoring user actions and system interactions, behavioral analysis can detect deviations from established baselines of normal behavior, signaling potential threats. Egele et al. [6] discuss how behavioral analysis complements AI-based detection systems by identifying sophisticated attacks that do not follow typical attack signatures. This form of analysis is particularly effective in countering insider threats and social engineering attacks, where traditional signature-based detection methods often fail.

2.1 Integration Challenges and Adversarial Attacks

Despite the significant benefits of integrating AI into cybersecurity systems, several challenges remain. One primary concern is the high volume of data generated by network traffic and user activities. As organizations expand their digital operations, the amount of data that must be processed for real-time threat detection becomes overwhelming. Nguyen et al. [12] emphasize the need for more efficient data processing algorithms that can handle the vast datasets typical in modern cybersecurity environments. The scalability of AI models is critical to ensure that detection remains effective as data volume increases.

Another pressing challenge is the vulnerability of AI models to adversarial attacks. Adversarial attacks involve subtle manipulations of input data to deceive ML models, allowing malicious activities to bypass detection. Biggio and Roli highlight the growing threat of adversarial attacks on ML systems, urging the development of more robust algorithms capable of withstanding these deceptive tactics. They argue that adversarial defense strategies, such as adversarial training and model hardening, must become a central focus of AI research in cybersecurity to ensure long-term viability. Mandiant's report on APT1 details how sophisticated groups use such tactics to evade detection [13].

Incorporating privacy considerations into AI-driven cybersecurity frameworks is also paramount. Behavioral analysis, while effective, involves the continuous monitoring of user activities, which raises ethical and legal concerns regarding user privacy. Smith et al. underscore the importance of designing privacy-preserving AI techniques that maintain the effectiveness of threat detection systems without infringing on user privacy. Federated learning, which enables AI models to be trained across decentralized data without sharing sensitive user information, and differential privacy, which ensures that outputs of AI models do not reveal individual data points, are two promising approaches in this direction [14].

2.2 Limitations of Traditional Defense Mechanisms

Traditional security systems, including signature-based antivirus software and rule-based Intrusion Detection Systems (IDS), are increasingly inadequate in the face of modern cyber threats. Signature-based detection, which relies on known malware patterns, is easily circumvented by new or polymorphic threats. Similarly, rule-based IDS, which depend on predefined signatures, struggle to detect sophisticated, evolving attack methods such as zero-day exploits and APTs. Nguyen et al. [12] emphasize that these limitations have driven the adoption of AI-based solutions, which focus on anomaly detection and behavioral deviations rather than relying solely on known attack patterns.

Machine learning-based systems, particularly those employing CNNs and RNNs, have been shown to significantly outperform traditional methods in detecting network anomalies and malware. Buczak and Guven [8] and Kim et al. [10] demonstrate that these models can accurately detect both known and unknown threats by analyzing subtle indicators of malicious activity that are often overlooked by traditional systems.

2.3 Case Studies and Real-world Applications

Several case studies validate the efficacy of AI-driven cybersecurity frameworks in detecting and mitigating advanced cyber threats. A prominent example is the FireEye report on Advanced Persistent Threat (APT) groups, which details the use of AI-based detection systems in countering watering hole attacks [15]. These attacks, which involve compromising a website to target specific visitors, are difficult to detect using traditional security measures. However, FireEye's AI-powered system, which incorporates both machine learning and behavioral analysis, successfully identified and neutralized these threats before they could cause significant harm.

Another example is the analysis of the Elderwood Project, a series of watering hole attacks that targeted defense, energy, and technology sectors. Nguyen et al. [12] document how ML algorithms were used to detect anomalies in network traffic, allowing security teams to respond quickly to the attacks. These case studies demonstrate the practical benefits of integrating AI and ML into cybersecurity frameworks, especially in high-risk environments where proactive threat detection is critical.

2.4 Future Research Directions

While AI-based cybersecurity systems have shown great promise, there is a clear need for further research to address several remaining challenges. One major focus should be on improving the scalability of AI models, ensuring they can handle the ever-increasing volume of data in large, distributed networks. Real-time threat detection algorithms must also be optimized for speed and accuracy to prevent delays in responding to potential threats. Additionally, the development of adversarial defense strategies remains a top priority, as adversarial attacks continue to threaten the integrity of AI models.

Finally, future research must explore new techniques for ensuring the privacy of user data. Privacy-preserving AI methods, such as federated learning and differential privacy, offer potential solutions, but these techniques are still in the early stages of development. As the field of AI-driven cybersecurity continues to evolve, balancing the need for comprehensive threat detection with the protection of user privacy will be a key challenge for researchers and practitioners alike [16].

3. Proposed Multi-Layered Defense Framework

3.1. Framework Overview

This section presents a comprehensive AI-based proactive threat detection framework designed to address the limitations of traditional cybersecurity measures and enhance the detection and mitigation of watering hole attacks. The framework integrates multiple components, including anomaly detection, threat intelligence integration, user behavior analysis, and automated response systems.

3.2. 3.2 Components of the Framework

3.2.1 Anomaly Detection

Anomaly detection is a crucial aspect of the framework, focusing on identifying deviations from normal behavior that may indicate potential threats. This is achieved through the use of ML models trained on extensive datasets of network traffic and user activities. By establishing a baseline of normal behavior, the system can detect anomalies that may signify malicious activities.

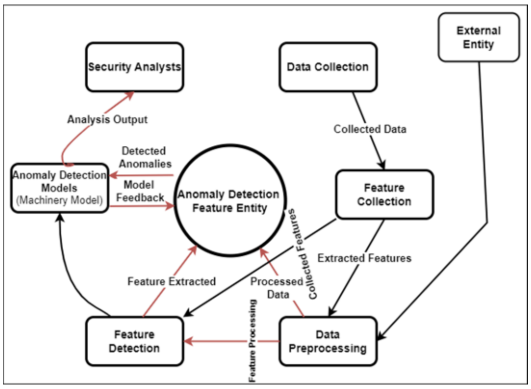


Fig 1: Anomaly Detection Workflow Using Artificial Intelligence

As illustrated in Figure 1, the anomaly detection process begins with data collection from various sources, such as internal systems and external entities. The collected data is then sent to the data preprocessing stage, where relevant features are extracted for further analysis. These extracted features are passed to the machine learning models and anomaly detection models, which analyze the data to identify any potential anomalies.

If anomalies are detected, they are flagged and sent to the security analysts for deeper investigation. The results from the analysis are also fed back into the anomaly detection models to continuously refine the detection process. Based on the outcome, the security team can take necessary actions to mitigate any identified risks.

3.2.2 Threat Intelligence Integration

Threat intelligence integration involves incorporating real-time threat intelligence feeds to enhance the system's ability to detect emerging threats. These feeds provide valuable insights into the latest attack vectors and techniques, allowing the system to adapt and respond to new threats promptly.

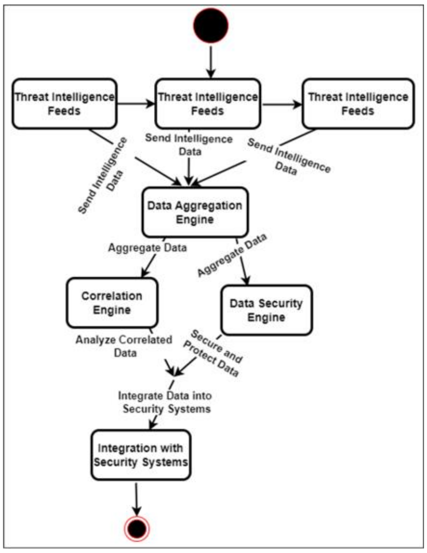


Fig 2: Threat Intelligence Integration Workflow

The diagram Fig.2. illustrates the workflow of integrating threat intelligence into cybersecurity systems. It begins with the collection of threat intelligence feeds from multiple sources. These feeds are aggregated in the Data Aggregation Engine, where raw threat intelligence data is compiled and organized.The aggregated data is then processed by the Correlation Engine to identify patterns and correlations between different threat vectors. Simultaneously, the Data Security Engine secures and protects the processed threat data to ensure integrity during the analysis phase.

Finally, the analyzed and correlated threat data is integrated into security systems to enhance their threat detection and response capabilities. This workflow enables the systems to continuously update their defenses, ensuring that they can respond proactively to new and evolving threats.

3.2.3 User Behavior Analysis

User behavior analysis complements anomaly detection by focusing on the actions and interactions of users. This component uses behavioral analysis techniques to establish a baseline of normal user behavior and identify deviations that may indicate malicious intent. By monitoring user behavior, the system can detect insider threats and other sophisticated attacks that may not exhibit obvious malicious signatures.

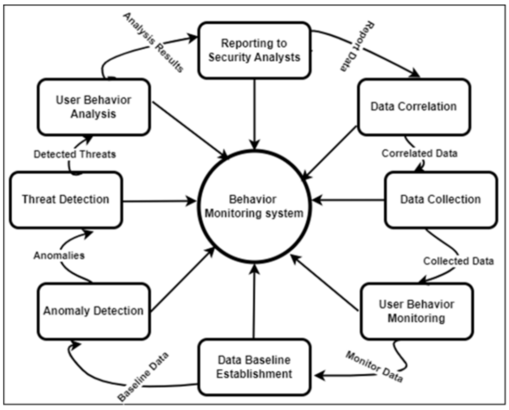


Fig 3: User Behavior Analysis Workflow

Fig.3. illustrates the user behavior analysis workflow, which begins with data collection from various user activities across the system. The collected data is continuously monitored by the User Behavior Monitoring system, which establishes a baseline for normal user behavior through the Data Baseline Establishment component.

The Anomaly Detection system continuously analyzes user behavior against the established baseline, identifying any deviations or suspicious activities. If anomalies are detected, they are passed to the Threat Detection system, which categorizes and flags potential threats.

The detected threats are then sent to the User Behavior Analysis system for further examination, and the results of this analysis are reported to the Security Analysts for further investigation and response. By proactively identifying abnormal behavior patterns, this workflow allows organizations to detect and mitigate insider threats or compromised user accounts more efficiently.

3.2.4 Automated Response Systems

The automated response system is designed to provide a swift and effective response to detected threats. It leverages the detection capabilities of the framework to implement appropriate countermeasures, such as isolating compromised systems, blocking malicious traffic, and alerting security analysts. This component ensures that threats are mitigated promptly, minimizing the potential impact on the organization.

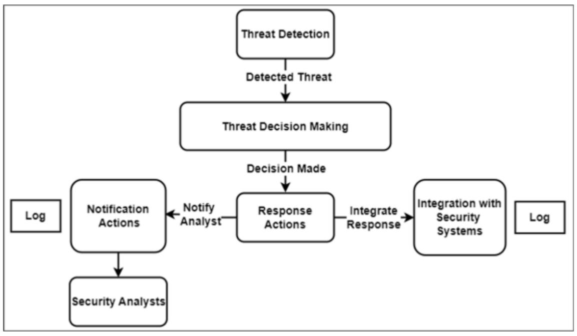


Fig 4: Automated Response Systems Workflow

As illustrated in Figure 4, the automated response system workflow begins with the threat detection phase, where potential threats are identified. The detected threat is then passed to the Threat Decision Making component, where appropriate response actions are determined based on the type and severity of the threat.

Once a decision is made, the system initiates Response Actions, which involve logging the event and notifying the relevant parties through Notification Actions. Notifications are sent to both Security Analysts and security systems to ensure a coordinated response.

Finally, the determined response is integrated into the security systems, allowing for immediate threat mitigation. This workflow ensures that potential threats are handled swiftly and effectively, minimizing the time between threat detection and resolution while ensuring all actions are properly logged and tracked.

3.3 Framework Workflow

The proposed framework's workflow integrates the various components to provide a comprehensive and proactive defense mechanism. The workflow begins with data collection from network traffic, user behavior, and threat intelligence feeds. This data is analyzed using ML and behavioral analysis techniques to detect anomalies and potential threats. Upon detecting a threat, the automated response system is triggered to mitigate the risk, and security analysts are alerted for further investigation.

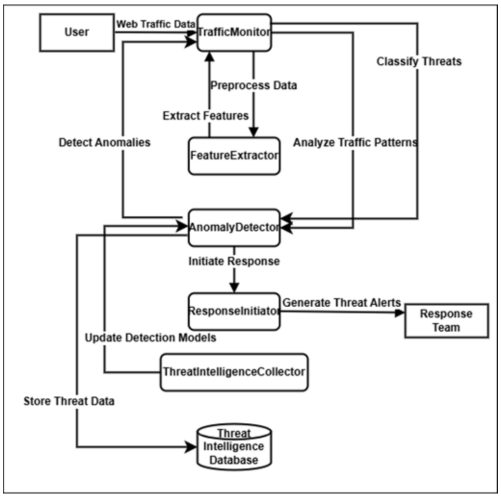
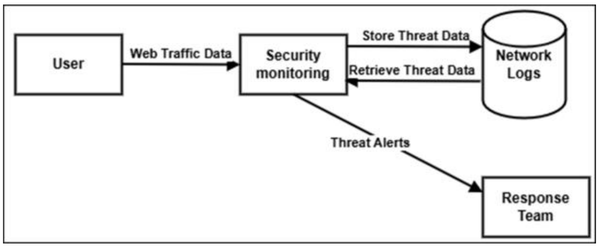


Fig 5: Framework Workflow

3.3.1 Level 0 Data Flow Diagram

The Level 0 Data Flow Diagram provides an overview of the data flow within the proposed framework. It illustrates the high-level processes and data interactions between the various components.

Fig 6: Level 0 Data Flow Diagram



The Level 0 Data Flow Diagram (DFD) provides a high-level overview of the data flow within the proactive threat detection framework. This diagram illustrates the interaction between the primary components of the system, highlighting the key processes involved in monitoring and analyzing web traffic data to detect potential threats. The diagram starts with the "User" entity, which provides web traffic data to the "TrafficMonitor" process. The "TrafficMonitor" preprocesses this data and passes it to subsequent processes for further analysis. The core processes include "FeatureExtractor," which extracts relevant features from the data, and "AnomalyDetector," which identifies anomalies that may indicate potential threats. The "ResponseInitiator" process takes appropriate actions based on the detected threats, generating alerts for the "Response Team" and storing critical threat data in the "Threat Intelligence Database." The "ThreatIntelligenceCollector" retrieves and updates threat intelligence data, ensuring that the system remains adaptive and responsive to emerging threats. This high-level DFD captures the essential data flows and interactions between the system components, providing a clear and concise representation of the overall threat detection workflow.

3.3.2 Level 1 Data Flow Diagram

The Level 1 Data Flow Diagram delves deeper into the specific processes involved in the framework. It details the flow of data between different modules, such as anomaly detection, threat intelligence integration, and user behavior analysis.

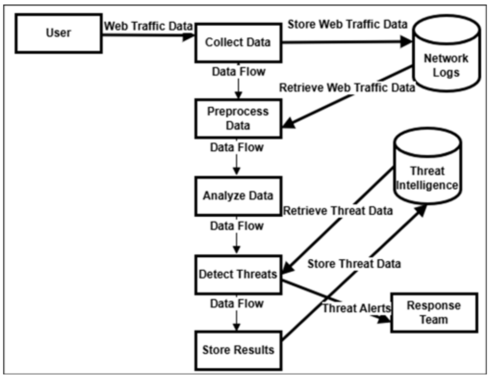


Fig 7: Level 1 Data Flow Diagram

The Level 1 Data Flow Diagram (DFD) offers a detailed view of the internal processes and data interactions within the proactive threat detection framework. This diagram delves deeper into the steps involved in monitoring and analyzing web traffic data to identify and respond to potential threats. It begins with the "User" entity providing web traffic data to the "Collect Data" process, where the initial data collection occurs. The data is then sent to the "Preprocess Data" process, where it is cleaned and normalized to ensure accuracy and relevance. Following preprocessing, the "Analyze Data" process performs detailed analysis to identify patterns and anomalies. The "Detect Threats" process evaluates these patterns to pinpoint potential security threats. Detected threats and their respective details are sent to the "Store Results" process, where the information is securely stored for future reference and analysis. The diagram also includes interactions with external entities, such as the "Threat Intelligence Database," where threat data is retrieved and stored, and the "Response Team," which receives threat alerts and takes necessary actions. This Level 1 DFD illustrates the comprehensive workflow of data handling and threat detection, highlighting the intricate processes and interactions that ensure robust and proactive cybersecurity measures.

3.4 System Architecture

The system architecture outlines the structure and components of the proposed framework. It includes the integration of AI models, data pipelines, threat intelligence feeds, and user behavior analysis.

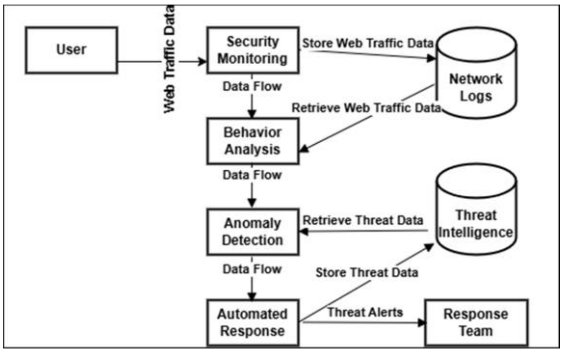


Fig 8: System Architecture

The System Architecture Diagram provides a detailed overview of the structural design and key components within the proactive threat detection framework. It visually represents the interaction between various modules and illustrates how they work together to achieve effective threat detection and mitigation. The architecture starts with the "User" who generates web traffic data, which is then captured and monitored by the "TrafficMonitor" module. This module preprocesses the data, removing noise and irrelevant information, and forwards the meaningful data to the "FeatureExtractor." The "FeatureExtractor" processes the data to extract significant features that are crucial for identifying patterns and anomalies. These features are analyzed by the "AnomalyDetector" to detect potential threats. Upon detecting a threat, the "ResponseInitiator" module initiates appropriate response actions to mitigate the identified threat. The "ThreatIntelligenceCollector" gathers data about known threats from various sources and updates the detection models in the "Threat Intelligence Database." This centralized repository stores all threat-related data, which can be retrieved for further analysis and to enhance detection models. The "Response Team" is responsible for investigating threat alerts generated by the system and taking necessary actions. The system also includes "Network Logs," which store all network activity logs for retrospective analysis. This architecture ensures a comprehensive and integrated approach to proactive threat detection, leveraging advanced data processing and analysis techniques to maintain robust cybersecurity measures.

3.5 Dynamic Behavior

The dynamic behavior of the proposed framework is represented through sequence diagrams, which detail the interactions between different system components during the detection and response process.

As shown in fig.9. the Sequence Diagram provides a detailed illustration of the interactions between various components within the proactive threat detection framework. This diagram traces the flow of operations from the initial user interaction through the detection and response processes. It begins with the user initiating the monitoring process by sending web traffic data to the system. The "TrafficMonitor" captures this data and forwards it to the "FeatureExtractor" for preprocessing and feature extraction. The extracted features are then sent to the "AnomalyDetector" for analysis, where anomalies are detected and classified as potential threats. Upon detecting a threat, the "AnomalyDetector" alerts the "ResponseInitiator," which triggers the appropriate response actions. Concurrently, the "ThreatIntelligenceCollector" retrieves and updates threat intelligence data from the "Threat Intelligence Database," ensuring that the system remains adaptive to new threats. The "ResponseInitiator" also communicates with the "Response Team," providing them with threat alerts and necessary information to mitigate the threats. This sequence of interactions is crucial for maintaining a robust and proactive defense against cyber threats, highlighting the dynamic and coordinated efforts of the system components. The Sequence Diagram effectively captures these interactions, providing a clear understanding of the workflow and the critical roles played by each component in threat detection and response.

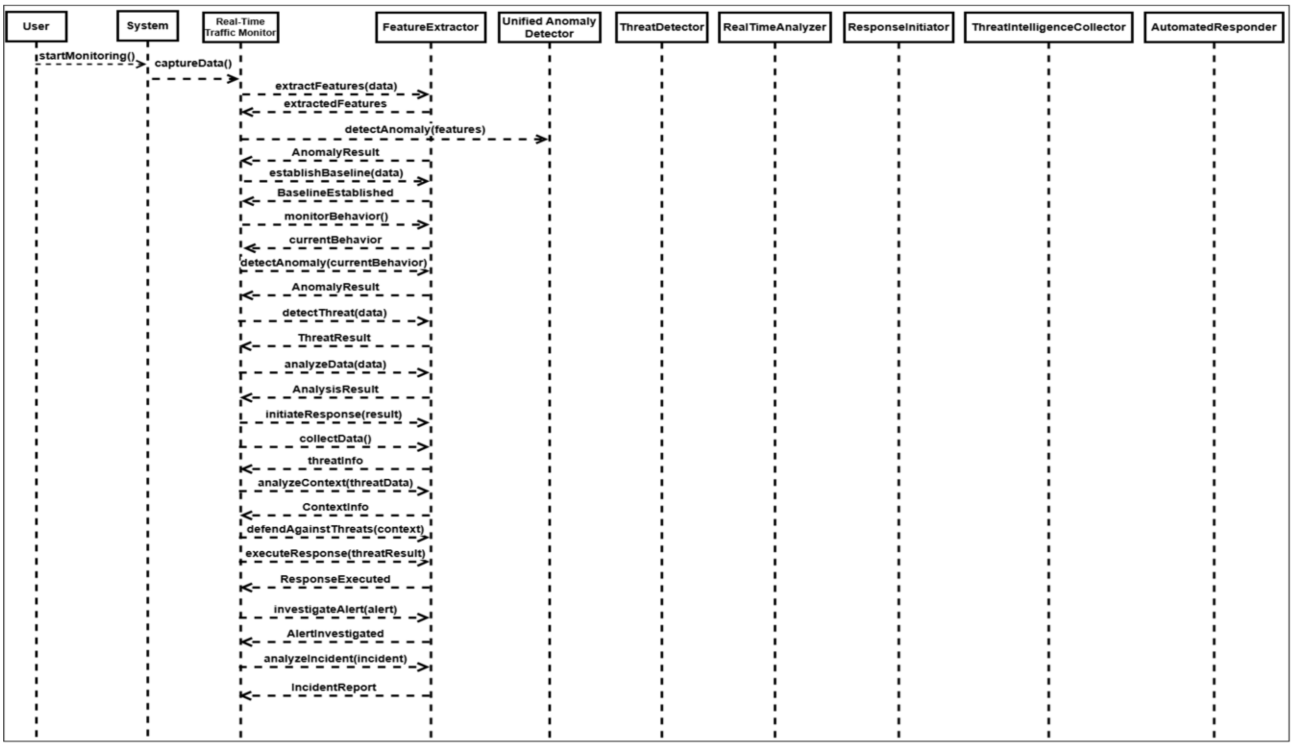


Fig 9: Sequence Diagram

4. Evaluation and Validation

4.1 Experimental Design

The proposed framework is a conceptual model designed to address the increasing complexity of cyber threats through AI-driven techniques. While this paper focuses on the theoretical structure of the framework, future research can involve experimental testing to evaluate its effectiveness in real-world environments. The framework is expected to perform well based on its design, leveraging machine learning (ML) and deep learning (DL) models to identify and mitigate cyber threats. Future experiments should measure performance using accuracy, precision, recall, F1-score, and response time as key metrics.

4.2 Evaluation Metrics:

• **Accuracy:** The ratio of correctly predicted instances to the total instances.

• **Precision:** The ratio of true positive instances to the total predicted positive instances.

• **Recall:** The ratio of true positive instances to the total actual positive instances.

• **F1-Score:** The harmonic mean of precision and recall.

• **Response Time:** The time taken by the framework to detect and respond to a threat.

4.3 Proposed Performance Evaluation

The performance of the proposed framework is theoretically expected to be strong based on the integration of machine learning (ML) and deep learning (DL) models. Future research should involve training and testing these models using real-world data to evaluate their accuracy, precision, and recall in detecting a wide range of cyber threats. Previous studies, such as that by Buczak and Guven [2], have demonstrated the potential of ML models in cybersecurity, particularly in identifying complex and evolving threats. However, real-world testing remains necessary to validate these theoretical assumptions and ensure the framework’s scalability and effectiveness.

4.4 Detection Capabilities Analysis

The detection capabilities of the framework can be assessed in future studies by testing its performance against a range of cyber threats, such as DDoS attacks, phishing attempts, and insider threats. By integrating real-time threat intelligence feeds, the framework is designed to remain adaptive to emerging threats. However, validation through real-world implementation and testing remains a critical future step.

4.5 Identifying Areas for Improvement

While this conceptual framework outlines a robust approach to proactive threat detection, future research should focus on identifying performance bottlenecks through experimental testing. Specific areas for improvement may include optimizing the data processing pipeline, enhancing model efficiency, and improving scalability and robustness in handling large datasets.

4.6 Future Research Directions

This conceptual framework provides a strong foundation for leveraging AI in cybersecurity; however, further research is necessary to implement and validate its effectiveness. Future studies should focus on developing real-world experiments to test the framework's performance across various types of cyber threats. Key challenges, such as adversarial attacks and data privacy concerns, should also be explored to ensure that the framework is both scalable and secure. The integration of privacy-preserving AI techniques, such as federated learning and differential privacy, may be particularly beneficial in protecting user data while maintaining robust threat detection capabilities.

5. Conclusion

This research proposes a conceptual AI-based proactive threat detection framework aimed at enhancing cybersecurity. The framework is designed to leverage machine learning and behavioral analysis to detect and mitigate cyber threats. By integrating multiple components—such as anomaly detection, threat intelligence integration, user behavior analysis, and automated response systems—the framework provides a theoretically robust and adaptive defense mechanism.

Although the framework has not yet been tested in real-world environments, its design suggests a promising solution to the growing threat of cyber attacks. The integration of real-time threat intelligence feeds is expected to significantly enhance the framework's adaptability to emerging threats, offering a dynamic and proactive approach to cybersecurity.

Future research will focus on implementing and validating the framework in actual environments, such as smart city infrastructure or large-scale enterprise systems. Testing will provide deeper insights into its scalability, efficiency, and adaptability in handling large and dynamic datasets. Additionally, addressing challenges like data processing efficiency and resilience to adversarial attacks will be essential in future iterations of the framework.

By continuing to innovate and refine these defense mechanisms, organizations will be better equipped to defend against the increasingly sophisticated cyber threats of the modern digital landscape.

Acknowledgements

I would like to express my sincere appreciation to King Faisal University for providing the essential resources and facilities. I am especially grateful to my family for their constant encouragement and understanding throughout this journey. Their unwavering support played a pivotal role in the successful completion of this work.

Author contributions

Mohammed Awad Mohammed Ataelfadiel carried out all aspects of the research, from conceptualizing the initial idea to working through the detailed procedures and arriving at the final conclusion.

Conflicts of interest

The author declare no conflicts of interest.

References

[1] S. M. Shamshirband, N. B. Anuar, M. L. M. Kiah, and A. Patel, "An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique," *Eng. Appl. Artif. Intell*., vol. 26, no. 9, pp. 2105-2127, Dec. 2013.

[2] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Commun. Surveys Tuts*., vol. 18, no. 2, pp. 1153-1176, 2nd Quart., 2016.

[3] N. Moustafa and J. Slay, "The significant features of the UNSW-NB15 and the KDD99 data sets for network intrusion detection systems," in *Proc. 4th Int. Workshop Building Anal. Datasets Gathering Exp. Returns Secur. (BADGERS)*, 2015, pp. 25-31.

[4] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: Methods, systems and tools," *IEEE Commun. Surveys Tuts*., vol. 16, no. 1, pp. 303-336, 1st Quart., 2014.

[5] W. Wang, M. Zhu, and X. Zeng, "Malware traffic classification using convolutional neural network for representation learning," in *Proc. 12th Int. Conf. Comput. Intell. Secur. (CIS)*, 2016, pp. 174-177.

[6] M. Egele, T. Scholte, E. Kirda, and C. Kruegel, "A survey on automated dynamic malware analysis techniques and tools," *ACM Comput. Surveys*, vol. 44, no. 2, pp. 1-42, 2012.

[7] S. Y. Yerima and S. Sezer, "Android malware detection: An eigenface based approach," in *Proc. 6th Int. Conf. Adv. Mobile Comput. Multimedia*, 2014, pp. 197-202.

[8] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Commun. Surveys Tuts*., vol. 18, no. 2, pp. 1153-1176, 2nd Quart., 2016.

[9] T. A. Tang et al., "Deep learning approaches to network anomaly detection," *IEEE Commun. Mag*., vol. 55, no. 2, pp. 42-47, Feb. 2017.

[10] Y. Kim, J. Kim, and H. K. Kim, "A deep learning based DDoS detection system in software-defined networking (SDN)," in *Proc. 2016 Int. Conf. Big Data Smart Comput. (BigComp)*, 2016, pp. 201-206.

[11] Y. Meidan, M. Bohadana, A. Shabtai, et al., "N-BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervasive Comput*., vol. 17, no. 3, pp. 12-22, Jul.-Sep. 2018.

[12] G. Wang, J. Hao, J. Ma, and L. Huang, "A new approach to intrusion detection using artificial neural networks and fuzzy clustering," *Expert Syst. Appl*., vol. 37, no. 9, pp. 6225-6232, Sep. 2010.

[13] Mandiant (FireEye), "APT1: Exposing one of China's cyber espionage units," *Mandiant Report*, 2013. [Online]. Available: https://www.fireeye.com

[14] Symantec, "The Elderwood project," *Symantec Security Response*, 2012. [Online]. Available: https://symantec-enterprise-blogs.security.com

[15]] M. Ambusaidi, X. He, P. Nanda, and Z. Tan, "Building lightweight intrusion detection systems using wrapper-based feature selection mechanisms," *Comput. Secur*., vol. 65, pp. 68-82, Mar. 2017.

[16] N. Papernot, M. Abadi, Ú. Erlingsson, I. Goodfellow, and K. Talwar, "Semi-supervised knowledge transfer for deep learning from private training data," in *Proc. 5th Int. Conf. Learn. Represent. (ICLR)*, 2017.