International Journal of Scientific Research in Engineering & Technology
Volume6, Issue2 (March-April 2026), PP: 232-238.
https://www.doi.org/10.59256/ijsreat.20260602029
www.ijsreat.com
ISSN No: 2583-1240

Zero Day Attack Detection System Using Ai with Multifactor Authentication

Ramya S[1], Revathi S[2], Rathisha M[3], Sandhiya S[4], Subashinni K[5]
[1]Assistant Professor, Department of Information Technology, Er. Perumal Manimekalai College of Engineering Hosur, Tamil Nadu, India.
[2,3,4,5]B.Tech. Department of Information Technology, Er. Perumal Manimekalai College of Engineering Hosur, Tamil Nadu, India.

To Cite this Article: *Ramya S[1], Revathi S[2], Rathisha M[3], Sandhiya S[4], Subashinni K[5], "Zero Day Attack Detection System Using Ai with Multifactor Authentication", International Journal of Scientific Research in Engineering & Technology, Volume 06, Issue 02, March-April 2026, PP: 232-238.*

Abstract: *Zero-day attacks are among the most critical cybersecurity threats as they exploit unknown vulnerabilities in software systems before patches are available. Traditional security mechanisms fail to detect such attacks due to their reliance on known signatures. This paper proposes an intelligent system that integrates Artificial Intelligence (AI) with Multi-Factor Authentication (MFA) to enhance both detection and prevention of zero-day attacks. The system uses machine learning algorithms, particularly Isolation Forest, to analyze user behavior and detect anomalies in real time. Additionally, MFA ensures secure access by requiring multiple verification factors such as passwords and one-time passwords. The proposed approach improves detection accuracy, reduces unauthorized access, and provides a robust solution for modern cybersecurity challenges.*

Key Words *Zero-Day Attack, Artificial Intelligence, Machine Learning, Anomaly Detection, Cybersecurity, Multi-Factor Authentication, Isolation Forest, Intrusion Detection System, Behavioral Analysis*

I. INTRODUCTION

The rapid growth of digital technologies has significantly increased the reliance on computer systems and internet-based services. Organizations across various domains such as banking, healthcare, and government depend on digital platforms for storing and managing sensitive data. However, this dependency has also introduced serious cybersecurity threats. Among these threats, zero-day attacks are particularly dangerous because they exploit vulnerabilities that are unknown to developers and security systems.

Traditional cybersecurity solutions rely on signature-based detection methods, which are effective only against known threats. These systems fail to detect new and unknown attacks, making them ineffective against zero-day vulnerabilities. To overcome this limitation, Artificial Intelligence (AI) has emerged as a powerful tool in cybersecurity. AI-based systems can analyze patterns of user behavior and detect anomalies that indicate potential threats.

In addition to detection, secure authentication is essential to prevent unauthorized access. Multi-Factor Authentication (MFA) enhances security by requiring multiple verification methods, such as passwords and one-time passwords. The combination of AI and MFA provides a comprehensive solution for detecting and preventing zero-day attacks.

II. LITERATURE REVIEW

[1] Zero-Day Attack Detection using Machine Learning (2021) by A. Kumar; R. Singh; P. Sharma This study focuses on detecting zero-day attacks using machine learning techniques. The authors propose an anomaly detection system that analyzes network traffic patterns to identify unusual behavior. The system uses algorithms such as Support Vector Machine (SVM) and K-Means clustering to classify normal and abnormal activities. The research highlights the importance of behavioral analysis in detecting unknown threats and demonstrates improved detection accuracy compared to traditional signature-based systems.

[2] Anomaly Detection using Isolation Forest (2019) by F. T. Liu; K. M. Ting; Z. Zhou This research introduces the Isolation Forest algorithm for anomaly detection. The method isolates anomalies faster than normal data points by using random partitioning. It does not require labeled data and is highly efficient for large datasets. The study shows that Isolation Forest is effective in identifying rare and unknown cyber threats.

[3] Artificial Intelligence in Intrusion Detection Systems (2020) by J. Park; M. Lee; S. Kim This paper explores the use of artificial intelligence in intrusion detection systems. The authors explain how machine learning models analyze network behavior and detect anomalies. The study emphasizes improved accuracy and adaptability of AI-based systems over traditional methods.

[4] Multi-Factor Authentication for Secure Systems (2018) by R. Das; S. Mishra This research discusses the role of Multi-Factor Authentication in improving system security. The system combines multiple authentication factors such as passwords, OTPs, and biometrics. The results show that MFA significantly reduces unauthorized access and enhances data protection**.**

III. PROPOSED SYSTEM

Nowadays, e-commerce platforms have become an important part of daily life, allowing people to shop, make payments, and manage orders online with ease. As the number of online users continues to grow, these platforms have also become common targets for cyber attacks. Since customers share personal details, addresses, and payment information, maintaining strong security is essential for every e-commerce business.

The proposed zero-day attack detection system can be integrated with e-commerce websites to provide better protection against modern cyber threats. Unlike traditional security systems that mainly focus on known attacks, this system uses Artificial Intelligence to identify unusual behavior and detect unknown threats in real time. This helps the platform respond quickly before any serious damage occurs.

The system can observe normal customer activities such as login times, browsing patterns, preferred devices, shopping habits, and payment behavior. By learning these regular patterns, it becomes easier to detect suspicious actions. For example, if a user account suddenly logs in from a different location, attempts multiple failed logins, or makes unusual high-value purchases, the system can treat it as a possible threat and take immediate action.

Another major advantage of this integration is improved payment security. Online payments are one of the most sensitive parts of an e-commerce platform, and attackers often try to misuse stolen accounts or payment information. In such situations, the system can request additional verification through Multi-Factor Authentication before completing the transaction. This extra step helps protect both customers and businesses from fraud.

1-E Commerce

The integration also increases customer confidence and trust. Users are more likely to continue shopping on platforms that keep their accounts and transactions safe. By reducing fraud, preventing unauthorized access, and protecting sensitive information, the system creates a safer and more reliable shopping experience.

In the future, this solution can be enhanced with advanced features such as biometric login, personalized fraud detection, chatbot-based alerts, secure transaction records, and smarter AI models. With these improvements, e-commerce platforms can become more secure, intelligent, and prepared to face future cybersecurity challenges

.IV. SYSTEM ARCHITECTURE

The system architecture of the proposed zero-day attack detection system is designed to integrate multiple modules that work together to ensure both security and efficient threat detection. The architecture follows a layered approach, where each component performs a specific function, and all components are interconnected to provide a seamless flow of data from user input to final decision-making. The main modules in the system include the user interface, authentication module, Multi-Factor Authentication module, data collection module, database, Artificial Intelligence engine, anomaly detection module, and alert and response system.

The process begins with the user interface, which acts as the entry point to the system. This module allows users to interact with the system by entering login credentials such as username and password. The interface is designed to be user-friendly and provides necessary feedback during the authentication process. Once the user submits their credentials, the request is forwarded to the authentication module for verification.

The authentication module is responsible for validating the user's credentials by comparing them with stored data in the database. If the credentials are correct, the system proceeds to the next level of security, which is the Multi-Factor Authentication module. This module adds an additional layer of protection by requiring the user to verify their identity using a second factor, such as a one-time password (OTP) sent to their registered device. This ensures that even if login credentials are compromised, unauthorized access can still be prevented.

After successful authentication, the system activates the data collection module. This module gathers various types of user behavior data, including login time, IP address, device information, location, and activity patterns. The collected data is

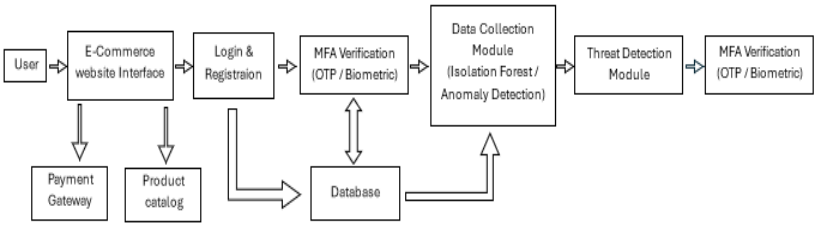
essential for understanding user behavior and is continuously stored in the database. This database acts as a central repository that maintains both historical and real-time data, which is later used for analysis.

The Artificial Intelligence engine is the core component of the system, responsible for processing and analyzing the collected data. It uses machine learning algorithms, particularly Isolation Forest, to learn patterns of normal user behavior. During the training phase, the AI model analyzes historical data to establish a baseline of normal activities. This baseline includes typical login times, frequently used devices, and common usage patterns.

Once the model is trained, the system enters the real-time analysis phase. In this phase, the anomaly detection module compares incoming user behavior data with the learned baseline. If the behavior matches the normal pattern, the system considers it safe and allows the user to continue their activities. However, if a deviation is detected, such as an unusual login time or unfamiliar device, the system identifies it as an anomaly.

When an anomaly is detected, the alert and response module is activated. This module is responsible for taking appropriate actions based on the severity of the detected threat. It may generate alerts to notify the system administrator, block the user's access, or request additional authentication. These actions help prevent potential security breaches and ensure the safety of the system.

Another important aspect of the architecture is its ability to support continuous learning and improvement. As more data is collected over time, the AI model updates its understanding of normal behavior, making it more accuratend reducing false positives. This adaptive capability allows the system to respond effectively to evolving cyber threats and changing user behavior.



2- System Architecture

V. METHODOLOGY

The methodology of the proposed system defines the step-by-step process followed to detect zero-day attacks and ensure secure user authentication. It is designed as a systematic workflow that integrates authentication, data collection, machine learning, and real-time decision-making. Each step in the methodology plays a crucial role in achieving accurate anomaly detection and preventing unauthorized access.

The process begins with user authentication, where the user enters their login credentials, including username and password, through the system interface. This step serves as the primary level of verification. The entered credentials are validated against the stored data in the database. If the credentials are incorrect, access is denied immediately. However, if the credentials are valid, the system proceeds to the next stage, which is Multi-Factor Authentication.

In the Multi-Factor Authentication stage, an additional layer of security is introduced. The system generates a one-time password (OTP) and sends it to the user's registered mobile number or email address. The user must enter the correct OTP within a specified time limit to proceed. This step ensures that even if an attacker gains access to the user's password, they cannot log in without completing the second level of verification. This significantly enhances system security.

After successful authentication, the system moves to the data collection phase. In this stage, various parameters related to user behavior are collected. These include login time, IP address, device information, location, and user activity patterns. The data collection process is continuous and occurs every time the user interacts with the system. This data is then stored in a database and used for analysis.

The next step involves data preprocessing, where the collected data is cleaned and prepared for machine learning. This includes removing inconsistencies, handling missing values, and converting data into a suitable format for analysis. Preprocessing ensures that the data is accurate and reliable, which is essential for building an effective AI model. a

Following preprocessing, the system enters the training phase. In this phase, the machine learning model, specifically the Isolation Forest algorithm, is trained using historical data. The model learns the normal behavior patterns of users by analyzing features such as typical login times, frequently used devices, and regular activity levels. It establishes a baseline that represents standard system behavior.

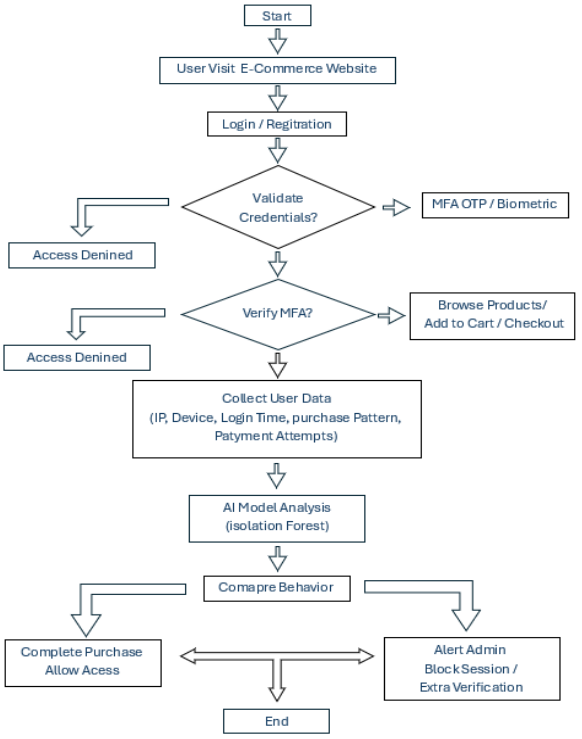
Once the model is trained, the system transitions to the real-time detection phase. In this phase, new user data is continuously fed into the trained model. The system compares the current behavior with the learned baseline to determine whether it is normal or anomalous. If the behavior aligns with the normal pattern, the system allows the user to continue without interruption. However, if a deviation is detected, such as an unusual login time or unknown device, the system identifies it as an anomaly

When an anomaly is detected, the system activates the decision-making and response phase. In this stage, the system evaluates the severity of the anomaly and takes appropriate action. This may include generating an alert, notifying the administrator, requesting additional authentication, or blocking the user's access. These actions help prevent potential security breaches and protect the system from zero-day attacks.

The above flowchart illustrates the step-by-step working of the proposed system. It begins with user login and credential validation, followed by Multi-Factor Authentication using OTP. After successful authentication, the system collects user behavior data such as IP address, login time, device, and activity. This data is analyzed using the AI model (Isolation Forest), and the behavior is compared with normal patterns. Based on the analysis, the system either allows access for normal behavior or detects anomalies and blocks the user while generating alerts.

Another important aspect of the methodology is continuous learning. The system continuously updates its model using new data collected over time. This allows the AI model to adapt to changes in user behavior and improve its detection accuracy. Continuous learning also helps reduce false positives, ensuring that normal activities are not mistakenly classified as threats.

Overall, the methodology follows a structured approach that combines authentication, data collection, machine learning, and real-time analysis. By integrating these steps, the system is capable of detecting zero-day attacks effectively while ensuring secure user access. This comprehensive methodology makes the system reliable, adaptive, and suitable for modern cybersecurity applications.



3- Frame work

VI. ALGORITHMS

The effectiveness of the proposed system in detecting zero-day attacks largely depends on the selection and implementation of appropriate machine learning algorithms. These algorithms are responsible for analyzing user behavior, identifying patterns, and detecting anomalies that may indicate potential cyber threats. In this system, the primary algorithm used is the Isolation Forest, along with supporting techniques such as Support Vector Machine (SVM) and clustering methods. These algorithms work together to enhance detection accuracy and system reliability.

The Isolation Forest algorithm is the core component of the anomaly detection process. It is an unsupervised machine learning algorithm specifically designed for identifying anomalies in large datasets. Unlike traditional algorithms that focus on profiling normal data points, Isolation Forest works by isolating anomalies. It randomly selects a feature from the dataset and splits the data based on a random value within the range of that feature. This process is repeated recursively to form a tree structure. Since anomalies are rare and significantly different from normal data points, they require fewer splits to be isolated. As a result, they appear closer to the root of the tree, making them easier to identify. This unique approach makes Isolation Forest highly efficient and suitable for detecting zero-day attacks, where labeled data is often unavailable.

Another algorithm considered in the system is the Support Vector Machine (SVM), which is a supervised learning algorithm used for classification tasks. SVM works by creating a boundary, known as a hyperplane, that separates data points into different classes. In the context of this system, SVM can be used to distinguish between normal and abnormal behavior based on labeled training data. Data points that lie far from the boundary are considered anomalies. SVM is particularly effective in handling high-dimensional data and can improve detection accuracy when combined with other algorithms.

Clustering techniques such as K-Means are also used to support anomaly detection. K-Means is an unsupervised learning algorithm that groups similar data points into clusters based on their features. In this approach, normal behavior forms dense clusters, while anomalies appear as outliers that do not belong to any cluster. By identifying these outliers, the system can detect unusual activities that may indicate potential attacks. Clustering is useful for understanding data distribution and enhancing the overall detection process.

In addition to these algorithms, basic classification techniques such as Logistic Regression may be used for initial analysis and comparison. Logistic Regression predicts the probability of a data point belonging to a particular class, such as normal or malicious. Although it is simpler compared to other algorithms, it can serve as a baseline model for evaluating system performance. The integration of these algorithms allows the system to handle different types of data and detect anomalies more effectively. Isolation Forest provides efficient anomaly detection without requiring labeled data, while SVM and clustering techniques enhance classification and pattern recognition. Together, these algorithms enable the system to identify zero-day attacks with high accuracy and low computational cost.

Overall, the use of advanced machine learning algorithms plays a crucial role in the success of the proposed system. By leveraging these techniques, the system can detect unknown threats, adapt to changing patterns, and provide real-time security. This makes it a powerful solution for modern cybersecurity challenges.

VII. IMPLEMENTATION

The implementation of the proposed zero-day attack detection system is carried out using a combination of programming tools, machine learning libraries, and web technologies. The system is primarily developed using the Python programming language due to its simplicity, flexibility, and strong support for data analysis and machine learning. Various libraries such as Pandas, NumPy, Scikit-learn, Matplotlib, and Seaborn are used to handle data processing, model training, and visualization tasks. Additionally, a web-based interface is developed using Streamlit to provide an interactive platform for users to simulate login behavior and observe system responses.

The implementation process begins with dataset creation and data handling. Since real-world datasets may not always be available, a sample dataset is created that represents user behavior. This dataset includes features such as login time, IP address change, device change, and activity level. These features are selected because they play a crucial role in identifying abnormal user behavior. The data is stored in a structured format using Pandas DataFrames, which allows efficient data manipulation and analysis. Once the dataset is prepared, the next step involves data preprocessing. In this stage, the data is cleaned and transformed into a suitable format for machine learning. This includes handling missing values, normalizing data if required, and ensuring consistency in feature representation. Proper preprocessing is essential to improve the accuracy and performance of the machine learning model.

After preprocessing, the system proceeds to model training. The Isolation Forest algorithm is implemented using the Scikit-learn library. The model is trained on the dataset to learn patterns of normal user behavior. During training, the algorithm builds multiple decision trees by randomly selecting features and splitting data points. This helps the model understand the structure of normal data and identify anomalies effectively.

Once the model is trained, it is used for prediction. New user behavior data is provided as input to the model, and the system predicts whether the activity is normal or anomalous. The output of the model is typically in the form of numerical values, where one value represents normal behavior and another represents anomalies. These values are then converted into meaningful labels such as “Normal” or “Attack” for better understanding.

To enhance user interaction, a web application is developed using Streamlit. The interface allows users to input parameters such as login time, IP change, device change, and activity level through sliders and selection boxes. When the user submits the input, the system processes the data using the trained model and displays the result instantly. This real-time interaction helps demonstrate how the system detects potential zero-day attacks.

Visualization is another important part of the implementation. Graphs such as scatter plots and count plots are generated using Matplotlib and Seaborn to represent the results. Scatter plots help visualize the distribution of normal and anomalous data points, while count plots show the number of detected attacks and normal activities. These visualizations make it easier to understand the system’s performance and behavior.

The system is further deployed online using platforms such as Streamlit Cloud or Render. Deployment allows the application to be accessed through a web browser, making it easier for users to test and demonstrate the system. The deployment process involves uploading the project files to a repository and configuring the application to run on a cloud server.

Overall, the implementation of the proposed system combines data processing, machine learning, and web development to create a complete and functional application. The use of Python and modern libraries ensures efficiency and scalability, while the web interface provides ease of use. This implementation demonstrates how AI can be effectively used to detect zero-day attacks and enhance cybersecurity.

VIII. RESULT

The proposed zero-day attack detection system was tested using simulated user behavior data to evaluate its performance in identifying anomalies. The system, powered by the Isolation Forest algorithm, was able to effectively distinguish between normal and abnormal activities. It successfully detected unusual patterns such as irregular login times, changes in IP address, unknown devices, and high activity levels, which are indicators of potential zero-day attacks.

The results were further analyzed using visualization techniques such as scatter plots and count plots. These visualizations clearly showed the separation between normal data points and anomalies. Normal activities formed clusters, while anomalous activities appeared as outliers, demonstrating the effectiveness of the machine learning model in identifying suspicious behavior.

The above figure shows the developed web application interface created using Streamlit. The system allows users to simulate login behavior by adjusting parameters such as login time, IP change, device change, and activity level. Based on the input, the AI model analyzes the data and classifies it as either normal activity or a potential attack. The interface also includes visualizations such as scatter plots and bar charts to represent user activity and detected anomalies. This interactive dashboard demonstrates the real-time working of the proposed system.

The integration of Multi-Factor Authentication added an additional layer of security to the system. Even when suspicious login attempts were detected, MFA ensured that unauthorized users could not gain access without proper verification. This combination of detection and prevention significantly improved the overall security of the system.

4 - Result

The system also demonstrated strong real-time performance, as it was able to analyze user input and provide immediate results through the web interface. However, the accuracy of the system depends on the quality of the training data, and there may be occasional false positives when user behavior varies significantly.

Overall, the results confirm that the proposed system is effective in detecting zero-day attacks and enhancing cybersecurity. The combination of Artificial Intelligence and Multi-Factor Authentication provides a reliable and efficient solution for modern security challenges.

IX. ADVANTAGES AND LIMITATIONS

The proposed system offers several advantages in enhancing cybersecurity, particularly in detecting zero-day attacks. One of the main strengths of the system is its ability to identify unknown threats using Artificial Intelligence. Unlike traditional methods that rely on predefined signatures, the system analyzes user behavior and detects anomalies in real time. This makes it highly effective in identifying new and emerging cyber threats.

Another important advantage is the integration of Multi-Factor Authentication, which significantly improves system security. By requiring multiple forms of verification such as passwords and one-time passwords, the system prevents unauthorized access even if login credentials are compromised. This combination of AI-based detection and MFA provides both detection and prevention, making the system more robust.

The system also supports real-time monitoring and response, allowing it to quickly detect and react to suspicious activities. Additionally, it has the ability to learn and adapt over time through continuous data analysis, which improves accuracy and reduces false positives. The use of machine learning algorithms ensures scalability and flexibility for different applications.
However, the system also has certain limitations. One of the primary challenges is the need for a large and high-quality dataset to train the machine learning model effectively. Without sufficient data, the accuracy of the system may be reduced. Additionally, the system may produce false positives in cases where user behavior deviates significantly from the norm.

Another limitation is the computational cost associated with real-time data processing and machine learning algorithms. Implementing and maintaining such a system may require significant resources and technical expertise. Despite these limitations, the advantages of the proposed system outweigh its drawbacks, making it a valuable solution for modern cybersecurity challenges.

X. CONCLUSION

The proposed system presents an effective solution for detecting zero-day attacks using Artificial Intelligence combined with Multi-Factor Authentication. By focusing on behavioral analysis rather than traditional signature-based methods, the system is capable of identifying unknown and emerging threats that are difficult to detect using conventional security techniques.

The use of machine learning algorithms, particularly Isolation Forest, enables the system to analyze user behavior and detect anomalies in real time. This approach allows the system to identify suspicious activities such as unusual login times, unknown devices, and abnormal usage patterns. As a result, the system improves detection accuracy and enhances overall cybersecurity.

In addition to detection, the integration of Multi-Factor Authentication strengthens system security by preventing unauthorized access. Even if login credentials are compromised, the additional verification step ensures that only legitimate users can access the system. This combination of detection and prevention provides a comprehensive security solution.

The system also demonstrates adaptability through continuous learning, allowing it to improve its performance over time. However, the effectiveness of the system depends on the quality of the data used for training, and there may be minor limitations such as false positives in certain cases.

Overall, the proposed system offers a reliable, efficient, and scalable approach to modern cybersecurity challenges. It successfully addresses the limitations of traditional methods and provides a strong foundation for future enhancements in zero-day attack detection systems.

REFERENCE

1. *Zero-Day Attack Detection using Machine Learning (2021)* by A. Kumar; R. Singh; P. Sharma
2. *Anomaly Detection using Isolation Forest (2019)* by F. T. Liu; K. M. Ting; Z. Zhou
3. *Artificial Intelligence in Intrusion Detection Systems (2020)* by J. Park; M. Lee; S. Kim
4. *Multi-Factor Authentication for Secure Systems (2018)* by R. Das; S. Mishra
5. *Behavior-Based Cyber Attack Detection (2022)* by K. Verma; A. Gupta
6. *Hybrid Security Model using AI and MFA (2023)* by S. Reddy; P. Nair
7. *Deep Learning for Cybersecurity Applications (2021)* by I. Goodfellow; Y. Bengio
8. *Network Intrusion Detection using Machine Learning (2020)* by L. Zhang; H. Wang.
9. *Clustering-Based Anomaly Detection (2019)* by P. Jain; M. Kumar
10. *Real-Time Cyber Threat Detection using AI (2022)* by S. Gupta; R. Mehta