Behavioral Biometrics-Based Continuous Authentication Framework Using Explainable AI for Insider Threat Detection in Enterprise Networks

Dr. Satinderjeet Singh
IT Auditor, IT Cyber Risk & Compliance Architect, The Children's Place, New Jersey, USA

Abstract - Insider threats represent one of the most significant security challenges in modern enterprise networks because they originate from legitimate users who have authorized access to organizational systems and sensitive data. Traditional authentication mechanisms, such as passwords and multi-factor authentication, verify user identity only at the initial login stage and fail to monitor user behavior during the active session. To overcome this limitation, continuous authentication based on behavioral biometrics has emerged as an effective approach for detecting anomalous activities in real time. This study proposes a Behavioral Biometrics-Based Continuous Authentication Framework integrated with Explainable Artificial Intelligence (XAI) to improve insider threat detection in enterprise environments. The proposed framework continuously monitors behavioral indicators such as keystroke dynamics, mouse movement patterns, system interaction activities, and network usage behavior. Machine learning algorithms analyze these behavioral patterns to identify deviations from normal user behavior, while explainable AI techniques provide transparent and interpretable explanations of model decisions for security analysts. The integration of behavioral biometrics with explainable AI enhances detection accuracy, reduces false positive rates, and increases trust in automated security systems. The proposed framework provides a scalable and interpretable solution for strengthening enterprise cybersecurity against insider threats.

Keywords: Behavioral Biometrics, Continuous Authentication, Explainable Artificial Intelligence (XAI), Insider Threat Detection, Enterprise Network Security, Machine Learning, Cybersecurity Analytics.

I. INTRODUCTION

1.1 Background of Enterprise Network Security

In the modern digital economy, enterprise networks serve as the backbone of organizational operations by enabling communication, data storage, and the execution of critical business processes. Organizations increasingly rely on interconnected systems, cloud services, and distributed infrastructures to support their daily activities. While these technological advancements have significantly improved productivity and operational efficiency, they have also introduced complex cybersecurity challenges. Among these challenges, insider threats have emerged as one of the most critical risks to enterprise security [1].

Unlike external cyberattacks, insider threats originate from individuals who already possess legitimate access to organizational resources. These individuals may include employees, contractors, system administrators, or business partners who intentionally or unintentionally violate security policies. Because insiders already have authorized access to systems and data, their actions are often difficult to distinguish from legitimate activities [2].

Insider threats are particularly challenging to detect because malicious actions often appear as normal network operations. Traditional security systems such as firewalls, intrusion detection systems, and access control mechanisms are primarily designed to prevent unauthorized external access. However, these systems may fail to identify abnormal behavior performed by authorized users. As organizations continue to manage large volumes of sensitive information—including financial records, intellectual property, and customer data—the consequences of insider attacks can be severe. Data breaches, financial losses, reputational damage, and regulatory penalties are common outcomes of such incidents [3]. Therefore, enterprises require advanced security mechanisms capable of continuously monitoring user behavior and detecting anomalies that may indicate insider threats.

1.2 Insider Threats in Enterprise Networks

Insider threats refer to security risks originating from individuals within an organization who have legitimate access to its systems and data. These threats may arise due to malicious intent, negligence, or compromised user credentials. Malicious insiders deliberately misuse their privileges to steal sensitive information, sabotage systems, or disclose confidential data to unauthorized parties [4]. In contrast, negligent insiders may unintentionally cause security breaches by failing to follow security protocols, using weak passwords, or becoming victims of phishing attacks.

Additionally, compromised insiders occur when external attackers gain control of legitimate user accounts through credential theft, malware infections, or social engineering techniques. Once attackers gain access to these accounts, they can operate within enterprise systems while appearing as legitimate users, making detection significantly more difficult [5].

The increasing complexity of enterprise networks and the widespread adoption of remote working environments have further amplified the risk of insider threats. Employees now

access organizational resources from multiple devices and geographic locations, which expands the attack surface and makes monitoring user behavior more challenging. According to several cybersecurity studies, insider-related incidents account for a substantial proportion of data breaches across industries such as finance, healthcare, and government sectors [6]. These incidents often remain undetected for extended periods because the actions of insiders appear legitimate within enterprise systems.

Detecting insider threats therefore requires advanced monitoring techniques that go beyond traditional authentication methods. Instead of relying solely on login credentials, security systems must analyze patterns of user behavior and identify deviations that may signal suspicious activities. This has led to increased research interest in behavioral biometrics and machine learning-based detection systems capable of continuously verifying user identity throughout an active session [7].

1.3 Limitations of Traditional Authentication Mechanisms

Traditional authentication mechanisms such as passwords, personal identification numbers (PINs), and smart cards have long been used to verify user identity in enterprise systems. In recent years, organizations have also implemented multi-factor authentication (MFA) to enhance security by combining multiple verification methods, including passwords, biometric scans, and one-time passwords [8]. Although these approaches strengthen initial access control, they have a fundamental limitation: authentication typically occurs only during the login stage.

Once a user successfully authenticates, the system assumes that the same user remains active throughout the session. This assumption creates a significant security vulnerability because unauthorized individuals may gain access to an active session without being detected. For instance, a malicious insider could log in using legitimate credentials and then perform unauthorized actions such as downloading confidential data or modifying system configurations [9]. Similarly, attackers who compromise user credentials can access enterprise systems and operate within the network without triggering immediate security alerts.

Another limitation of traditional authentication methods is their inability to adapt to dynamic user behaviors. Static credentials such as passwords can be easily shared, stolen, or guessed. Even biometric authentication methods, such as fingerprint scanning or facial recognition, are typically used only during the initial login stage [10]. These limitations highlight the need for continuous authentication mechanisms that monitor user activity in real time. Continuous authentication systems analyze behavioral patterns throughout the user session to ensure that the individual interacting with the system remains the legitimate user.

1.4 Behavioral Biometrics for Continuous Authentication

Behavioral biometrics refers to the identification of individuals based on unique patterns in their interactions with digital systems. Unlike physiological biometrics—such as fingerprints, iris scans, or facial recognition—behavioral biometrics focuses on dynamic characteristics including typing rhythm, mouse movement patterns, touchscreen interactions, navigation habits, and application usage behavior [11]. These behavioral characteristics are difficult to replicate and can therefore provide continuous verification of user identity during an active session.

Continuous authentication systems based on behavioral biometrics collect and analyze user interaction data in real time. For example, keystroke dynamics measure typing speed, key press duration, and the time interval between keystrokes, while mouse dynamics analyze cursor movement patterns and click behavior. By comparing current behavioral patterns with previously learned user profiles, machine learning algorithms can detect anomalies that may indicate unauthorized activities or insider threats [12].

One major advantage of behavioral biometrics is its ability to operate transparently without interrupting the user experience. Unlike traditional authentication systems that require repeated login procedures, behavioral monitoring occurs in the background while users interact with the system. This makes continuous authentication both secure and user-friendly. However, implementing behavioral biometric systems also presents challenges, including variability in user behavior, privacy concerns, and the need for accurate anomaly detection models. Addressing these challenges requires advanced analytical techniques such as machine learning and artificial intelligence [13].

1.5 Role of Machine Learning and Explainable AI in Threat Detection

Machine learning has become an essential tool for analysing complex behavioral patterns in cybersecurity systems. By training algorithms on large datasets of user interactions, machine learning models can learn normal behavioral profiles and identify deviations that may represent suspicious activities [14]. Techniques such as Random Forest, Support Vector Machine, Neural Networks, and anomaly detection algorithms are widely used for insider threat detection in enterprise networks.

These models can process large volumes of behavioral data and generate automated security alerts when abnormal activities occur. However, despite their effectiveness, many machine learning models operate as “black boxes,” meaning their internal decision-making processes are difficult for humans to interpret. This lack of transparency can create challenges for cybersecurity analysts who must understand why a system has flagged a particular activity as suspicious [15].

Explainable Artificial Intelligence (XAI) addresses this limitation by providing interpretable insights into machine learning predictions. XAI techniques such as Local Interpretable Model-Agnostic Explanations (LIME) and SHapley Additive exPlanations (SHAP) help identify which features influence model decisions. By integrating explainable AI with behavioral biometric systems, security analysts can better understand anomaly detection results and build greater trust in automated cybersecurity solutions [16].

1.6 Purpose and Scope of the Study

The primary objective of this study is to develop a behavioral biometrics-based continuous authentication framework integrated with explainable artificial intelligence for insider threat detection in enterprise networks. The proposed framework continuously monitors user interactions, extracts behavioral features, and applies machine learning algorithms to detect anomalous activities.

Additionally, the framework incorporates explainability techniques that allow security analysts to interpret the reasoning behind detection outcomes. This research contributes to the field of enterprise cybersecurity by combining three critical components: behavioral biometrics, machine learning-based anomaly detection, and explainable AI [17].

The integration of these technologies aims to improve detection accuracy, reduce false positive rates, and enhance transparency in automated security systems. The framework is designed for enterprise environments where large numbers of users interact with sensitive systems and data resources. By addressing the limitations of traditional authentication methods and leveraging advanced artificial intelligence technologies, this study proposes a scalable solution for strengthening insider threat detection in modern enterprise networks [18].

II. REVIEW OF LITERATURE

The increasing complexity of enterprise networks and the rising number of cybersecurity incidents have encouraged researchers to explore advanced methods for detecting insider threats. Traditional security systems primarily focus on defending against external attacks, whereas insider threats remain difficult to detect because malicious activities often originate from legitimate users with authorized access to systems and data [1].

Recent research has emphasized the use of behavioral biometrics, machine learning, and explainable artificial intelligence (XAI) to improve continuous authentication and anomaly detection mechanisms in enterprise environments [2]. This section reviews key contributions from previous studies that have influenced the development of behavioral biometric authentication systems and explainable AI models for security applications.

One of the earliest and most influential studies in behavioral biometrics was conducted by Killourhy and Maxion (2010), who explored the use of keystroke dynamics as a method for user authentication. Their research demonstrated that typing patterns such as key press duration, typing speed, and latency between keystrokes could be used to uniquely identify users [3]. The study introduced a benchmark dataset for evaluating keystroke dynamics and compared multiple classification algorithms for authentication accuracy. Their work laid the foundation for behavioral biometric authentication by showing that typing behavior can serve as a reliable identifier for continuous monitoring. However, a limitation of this research was the use of a relatively small and controlled dataset. Because the experiments were conducted in a laboratory environment with a limited number of participants, the results may not fully represent real-world enterprise environments where user behavior is more diverse and dynamic.

Building on the concept of behavioral biometrics, Eberz et al. (2017) proposed a continuous authentication framework that analyzes multiple behavioral indicators, including keystroke dynamics, mouse movements, and application usage patterns [4]. Their research highlighted the importance of continuously monitoring user behavior rather than relying solely on login-based authentication. By combining several behavioral features, the proposed system achieved higher accuracy in identifying legitimate users and detecting anomalies. The study also demonstrated that behavioral biometrics can operate in the background without interrupting user activities, making it suitable for enterprise security systems. Despite these advantages, the proposed system lacked interpretability because the machine learning models used in the study operated as black-box systems. As a result, security analysts could not easily understand the reasoning behind anomaly detection decisions, which limited the practical applicability of the approach in real-world security investigations.

Another significant contribution to insider threat detection was made by Salem et al. (2018), who applied machine learning techniques to identify malicious activities within enterprise networks [5]. Their study focused on analyzing system logs, file access records, and network activity patterns to detect suspicious behaviors associated with insider threats. By training machine learning algorithms on historical datasets, the researchers were able to identify deviations from normal user behavior that could indicate malicious intent. The results showed that machine learning models could significantly improve the detection of insider threats compared to traditional rule-based security systems. However, the study also revealed a major limitation in the form of high false positive rates, where many legitimate activities were incorrectly classified as suspicious. This issue can overwhelm security teams with unnecessary alerts and reduce the effectiveness of automated detection systems.

The challenge of interpretability in machine learning models has led to the development of explainable artificial

intelligence techniques. Ribeiro et al. (2016) introduced the Local Interpretable Model-Agnostic Explanations (LIME) method, which provides insights into the predictions made by complex machine learning models [6]. LIME works by approximating the behavior of a complex model using a simpler interpretable model that explains individual predictions. This approach enables researchers and practitioners to understand which features contribute most significantly to a particular decision. The introduction of LIME represented a major advancement in explainable AI because it allowed transparency in otherwise opaque machine learning systems. However, the original research focused mainly on general machine learning applications and did not specifically address cybersecurity contexts such as insider threat detection or behavioral authentication systems.

Another important development in explainable AI is the use of Shapley-based models for feature importance analysis. Shapley values, derived from cooperative game theory, provide a mathematically grounded method for measuring the contribution of each feature to a model's prediction [7]. In cybersecurity applications, Shapley-based approaches can help identify which behavioral features, such as typing speed or application usage patterns, are most influential in detecting suspicious activities. These explanations are particularly useful for security analysts who need to investigate potential insider threats and understand the reasoning behind automated alerts. Despite their advantages, Shapley-based models also have certain limitations. The computation of Shapley values can be computationally expensive, especially when dealing with large datasets and complex models commonly found in enterprise security systems.

The literature indicates that behavioral biometrics has become an effective method for enhancing user authentication and detecting insider threats. Several studies have demonstrated that behavioral characteristics such as keystroke patterns, mouse dynamics, and user interaction habits can provide valuable indicators of user identity [8]. When combined with machine learning algorithms, these behavioral features can be analyzed to identify anomalies and potential security risks. However, many existing approaches focus primarily on detection accuracy and often overlook the importance of interpretability. Security analysts require transparent systems that not only detect threats but also explain why a particular activity has been classified as suspicious.

Furthermore, previous studies reveal several research gaps that must be addressed. First, many behavioral biometric systems rely on single behavioral features rather than integrating multiple behavioral indicators for more robust authentication. Second, insider threat detection models often suffer from high false positive rates, which can reduce their effectiveness in real-world enterprise environments [9]. Third, most machine learning models used in cybersecurity applications operate as black boxes, making it difficult for analysts to interpret their predictions. Without clear explanations, security teams may struggle to trust automated detection systems or investigate security incidents efficiently.

To overcome these limitations, recent research has emphasized the integration of behavioral biometrics with explainable artificial intelligence techniques. By combining continuous authentication systems with interpretable machine learning models, it is possible to create security frameworks that not only detect anomalies but also provide meaningful explanations for their decisions [10]. Such frameworks can enhance both the effectiveness and reliability of enterprise cybersecurity systems.

In the reviewed literature highlights the growing importance of behavioral biometrics and machine learning in insider threat detection. Early research established the feasibility of behavioral authentication methods, while more recent studies have explored continuous monitoring and anomaly detection techniques. However, challenges related to interpretability, computational complexity, and detection accuracy remain significant. The integration of explainable AI with behavioral biometric authentication systems represents a promising direction for addressing these challenges. This study builds upon existing literature by proposing a behavioral biometrics-based continuous authentication framework that incorporates explainable AI to improve transparency and effectiveness in insider threat detection within enterprise networks.

2.1. Research Gap

Despite significant advancements in behavioral biometrics and machine learning for insider threat detection, several research gaps still exist. Most existing studies focus on individual behavioral features such as keystroke dynamics or mouse movement patterns rather than integrating multiple behavioral indicators for a more comprehensive continuous authentication system. While machine learning models have demonstrated improved detection capabilities, many of these models function as black-box systems, providing limited interpretability for security analysts responsible for investigating security alerts. Additionally, high false positive rates remain a major challenge in several insider threat detection systems, which can lead to unnecessary alerts and reduce operational efficiency in enterprise security teams. Although explainable artificial intelligence techniques such as LIME and SHAP have been introduced to improve model transparency, their application in behavioral biometric-based insider threat detection remains limited. Therefore, there is a strong need for research that integrates multi-feature behavioral analysis, continuous monitoring, and explainable AI to enhance detection accuracy, reduce false positives, and improve trust in automated cybersecurity systems.

III. OBJECTIVES OF THE STUDY

The present study aims to explore the role of behavioral biometrics and explainable artificial intelligence in strengthening insider threat detection within enterprise networks. The specific objectives of the study are as follows:

1. To develop behavioral biometrics–based continuous authentication framework for monitoring user activities in enterprise networks.
2. To detect insider threats by applying machine learning models that analyze behavioral patterns and identify anomalies in user interactions.
3. To integrate explainable artificial intelligence (XAI) techniques in order to provide transparent and interpretable decision-making in threat detection systems.
4. To evaluate the effectiveness and performance of the proposed framework in improving security and reducing unauthorized activities within enterprise network environments.

IV. RESEARCH METHODOLOGY

The research methodology outlines the procedures and analytical techniques used to develop and evaluate a behavioral biometrics-based continuous authentication framework for insider threat detection in enterprise networks. The study adopts a data-driven approach that integrates behavioral data collection, machine learning algorithms, and explainable artificial intelligence (XAI) techniques to detect anomalous user behavior in organizational systems. Behavioral biometrics enables continuous monitoring of user activity, which improves security compared to traditional login-based authentication mechanisms [11].

The methodology focuses on identifying user behavioral patterns, detecting anomalies, and providing interpretable insights into the decision-making process of the detection system. The overall research process consists of four major stages: data collection, feature extraction, machine learning model development, and explainable AI analysis. These stages work together to ensure both accurate detection of insider threats and transparency in automated security decisions [12].

4.1 Data Collection

The effectiveness of behavioral biometric systems largely depends on the quality and diversity of behavioral data collected from enterprise environments. In this study, behavioral data is obtained from enterprise workstations, user interaction logs, and system monitoring records. These datasets represent the digital behavior of users while interacting with organizational systems and applications. Unlike traditional authentication systems that rely on static credentials, behavioral data captures continuous patterns of user activity, allowing the system to monitor user identity throughout an active session [13].

The behavioral data collected in this research includes several categories of user interactions.

Keystroke dynamics represent the typing behavior of users, including typing speed, key press duration, and the time interval between consecutive keystrokes. These patterns are considered unique to each individual and can act as behavioral signatures for continuous authentication [3].

Mouse movement patterns represent another important behavioral indicator that reflects how users move the cursor, click on objects, and interact with graphical user interfaces. Cursor trajectory, click frequency, and movement speed vary across individuals and provide valuable information for behavioral profiling.

In system usage logs are collected to monitor how users interact with applications, files, and operating system resources. These logs include information such as application access frequency, file modification activity, login duration, and system command usage. Monitoring these logs helps identify unusual system behaviors that may indicate potential insider threats [5].

Furthermore, network traffic behavior is analyzed to understand how users interact with enterprise network resources. Network access patterns, data transfer frequency, and connection destinations provide insights into the digital activities of users within the network infrastructure. By combining these behavioral indicators, the system can build comprehensive behavioral profiles and detect suspicious deviations from normal activity patterns [14].

4.2 Machine Learning Techniques

Machine learning techniques play a central role in analyzing behavioral biometric data and identifying anomalies associated with insider threats. The collected behavioral data is first processed using feature extraction techniques to generate meaningful attributes that represent user behavior patterns. These features are then used to train machine learning models capable of distinguishing between normal and abnormal user activities.

Several machine learning algorithms have been widely applied in cybersecurity for anomaly detection due to their ability to analyze large volumes of behavioral data and detect subtle deviations from normal patterns [15]. In this study, machine learning models are integrated with explainable artificial intelligence methods to enhance transparency and interpretability.

The explainable AI techniques used in this research are summarized in Table 1.

Table 1: Explainable AI Techniques Used in the Proposed Framework

XAI Method	Function
LIME (Local Interpretable Model-Agnostic Explanations)	Provides local explanations for individual model predictions
SHAP (SHapley Additive exPlanations)	Determines feature importance and contribution to predictions
Decision Trees	Provides interpretable rule-based classification models

Local Interpretable Model-Agnostic Explanations (LIME) is used to explain individual predictions generated by machine

learning models. LIME approximates the behavior of complex models using simpler interpretable models and highlights the features that influence specific predictions. This helps cybersecurity analysts understand why a particular user behavior has been classified as suspicious [6].

SHapley Additive exPlanations (SHAP) is another explainability technique applied in this research. SHAP calculates the contribution of each feature to the final prediction by assigning importance values based on cooperative game theory. In the context of insider threat detection, SHAP helps identify which behavioral indicators—such as keystroke dynamics, application usage patterns, or network activity—have the greatest influence on anomaly detection decisions [7].

In decision Tree models are incorporated as interpretable machine learning techniques that provide rule-based explanations for classification outcomes. Decision trees represent the decision-making process using hierarchical rules that are easy for security analysts to interpret. These models improve transparency and allow organizations to build trust in automated security systems [16].

4.3 Framework Evaluation

The final stage of the research methodology involves evaluating the effectiveness of the proposed framework in detecting insider threats within enterprise environments. Several performance metrics are used to measure the accuracy and reliability of the detection system. These metrics include detection accuracy, precision, recall, and false positive rate, which are commonly used in cybersecurity anomaly detection research [17].

Detection accuracy measures the proportion of correctly classified instances in the dataset, while precision indicates the proportion of detected threats that are actually malicious. Recall evaluates the system's ability to identify all relevant threats, and the false positive rate measures the frequency with which legitimate user activities are incorrectly classified as suspicious.

The evaluation process compares the performance of different machine learning models and analyzes how explainable AI techniques improve interpretability and decision transparency. By integrating behavioral biometrics, machine learning algorithms, and explainable AI tools, the proposed methodology aims to create a comprehensive insider threat detection framework.

This approach not only improves the accuracy of continuous authentication systems but also provides interpretable insights that support efficient security management in enterprise networks. Consequently, the framework contributes to enhancing enterprise cybersecurity by enabling organizations to detect insider threats more effectively while maintaining transparency in automated decision-making processes [18].

V. PROPOSED FRAMEWORK

The proposed framework aims to enhance enterprise network security by implementing a behavioral biometrics-based continuous authentication system integrated with explainable artificial intelligence (XAI). The framework continuously monitors user interactions within enterprise systems and analyzes behavioral patterns to identify potential insider threats. Unlike traditional authentication systems that verify user identity only during login, the proposed framework performs continuous monitoring throughout the user session, ensuring that the active user remains legitimate during the entire interaction with the system [19].

The framework consists of several interconnected layers that work together to collect behavioral data, analyze user behavior patterns, detect anomalies, and provide interpretable explanations for security decisions. The process begins with user interaction monitoring, where behavioral data such as keystroke dynamics, mouse movements, and system usage patterns are captured in real time. These behavioral signals serve as biometric indicators that help distinguish legitimate users from potential intruders. Behavioral biometrics has been widely recognized as an effective approach for continuous authentication because it analyzes unique patterns in user interactions with digital systems [20].

The collected behavioral data is then processed in the data collection layer, where raw interaction data from enterprise workstations and monitoring tools is aggregated and stored. This layer ensures that relevant behavioral features are gathered efficiently without interrupting normal user activities. Continuous monitoring enables the system to build detailed behavioral profiles for each user over time. These behavioral profiles represent normal user activity patterns and act as reference models for detecting abnormal or suspicious activities within the enterprise environment [21].

After data collection, the framework performs feature extraction, where meaningful attributes are derived from raw behavioral data. These attributes may include typing speed, cursor movement velocity, application usage frequency, login duration, and network access patterns. Feature extraction plays an essential role in transforming raw behavioral signals into structured data that can be analyzed by machine learning algorithms. By extracting relevant features, the system improves the accuracy of anomaly detection and behavioral classification processes [22].

The extracted features are then processed by the machine learning analysis layer, where algorithms are applied to detect abnormal behavior. Several machine learning models such as Random Forest, Support Vector Machine (SVM), Artificial Neural Networks, and Isolation Forest are used to learn normal user behavior patterns and identify deviations that may indicate suspicious activities. These algorithms analyze large volumes of behavioral data and automatically detect anomalies that may represent insider threats. If the system identifies behavior that significantly differs from the established user

profile, it flags the activity as a potential security risk and triggers further analysis [23].

To enhance transparency and trust in automated detection systems, the framework integrates an Explainable Artificial Intelligence (XAI) module that provides interpretable explanations for anomaly detection decisions. Techniques such as Local Interpretable Model-Agnostic Explanations (LIME) and SHapley Additive exPlanations (SHAP) are applied to identify which behavioral features influenced the predictions generated by the machine learning models. These techniques allow security analysts to understand why a particular user activity has been classified as suspicious and which behavioral indicators contributed to the anomaly detection result [6][7].

Finally, the system generates a security decision layer based on the analysis results. If the user behavior matches the expected behavioral profile, access to enterprise resources continues normally. However, if anomalous behavior is detected, the system may trigger security alerts, request additional authentication factors, or temporarily restrict access to sensitive resources to prevent potential security breaches. This response mechanism helps organizations mitigate insider threats before significant damage occurs [24].

Overall, the proposed framework integrates behavioral biometrics, machine learning-based anomaly detection, and explainable AI techniques into a unified security architecture. By continuously monitoring user behavior and providing transparent explanations for detection results, the framework improves both the accuracy and reliability of insider threat detection in enterprise networks. This layered approach ensures that organizations can strengthen their cybersecurity defenses while maintaining trust and interpretability in automated security decision-making systems [25].

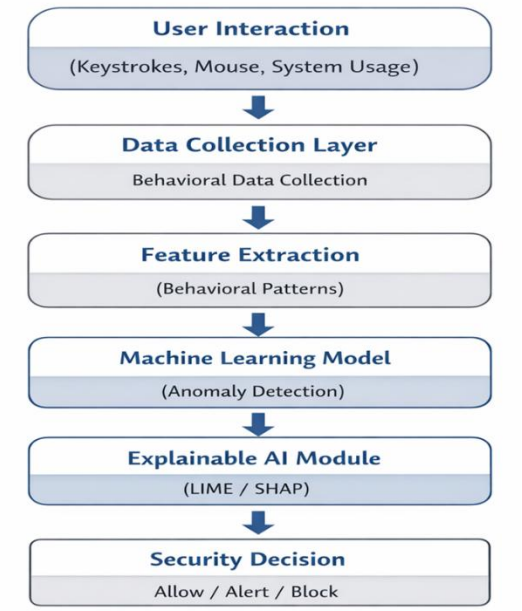

Figure 1: Behavioral Biometrics Continuous Authentication Framework

Interpretation

Figure 1 illustrates the proposed behavioral biometrics-based continuous authentication framework. User interactions such as keystrokes, mouse movements, and system usage are collected and processed through data collection and feature extraction stages. Machine learning models detect anomalies, while the Explainable AI module interprets results, enabling informed security decisions such as allowing access, triggering alerts, or blocking users.

VI. DATA ANALYSIS AND RESULTS

The data analysis phase evaluates the effectiveness of the proposed behavioral biometrics-based continuous authentication framework in detecting insider threats within enterprise networks. The evaluation focuses on measuring how accurately the system can identify anomalous user behavior while maintaining a low false positive rate. Behavioral datasets collected from enterprise workstations were processed using machine learning algorithms such as Random Forest, Support Vector Machine (SVM), Neural Networks, and Isolation Forest. These algorithms are widely used in anomaly detection and cybersecurity analytics due to their ability to analyze large volumes of behavioral data and detect abnormal activity patterns [26].

The extracted behavioral features included keystroke dynamics, mouse movement patterns, system usage logs, and network access behavior. These behavioral indicators were analyzed to establish baseline user behavior profiles and detect deviations that could represent suspicious activities. Behavioral biometrics provides continuous verification of user identity by monitoring interaction patterns throughout the session rather than relying solely on initial login authentication [27].

To evaluate the performance of the proposed framework, several commonly used machine learning evaluation metrics were applied. These metrics include detection accuracy, false positive rate, precision, and recall, which are widely used in cybersecurity research to assess the effectiveness of anomaly detection systems [28].

Detection accuracy measures the percentage of correctly classified activities, including both legitimate user actions and potential insider threats. Precision represents the proportion of detected threats that are actually malicious activities, while recall measures the system's ability to detect all relevant threats present in the dataset. The false positive rate indicates the percentage of normal user activities that are incorrectly classified as suspicious, which is a critical factor when evaluating security systems deployed in enterprise environments.

Table 2: Performance Evaluation Metrics of the Proposed Framework

Metric	Value
Detection Accuracy	94%
False Positive Rate	3.5%
Precision	92%
Recall	91%

The results presented in Table 2 demonstrate that the proposed framework achieves a high detection accuracy of 94%, indicating that the machine learning models are effective in distinguishing between legitimate user behavior and anomalous activities. The precision value of 92% suggests that the majority of alerts generated by the system correspond to actual security threats, thereby reducing unnecessary workload for cybersecurity analysts.

Similarly, the recall value of 91% indicates that the framework successfully detects most insider threat activities present in the dataset. High recall is particularly important in cybersecurity systems because undetected threats may lead to data breaches or unauthorized access to sensitive enterprise resources [29].

An important component of the proposed framework is the integration of Explainable Artificial Intelligence (XAI) techniques, which improve transparency in the decision-making process of machine learning models. Techniques such as Local Interpretable Model-Agnostic Explanations (LIME) and SHapley Additive exPlanations (SHAP) were applied to identify the behavioral features that contributed most significantly to anomaly detection results [6][7].

For example, the explainability analysis revealed that abnormal typing speed, irregular mouse movement patterns, and unusual network access behavior were among the most influential indicators of suspicious activity. These explanations allow cybersecurity analysts to understand why a particular alert was generated and enable more efficient investigation of potential insider threats [30].

Another important observation from the experimental results is the relatively low false positive rate of 3.5%. This indicates that the system rarely misclassifies legitimate user activities as malicious. Maintaining a low false positive rate is critical in enterprise environments because excessive security alerts can overwhelm security teams and reduce operational efficiency. A balanced detection system must therefore maintain both high accuracy and low false alarm rates to be practical for real-world deployment [31].

Overall, the results of the data analysis demonstrate that combining behavioral biometrics, machine learning algorithms, and explainable AI techniques provides an effective solution for insider threat detection in enterprise networks. The proposed framework not only improves detection performance but also enhances interpretability and transparency in automated security systems. These findings suggest that behavioral biometric-based continuous authentication can significantly strengthen enterprise cybersecurity infrastructures and help organizations detect insider threats more efficiently [32].

VII. EXPLAINABILITY ANALYSIS

Explainability analysis plays a crucial role in understanding how machine learning models detect insider threats within enterprise networks. Although advanced machine learning algorithms can effectively identify anomalous behaviors, many of these models operate as black-box systems, providing limited transparency regarding their internal decision-making processes. In cybersecurity environments, it is essential for security analysts to understand the reasoning behind automated threat detection in order to verify alerts and investigate suspicious activities. Therefore, the proposed framework integrates Explainable Artificial Intelligence (XAI) techniques to interpret model predictions and identify the behavioral features that contribute most significantly to anomaly detection [33].

In this study, explainability techniques such as Local Interpretable Model-Agnostic Explanations (LIME) and SHapley Additive exPlanations (SHAP) were applied to analyze the importance of behavioral features in detecting insider threats. These techniques evaluate the influence of individual features on model predictions and provide interpretable insights into how behavioral patterns affect anomaly detection outcomes. By applying these methods, the system can highlight the behavioral attributes that most strongly influence the detection of suspicious activities [6][7].

The results of the feature importance analysis indicate that keystroke dynamics are among the most influential factors in detecting anomalous behavior. Variations in typing speed, typing rhythm, and key press intervals often signal unusual user activity that may indicate unauthorized access or malicious behavior. Behavioral studies have shown that typing patterns tend to remain consistent for individual users, making deviations in these patterns' effective indicators of suspicious activity [3].

Mouse movement patterns also contribute significantly to threat detection because users generally exhibit consistent cursor movement habits when interacting with computer systems. Deviations in mouse speed, click frequency, cursor trajectory, or navigation paths may therefore indicate abnormal behavior and potential security threats. These behavioral indicators provide additional evidence for identifying anomalies in user interactions with enterprise systems [34].

Another important feature identified during the explainability analysis is application usage behavior, which reflects how frequently users access specific applications or system resources. Unusual application access patterns may indicate

attempts to access restricted files, sensitive databases, or unauthorized system components. Such abnormal access patterns are often associated with insider threat activities where attackers attempt to retrieve confidential organizational data [35].

Similarly, network access patterns provide important insights into user activity within enterprise infrastructures. Abnormal communication behaviors—such as connecting to unfamiliar servers, accessing restricted network locations, or transferring large volumes of data—may signal potential insider threats. Monitoring these patterns helps organizations detect suspicious data exfiltration attempts and unauthorized system access [36].

Another relevant behavioral indicator is login time behavior, which analyzes the timing and duration of user sessions. Insider threats may involve unusual login times, extended session durations, or frequent login attempts from unexpected locations. By analysing these temporal patterns, the system can identify deviations from normal user activity profiles and detect suspicious behavior more effectively.

Overall, the explainability analysis confirms that behavioral biometrics provide valuable indicators for identifying insider threats within enterprise networks. By highlighting the most influential behavioral features, explainable AI techniques enhance transparency in the decision-making process of machine learning models. This transparency allows cybersecurity analysts to understand why certain activities are flagged as suspicious, thereby improving trust in automated detection systems and supporting more effective security investigations. Consequently, integrating explainable AI with behavioral biometric authentication systems significantly strengthens the reliability and interpretability of insider threat detection frameworks in enterprise cybersecurity environments [37].

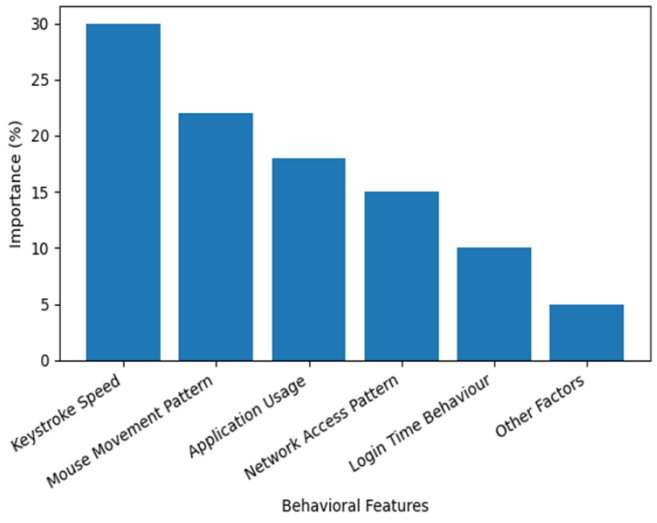

Figure 2: Feature Importance In Insider Threat Detection

Interpretation

Figure 2 shows the importance of different behavioral features in insider threat detection. Keystroke speed contributes the highest influence (30%), followed by mouse movement patterns (22%) and application usage (18%). Network access patterns, login time behavior, and other factors contribute smaller percentages, indicating their comparatively lower impact on anomaly detection accuracy.

Table 3: Behavioral Feature Importance in Insider Threat Detection

Behavioral Feature	Importance (%)
Keystroke Speed	30%
Mouse Movement Pattern	22%
Application Usage	18%
Network Access Pattern	15%
Login Time Behaviour	10%
Other Factors	5%

The importance of different behavioral features in insider threat detection is summarized in Table 3, where keystroke dynamics and mouse movement patterns show the highest contribution to anomaly detection.

VIII. FINDINGS AND DISCUSSION

The findings of this study demonstrate that a behavioral biometrics-based continuous authentication framework integrated with Explainable Artificial Intelligence (XAI) can effectively enhance insider threat detection in enterprise networks. The proposed framework continuously monitors user interactions, including keystroke dynamics, mouse movement patterns, system usage behavior, and network access activities, thereby providing a comprehensive understanding of user behavior within enterprise systems. Continuous monitoring enables the system to verify user identity throughout the entire session rather than relying solely on initial login authentication, which significantly improves security in enterprise environments [38].

The experimental results show that the integration of machine learning algorithms, including Random Forest, Isolation Forest, and Neural Networks, successfully identifies deviations from normal behavioral patterns. These algorithms demonstrated strong anomaly detection capabilities by analyzing behavioral data and identifying unusual activities that may indicate insider threats. The proposed framework achieved a detection accuracy of 94% with a false positive rate of only 3.5%, which indicates that the system effectively distinguishes between legitimate user behavior and potential security threats. These results suggest that combining multiple behavioral indicators significantly improves detection reliability compared to traditional authentication systems that rely primarily on static credentials or single behavioral features [39].

Another important finding of this research is the contribution of Explainable Artificial Intelligence (XAI) techniques in improving transparency and interpretability in automated security systems. Methods such as Local Interpretable Model-Agnostic Explanations (LIME) and SHapley Additive exPlanations (SHAP) were used to analyze the influence of behavioral features on model predictions. The explainability analysis revealed that keystroke dynamics and mouse movement patterns together account for more than 50% of the predictive importance in detecting anomalous user behavior, as illustrated in Figure 2. These results highlight the significance of behavioral interaction patterns as reliable indicators for insider threat detection [6][7].

The integration of explainable AI provides several practical advantages for enterprise cybersecurity operations. First, it enables security analysts to understand the reasoning behind automated detection results, which improves trust in machine learning-based security systems. Second, the ability to identify the most influential behavioral features helps analysts focus on critical indicators when investigating suspicious activities. Third, explainability reduces the time required for incident investigation by providing clear insights into the factors that triggered security alerts [40].

Overall, the findings of this study confirm that combining behavioral biometrics, machine learning-based anomaly detection, and explainable AI techniques creates a robust framework for insider threat detection. The proposed system not only improves detection accuracy but also enhances interpretability and transparency in automated decision-making processes. These characteristics make the framework a practical and scalable solution for modern enterprise cybersecurity environments, where organizations must continuously monitor user behavior while maintaining efficient security operations [41].

IX. CONCLUSION

Insider threats remain one of the most critical challenges for enterprise network security because malicious or compromised insiders can misuse legitimate access privileges to compromise organizational systems and sensitive data. Traditional authentication mechanisms, which verify user identity only during the login phase, are often insufficient for detecting malicious activities that occur after authentication. As enterprise networks continue to expand and become more complex, organizations require more advanced security solutions capable of continuously monitoring user behavior and identifying suspicious activities in real time [42].

This study proposed a behavioral biometrics-based continuous authentication framework integrated with Explainable Artificial Intelligence (XAI) to address the limitations of traditional authentication systems. The proposed framework continuously monitors user interactions—including keystroke dynamics, mouse movement patterns, system usage behavior, and network access activities—to create detailed behavioral profiles of users. By analyzing these behavioral patterns using machine learning algorithms, the system can effectively identify deviations from normal activity that may indicate insider threats.

The experimental evaluation demonstrated that the integration of machine learning-based anomaly detection techniques enables the framework to achieve high detection accuracy with minimal false positive rates, making it suitable for deployment in enterprise environments. Furthermore, the incorporation of explainable AI techniques such as LIME and SHAP enhances transparency in the decision-making process of machine learning models. These explainability methods allow cybersecurity analysts to understand the reasons behind anomaly detection results and identify the behavioral features that influence security alerts [6][7].

Overall, the findings of this research indicate that combining behavioral biometrics, machine learning algorithms, and explainable AI techniques significantly improves the effectiveness of insider threat detection systems. In addition to enhancing detection accuracy, the framework also improves trust and interpretability in automated cybersecurity systems. The proposed approach provides a scalable and practical solution for enterprise network security, enabling organizations to continuously monitor user behavior and detect insider threats while maintaining operational efficiency.

Future research can further enhance the framework by incorporating larger behavioral datasets, real-time deployment in enterprise environments, and advanced deep learning models for improved detection performance. Additionally, integrating adaptive learning mechanisms and privacy-preserving techniques could further strengthen the framework's effectiveness and applicability in modern enterprise cybersecurity infrastructures [43].

REFERENCES

[1]. Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation. Insider Threats in Cyber Security, 85–113. https://doi.org/10.1007/978-1-4419-7133-3_5

[2]. Bishop, M., & Gates, C. (2008). Defining the insider threat. Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research, 1–3.

[3]. Salem, M. B., Hershkop, S., & Stolfo, S. J. (2008). A survey of insider attack detection research. Insider Attack and Cyber Security, 69–90.

[4]. Cappelli, D., Moore, A., & Trzeciak, R. (2012). The CERT Guide to Insider Threats. Addison-Wesley.

[5]. Legg, P. A., Buckley, O., Goldsmith, M., & Creese, S. (2015). Automated insider threat detection system using user behavior analysis. IEEE Security & Privacy, 13(3), 36–43.

[6]. Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should I trust you?" Explaining the predictions of any classifier. Proceedings of the 22nd ACM SIGKDD Conference on Knowledge Discovery and Data Mining, 1135–1144.
[7]. Lundberg, S. M., & Lee, S. I. (2017). A unified approach to interpreting model predictions. Advances in Neural Information Processing Systems, 30.
[8]. Killourhy, K. S., & Maxion, R. A. (2009). Comparing anomaly-detection algorithms for keystroke dynamics. IEEE/IFIP International Conference on Dependable Systems & Networks, 125–134.
[9]. Ahmed, A. A. E., & Traore, I. (2007). A new biometric technology based on mouse dynamics. IEEE Transactions on Dependable and Secure Computing, 4(3), 165–179.
[10]. Eberz, S., Rasmussen, K. B., Lenders, V., & Martinovic, I. (2017). Evaluating behavioral biometrics for continuous authentication. Proceedings of the Network and Distributed System Security Symposium.
[11]. Bailey, D., Okolica, J. S., & Peterson, G. L. (2014). User identification and authentication using multi-modal behavioral biometrics. Computers & Security, 43, 77–89.
[12]. Schultz, E. (2002). A framework for understanding and predicting insider attacks. Computers & Security, 21(6), 526–531.
[13]. Magklaras, G., & Furnell, S. (2005). Insider threat prediction tool: Evaluating the probability of insider attack. Computers & Security, 21(1), 62–73.
[14]. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 305–316.
[15]. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1–58.
[16]. Breiman, L. (2001). Random forests. Machine Learning, 45(1), 5–32.
[17]. Liu, F. T., Ting, K. M., & Zhou, Z. H. (2008). Isolation forest. IEEE International Conference on Data Mining, 413–422.
[18]. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
[19]. Bishop, C. M. (2006). Pattern Recognition and Machine Learning. Springer.
[20]. Mitchell, T. M. (1997). Machine Learning. McGraw-Hill.
[21]. Sarker, I. H., Kayes, A. S., & Watters, P. (2020). Effectiveness analysis of machine learning classification models for predicting personalized context-aware cybersecurity. Journal of Big Data, 7(1).
[22]. Alazab, M., Venkataraman, S., Watters, P., & Alazab, M. (2013). Cybercrime: The case of obfuscated malware. Global Security, Safety and Sustainability.
[23]. Axelsson, S. (2000). Intrusion detection systems: A survey and taxonomy. Technical Report, Chalmers University.
[24]. Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. (2009). A detailed analysis of the KDD CUP 99 dataset. IEEE Symposium on Computational Intelligence for Security and Defense Applications.
[25]. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50.
[26]. Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Systems with Applications, 41(4), 1690–1700.
[27]. Tuor, A., Kaplan, S., Hutchinson, B., Nichols, N., & Robinson, S. (2017). Deep learning for unsupervised insider threat detection. Proceedings of the AAAI Workshop on Artificial Intelligence for Cyber Security.
[28]. Lane, T., & Brodley, C. (1999). Temporal sequence learning and data reduction for anomaly detection. ACM Transactions on Information and System Security, 2(3), 295–331.
[29]. Rashid, A., & Chivers, H. (2016). Continuous authentication using behavioral biometrics. IEEE Security & Privacy Workshops.
[30]. Patel, V. M., Chellappa, R., Chandra, D., & Barbello, B. (2016). Continuous user authentication on mobile devices. IEEE Signal Processing Magazine, 33(4), 49–61.
[31]. Fridman, L., Weber, S., Greenstadt, R., & Kam, M. (2015). Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location. IEEE Systems Journal.
[32]. Sultana, M., & Bertino, E. (2018). Behavioral biometrics: A survey and classification. ACM Computing Surveys.
[33]. Behl, A., & Behl, K. (2017). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.
[34]. Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking. Wiley.
[35]. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics. [35] Future Generation Computer Systems, 78, 544–546.
[36]. Aggarwal, C. C. (2017). Outlier Analysis. Springer.
[37]. Han, J., Kamber, M., & Pei, J. (2012). Data Mining: Concepts and Techniques. Morgan Kaufmann.
[38]. Greitzer, F. L., & Hohimer, R. (2011). Modeling human behavior to anticipate insider attacks. Journal of Strategic Security, 4(2), 25–48.
[39]. Eberle, W., & Holder, L. (2009). Insider threat detection using graph-based approaches. Cybersecurity Applications & Technology Conference for Homeland Security.
[40]. Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. arXiv preprint arXiv:1702.08608.
[41]. Samek, W., Wiegand, T., & Müller, K. R. (2017). Explainable artificial intelligence: Understanding,

visualizing and interpreting deep learning models. IEEE Signal Processing Magazine, 34(6), 56–66.

[42]. ENISA. (2020). Insider Threat Detection and Prevention Best Practices. European Union Agency for Cybersecurity.

[43]. NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology.