Grenze International Journal of Engineering and Technology, June Issue

Biotrap: Biometric Honeytrap Security System

Aparna R[1], Gagan K J[2], Shrusti Goud[3], Suchithra B S[4] and Vasudha C P[5]
[1-5]Department of ISE, Siddaganga Institute of Technology, Visvesvaraya Technological University, Tumakuru, Karnataka, India
Email: raparna@sit.ac.in, gagankj4@gmail.com, shrustigoud2004@gmail.com, suchithrabs3924@gmail.com, vasudhacp1@gmail.com

Abstract*— Traditional authentication and access control sys-tems in contemporary cybersecurity environments mainly follow a binary allow-or-deny model, which restricts their capacity to comprehend attacker intent or obtain useful intelligence. Even though these systems might be effective in preventing unwanted access, they frequently fall short in identifying, evaluating, and correlating malicious activity across multiple intrusion attempts. As a result, chances for intelligence-driven defense and long-term threat profiling are lost. This paper introduces BioTrap, a Biometric Honeytrap Security System that combines behavioral biometrics, deep learning-based anomaly detection, and deception technology. A completely isolated honeytrap environment that mimics authentic application interfaces is where suspicious login attempts are dynamically redirected. This decoy system continu-ously records and analyzes fine-grained behavioral signals, such as mouse movements, keystroke dynamics, navigation patterns, and session timing. These time-series interactions are processed by a Long Short-Term Memory (LSTM) model to produce anomaly scores and compact behavioral embeddings, which are then saved in a vector database for attacker correlation and cross-session similarity analysis. BioTrap converts intrusion attempts into opportunities for intelligence gathering through the combination of deception-based engagement and real-time behavioral analysis. The proposed system is designed for scal-ability in the cloud, maintains privacy through anonymization and data retention policies, and enables adaptive multi-factor authentication to reduce false positives. The effectiveness of BioTrap in distinguishing between malicious and legitimate users and enabling long-term behavioral fingerprinting and threat attribution is validated through experimental evaluation.

***Keywords*— Behavioral Biometrics, Honeytrap, Cybersecurity, LSTM, Anomaly Detection, Deception Technology, Vector Em-beddings.**

I. INTRODUCTION

The attack surface of contemporary information systems has greatly increased due to the quick development of cloud-based apps and digital services. In order to get around traditional security measures [9], [13], [16], cyber adversaries are increasingly using automated bots, stolen credentials, and adaptive intrusion techniques [13], [17], [21]. Conventional authentication methods, such as multi-factor authentication and password-based logins, mainly use a binary decision model that allows or prohibits access [23]. Although these methods work well to stop unwanted access right away, they don't produce useful intelligence after an intrusion attempt is stopped and offer little insight into the behavior of the attacker.

Grenze ID: 01.GIJET.12.2.666_26

Deception-driven security methods, such as honeypots and honeytraps, have emerged as a preventive defense mechanism to counter this limitation [2], [10], [11]. These systems misdirect attackers towards a decoy environment where their behavior can be monitored without risk, rather than blocking them altogether. Nevertheless, the conventional honeypot solution typically focuses on surface-level cues such as Internet Protocol addresses or request logs and tends to focus on the network or system level. Such cues lack a reliable correlation between multiple instances of attack attempts from different sessions or identities and are prone to deception.

Behavioral biometrics provides a promising answer to this challenge by examining how users interact with systems rather than focusing on static credentials. Keystroke dynamics, mouse movements, navigation patterns, and timing patterns are difficult to mimic and remain relatively stable from session to session [1], [12], [15]. When paired with machine learning algorithms that are able to process sequential data, behavioral biometrics can provide real-time authentication and anomaly detection [3], [8]. In this paper, the BioTrap Biometric Honey-trap Security System is proposed, which combines deception technology with behavioral biometrics and deep learning-based analysis. The system assesses login attempts based on contextual and behavioral risk factors and chooses to redirect malicious sessions to a fully isolated honeytrap environment that simulates the legitimate application as closely as possible. [10] In this environment, user behavior is continuously monitored and analyzed using a Long Short-Term Memory (LSTM) model to produce anomaly scores and behavioral embeddings [4]. These embeddings support long-term attacker fingerprinting and correlation across multiple attack attempts, even if surface-level identifiers are changed.

BioTrap goes beyond the traditional reactive models of defense by turning intrusion attempts into opportunities for intelligence gathering. The proposed solution improves the visibility of security, minimizes false positives by adapting verification processes, and is deployable on a cloud scale while respecting privacy and ethical standards.

II. Literature Survey

The rising complexity of cyber threats has fueled research into approaches that move beyond the conventional authentication and perimeter defense strategies to more adaptive and intelligence-led defense approaches. Current research trends include behavioral biometrics, deception technologies, and machine learning-based anomaly detection as promising methods for detecting malicious traffic that evades conventional defenses. This section discusses existing research work that is relevant to the development of the BioTrap system, including behavioral identity verification, deception technologies, deep learning-based sequence modeling, vector-based attacker correlation, and the shortcomings of existing solutions [9], [13].

1) Behavioral Biometrics in Cybersecurity: Behavioral biometrics has been identified as a trustworthy technique for user authentication based on the observation of how people interact with computer systems rather than static credentials [1], [2], [15], [18].Previous studies have shown that characteristics such as keystroke dynamics, mouse movement patterns, and navigation patterns are highly associated with neuromotor behaviors and are very difficult to replicate or spoof. These patterns remain relatively stable across different sessions and devices, allowing for continuous and passive authentication [1].

Research studies on social and behavioral biometrics have also emphasized the efficacy of observing interaction patterns in real-time without affecting the user experience. These studies have emphasized non-intrusive authentication techniques and have been found to be very effective in identifying account compromise attacks where the attacker already has valid credentials.

A. Deception Technology and Honeytrap Systems

Deception technology, such as honeypots and honeytraps, has been extensively researched as a proactive means of defense [2], [10], [11]. Rather than simply blocking malicious traffic, deception technology steers malicious actors towards controlled decoy environments that mimic valuable resources. This enables defenders to monitor malicious activity, tactics, and intentions without impacting production environments.

Current research is mainly centered on network honeypots that record elementary information like IP addresses, request data, or command data. Although useful for initial threat detection, these systems tend to be application-agnostic and do not track malicious activity across multiple connections.

More recent research suggests authentication deception tac-tics, such as steering malicious login attempts towards decoy dashboards, which is very much in line with BioTrap’s decoy environment concept of extending malicious engagement and data gathering.

B. Machine Learning Models for Behavioral Anomaly Detection

Machine learning models have emerged as popular choices for modeling user behavior and performing anomaly detection in the field of cybersecurity. Among the different machine learning models, Long Short-Term Memory (LSTM) networks have been identified as highly effective models for modeling sequential data, including time-series data, by learning long-term dependencies. [3], [8] The basic research work on LSTM models has demonstrated their effectiveness in modeling complex temporal patterns, which are hard to learn using traditional models [3], [4], [20].

Subsequent research work has applied LSTM models for intrusion detection and behavioral analysis, demonstrating their effectiveness in distinguishing normal user behavior from malicious and automated behavior [4], [13]. The outcomes have demonstrated the effectiveness of deep learning models for real-time behavioral risk scoring and have validated Bio-Trap's choice of using LSTM networks for anomaly detection in interactive sessions [5], [7].

C. Vector Embeddings and Identity Correlation

Current trends in representation learning highlight the importance of employing high-dimensional vector embeddings to represent behavioral patterns in a compact numerical representation. [6], [14] Behavioral embeddings facilitate similarity-based comparisons across sessions, which helps to track persistent attackers even when using different surface-level identifiers such as IP addresses or credentials.

Studies on vector-based identity analysis have shown that embedding similarity search facilitates clustering, correlation, and long-term profiling of malicious behavior. [6] This is a paradigm shift from signature-based detection to behavioral fingerprinting, which facilitates intelligence-driven threat anal-ysis. BioTrap implements this paradigm by maintaining behavioral embeddings in a vector database for attacker correlation and session replay.

D. Research Gaps and Motivation for BioTrap

Although there has been considerable progress in the areas of behavioral biometrics, deception systems, and machine learning-based detection, the current state-of-the-art solutions have some obvious shortcomings. Most of the existing solutions target authentication, anomaly detection, or deception individually, rather than providing a comprehensive framework that encompasses all three. Moreover, most of the existing solutions are based on static rules or short-term session monitoring, and they do not have any provision for long-term correlation of attackers. Furthermore, the traditional defense mechanisms are primarily designed to prevent intrusion attacks rather than exploiting them for intelligence purposes.

BioTrap fills these research gaps by providing a comprehen-sive framework that integrates deception engineering, behav-ioral biometrics, and deep learning-based analysis. By steer-ing malicious users into a controlled honeytrap environment and creating persistent behavioral embeddings, BioTrap con-verts intrusion attempts into intelligence. This comprehensive framework that integrates adaptive authentication, behavioral profiling, and deception-driven engagement makes BioTrap different from the existing solutions and thus motivates the proposed design.

III. PROPOSED SYSTEM

The proposed system is an intelligent cybersecurity system named BioTrap that utilizes behavioral biometrics, deception technology, and machine learning-based anomaly detection to detect malicious login activities. Unlike other cybersecurity systems that depend on passwords and multi-factor verification, the proposed system will evaluate the behavior of the user when using the system.

The proposed system has the following layers: the authentication layer, the risk evaluation engine, the deception layer, the behavioral capture module, and the intelligence storage layer. Once the user initiates the login process, the proposed system will first evaluate the contextual information such as the metadata of the device, the patterns of the IP address, and the patterns of the login time.

If the behavior is normal and not malicious, the user can proceed with the normal authentication process and gain access to the actual application dashboard. However, if the behavior is malicious, the user will be redirected to the honeytrap environment without knowing that the environment is not the real system. The honeytrap environment is almost identical to the real system environment, and the user can interact with the system without any problem.

Within the honeytrap environment, the system continuously captures behavioral signals such as keystroke dynamics, mouse movement patterns, page navigation sequences, and session timing metrics. These behavioral

sequences are processed using a Long Short-Term Memory (LSTM) model that analyzes temporal patterns in user interaction data. The model generates an anomaly score indicating whether the behavior deviates from legitimate user patterns.

The extracted behavioral features are converted into compact vector embeddings and stored in a vector database [6], [14]. These embeddings enable similarity analysis across sessions, allowing the system to identify repeat attackers even if they change credentials, IP addresses, or devices.

By combining deception mechanisms with behavioral ana-lytics, BioTrap transforms intrusion attempts into intelligence-gathering opportunities. Security analysts can monitor attacker behavior through an administrative dashboard that provides de-tailed logs, session replays, and anomaly scores. This approach enables proactive cybersecurity defense by identifying attacker strategies and improving future detection capabilities.

IV. System Architecture and Methodology

The system architecture of the proposed system is based on a multi-layered approach that combines the functionalities of authentication, behavioral monitoring, deception, and machine learning-based anomaly detection. This system architecture is designed to identify suspicious login attempts and redirect the attacker to the honeytrap environment while maintaining the behavioral intelligence of the attacker. The overall system methodology is represented through the system architecture diagram.

A. Overall System Architecture

The system architecture of the proposed system is based on five layers of functionalities: Authentication Layer Risk Evaluation Layer Honeytrap/Deception Layer Behavior Capture and Analysis Layer Intelligence Storage Layer These layers work sequentially to provide the overall system functionalities.

- Authentication Layer: The authentication layer is the entry point of the system through which users provide their credentials through the web interface. This layer is respon-sible for authenticating the user credentials while providing additional information about the user through the parameters provided during the user request, such as the metadata pro-vided through the user's device, browser type, IP address, and timestamps of the user's requests.

To avoid false positives during the risk evaluation phase, users can be authenticated through adaptive multi-factor authentication techniques such as One-Time Password verification.

- Risk Evaluation Layer: The risk evaluation engine checks for contextual or behavioral signals associated with a particular login attempt. Parameters such as unusual timing for the login attempt, repeated failed attempts for a certain period, unusual typing speeds, or unusual device activity are taken into account in this process.

Based on this risk evaluation score, a decision is made on whether a particular session should be allowed access through normal authentication or redirected to the deception environment.

- Honeytrap (Deception) Layer: The honeytrap layer is a decoy environment designed to replicate the normal en-vironment of a legitimate application. A suspicious user is redirected to this environment without their knowledge or awareness. The honeytrap environment consists of dashboards, data stores, or functionalities that are decoys for a potential attacker.

The attacker is unable to access the legitimate environment while at the same time being tracked by this system.

- Behavior Capture and Analysis Layer: After the user has entered the honeytrap environment, the system will start capturing the behavioral interaction data. The parameters cap-tured include:

Keystroke dynamics Mouse movement trajectories Naviga-tion behavior Session timing characteristics

These behavioral interaction sequences will be treated as time series data and will be analyzed using the Long Short-Term Memory (LSTM) neural network. This LSTM will determine whether the user is legitimate or malicious based on the behavioral pattern.

- Intelligence Storage Layer: Behavioral information will be stored for later analysis. Two types of storage systems will be used:

Relational Database System: This will store session infor-mation, timestamps, and authentication information.

Vector Database System: This will store behavioral embed-dings obtained from the LSTM.

Behavioral embeddings will be used to perform similarity queries on the sessions. This will help the system to detect the attacker even if the attacker changes the credentials, IP address, or devices used.

B. System Workflow

The methodology of BioTrap, as a whole, consists of the following steps:

A user sends a login request to the system.
The authentication module requests login information, as well as context information.
The risk evaluation engine evaluates the login activity, assigning a risk score.
Normal users are directed to the real system, while suspi-cious users are sent to the honeytrap.
Behavioral interactions are detected, processed, and ana-lyzed through the LSTM model.
Behavioral information, as well as session logs, are stored for long-term attacker correlation and intelligence analysis.
As a result, BioTrap turns potential intrusion into valuable intelligence, all while protecting legitimate users.

V. Results and Analysis

The BioTrap system has been tested through various simu-lated login scenarios to determine its capability in differentiat-ing legitimate users from attackers [9], [13]. In the evaluation of the system, three main characteristics were considered: accuracy in user authentication, anomaly detection in user behavior, and the effectiveness of the honeytrap system in detecting attackers. The system has been tested using differ-ent types of user behavior, including normal and suspicious behavior.

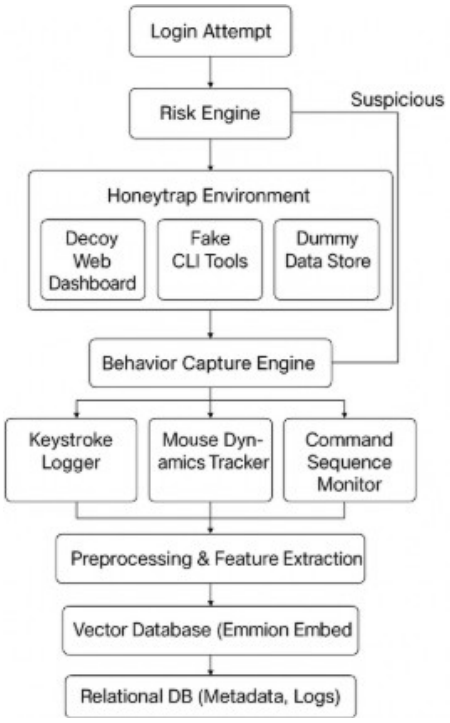

Fig. 1. System Architecture of the BioTrap Biometric Honeytrap Security System.

The framework evaluates login attempts using a risk engine and redirects suspicious sessions to a controlled honeytrap environment. Within this environment, behavioral data such as keystroke patterns, mouse dynamics, and command sequences are captured and analyzed. The extracted features are stored as behavioral embeddings in a vector database and correlated with session metadata stored in a relational database for long-term attacker profiling and intelligence analysis

A. Login Interface and User Interaction

The BioTrap system starts with a web-based interface for users to enter their login credentials. In addition to entering their credentials in the system, users are also monitored in terms of their behavioral interactions, such as the time it took for users to enter their credentials, the speed of their typing, mouse movements, and navigation behaviors. These interactions are monitored in real time using the behavior capture module in the frontend interface of the system.
In the evaluation of the system, legitimate users were able to interact with the system without any problem or delay in the login interface of the system. The system has been able to record the behavioral interactions of users in the system and store it in the behavioral database.

B. Behavioral Profile Generation

During user registration and initial login sessions, the system generates a behavioral baseline for each legitimate user. This is the normal behavioral pattern of the user, including the average typing speed, mouse movement trajectory, and navigation time.

The collected behavioral sequence is converted into a feature vector and fed into the LSTM-based behavioral analysis model for processing. The system generates embeddings representing the behavioral signature of the user and stores it in the vector database.

The experimental results show that the system can successfully generate stable behavioral fingerprints for legitimate users in multiple sessions.

C. Legitimate User Authentication

In order to validate the accuracy of the authentication system, several legitimate user login sessions are performed under normal circumstances. In these cases, the system assigns low anomaly scores and allows users to access the real application dashboard after successful user credential and optional one-time password authentication.

The authentication process is smooth and does not disrupt the user experience, indicating the ability of the BioTrap framework to provide a seamless user experience with security monitoring in place.

D. Suspicious Behavior Detection

To simulate suspicious login scenarios, abnormal patterns of interaction, such as extremely fast typing speed, unusual mouse movements, repetitive login attempts, and unknown device information, were introduced into the system.

As abnormal patterns are detected, the LSTM model increases the risk score accordingly. The risk evaluation engine then classifies the session as suspicious, triggering the deception mechanism.

As indicated in the experimental results, the system ef-fectively detects abnormalities in normal behavioral patterns, accurately classifying suspicious sessions [13].

E. Honeytrap Redirection and Monitoring

As the session is classified as a high-risk session, the system redirects the user to a honeytrap environment, mimicking the original application interface, without the attacker's knowledge. The attacker continues interacting with the decoy system, unaware of the redirection.

As the attacker navigates the system, all activities are monitored, including navigation patterns, command input, and interaction patterns. This provides the system with valuable intelligence regarding the attacker's activities.

As indicated in the results, the system effectively captures detailed behavioral information, utilizing the honeytrap mechanism without exposing the system resources.

F. Administrative Dashboard and Threat Analysis

The administrative dashboard of BioTrap allows security analysts to gain insight into all activity in the system. The dashboard contains various pieces of information, which may include recent login attempts, anomaly scores, suspicious session alerts, and behavioral analytics.

The security analysts are also able to access captured interaction data, monitor attacker sessions, and carry out correlation analysis of stored behavioral embeddings. This feature also facilitates long-term tracking of attackers, thereby providing proactive defense in cybersecurity.

As expected, the experimental evaluation of BioTrap confirms that it is capable of differentiating between legitimate users and attackers at the same time, transforming attacks into opportunities for behavioral intelligence gathering.

VI. CONCLUSION AND FUTURE WORK

A. Conclusions

In this paper, a Biometric Honeytrap Security System, called BioTrap, was introduced as a potential solution to improve cybersecurity defenses through the incorporation of behavioral biometrics, deception technology, and machine learning-based anomaly detection systems.

Unlike other conventional security systems, which only rely on password-based or fixed identity-based information, BioTrap provides a novel security mech-anism based on user behaviors, which are used to identify suspicious activities based on user interactions.

In this paper, a novel cybersecurity system was introduced, which evaluates login requests based on various context infor-mation and behavioral information, such as keystroke patterns, mouse movement patterns, and session timing patterns, which are then analyzed as a sequence of behaviors using a Long Short-Term Memory model to identify anomalous behaviors between legitimate users and attackers, where suspicious users are directed to a controlled environment called a ”honeytrap.” The honeytrap environment facilitates the observation of the attackers' behavior in a safe and sandboxed environment, and the interaction logs can be recorded and analyzed. These interaction logs can be mapped to behavioral embeddings and stored in a vector database, which facilitates the correlation and behavioral fingerprinting of attackers over multiple ses-sions.

The experiment has proved that the BioTrap system is able to detect abnormal behavior while providing users with a seamless and uninterrupted experience. The incorporation of deception mechanisms with behavioral analytics not only improves the security posture of the system, it also utilizes the intrusion attempts as valuable intelligence that can be used for security analysis, making BioTrap an intelligence-driven cybersecurity defense framework that is way beyond the conventional security paradigm [15], [16].

B. Future Work

Although the BioTrap system has exhibited promising re-sults in detecting suspicious behaviors and tracking attacker activities, there are still several avenues for improving the system.

Future work can be focused on improving the behavioral analysis model by using other machine learning techniques like the Transformer architecture and ensemble anomaly de-tection methods. Improving the behavioral features by adding touchscreen gestures, motion patterns of the devices, and advanced user interaction features can be used to improve the system's ability to differentiate normal users from attacker users.

Another area that can be explored is the integration of the system with large-scale threat intelligence systems. This can be achieved by integrating the system with Security Information and Event Management (SIEM) systems to enable the cor-relation of attacker behaviors across multiple environments. The scalability of the system can be further enhanced through more in-depth cloud integration using distributed architectures and containerization-based deployment strategies. Integrating large-scale vector databases and real-time stream processing pipelines would allow the BioTrap system to efficiently func-tion in an enterprise-scale environment where there are high volumes of ongoing authentication requests.

Furthermore, future work can be done in the area of advanced visualization and behavioral clustering methods that would allow security analysts to gain insights into the strate-gies and tactics employed by attackers.

With the continued development and integration of ad-vanced analytics, the BioTrap system has the potential to be transformed into a fully-fledged cybersecurity intelligence system that would be capable of proactively identifying, ana-lyzing, and responding to complex cyber threats.

REFERENCES

[1] O. L. Finnegan, J. W. White III, and B. Armstrong, “The utility of behavioral biometrics in user authentication,” Systematic Reviews, vol. 13, no. 1, 2024.

[2] M. Sultana, P. P. Paul, and M. Gavrilova, “Social behavioral biometrics,” in Proc. Int. Conf. Cyberworlds, 2014, pp. 271–278.

[3] S. Hochreiter and J. Schmidhuber, “Long short-term memory,” Neural Computation, 1997.

[4] R. C. Staudemeyer and E. R. Morris, “Understanding LSTM,” IEEE, 2019.

[5] L. Antiga, E. Stevens, and T. Viehmann, Deep Learning with PyTorch, 2020.

[6] S. Kukreja, T. Kumar, and V. Bharate, “Vector embeddings review,” IEEE, 2023.

[7] A. Paszke et al., “PyTorch library,” in NeurIPS, 2019.

[8] A. Sherstinsky, “RNN and LSTM fundamentals,” Neural Networks, 2019.

[9] P. Braca et al., “Machine learning performance,” IEEE, 2023.

[10] N. Provos and T. Holz, Virtual Honeypots, Addison-Wesley, 2022.

[11] K. Salah et al., “Advanced honeypots,” IEEE Access, 2022.

[12] A. A. E. Ahmed and I. Traore, “Mouse dynamics biometrics,” IEEE, 2023.

[13] Y. Meng et al., “Intrusion detection using deep learning,” IEEE Access, 2023.

[14] J. Shlens, “Deep learning embeddings tutorial,” arXiv, 2022.

[15] M. Conti et al., “Behavioral biometrics survey,” ACM Computing Sur-veys, 2024.

[16] S. Bhattacharya et al., “Zero trust security,” IEEE Security & Privacy, 2023.

[17] D. Dasgupta, Z. Akhtar, and S. Sen, “Machine learning in cybersecurity,” IEEE Access, vol. 10, pp. 47305–47325, 2022.

[18] R. Mitchell and I. R. Chen, “Behavior-rule based intrusion detection systems,” IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 6, pp. 688–699, 2021.

[19] S. Axelsson, “The base-rate fallacy and intrusion detection,” ACM Transactions on Information and System Security, vol. 3, no. 3, pp. 186–205, 2020.
[20] E. Alpaydin, Introduction to Machine Learning, 4th ed. Cambridge, MA, USA: MIT Press, 2021.
[21] C. Tankard, “Advanced persistent threats and how to monitor and deter them,” Network Security, vol. 2019, no. 8, pp. 16–19, 2019.
[22] M. Bishop, “Computer security: Art and science,” Addison-Wesley, 2021.
[23] W. Stallings and L. Brown, Computer Security: Principles and Practice, 5th ed. Pearson, 2023.
[24] B. Schneier, “Attack trees and intrusion analysis,” Dr. Dobb’s Journal, vol. 24, no. 12, pp. 21–29, 2020.