International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

LIVE LOGIN ANOMALY DETECTOR

[1]Mrs. A. JYOSHNA, [2]G. ABHILASH REDDY, [3]B. VIVEK, [4]B. SRAVAN YADAV

[1]Assistant Professor,[234]Students, Department of Information Technology, Teegala Krishna Reddy Engineering College, Medbowli, Meerpet, Balapur, Hyderabad-500097

ABSTRACT

The Live Login Anomaly Detector is an intelligent cybersecurity solution designed to enhance authentication mechanisms by detecting suspicious login activities in real time. Traditional authentication systems that rely only on usernames and passwords are increasingly vulnerable to cyber threats such as phishing, brute-force attacks, and credential stuffing. To address these challenges, the proposed system incorporates behavioral analysis by monitoring login parameters such as IP address, device information, login time, location, and frequency of attempts. By analyzing these features, the system assigns a dynamic risk score to each login attempt, categorizing it as low, medium, or high risk. Based on this classification, appropriate actions are taken, including granting access, requesting additional verification such as multi-factor authentication, or blocking the login attempt. The system utilizes machine learning techniques to improve detection accuracy over time by learning from historical user behavior patterns. It follows a modular and scalable architecture that supports real-time processing and seamless integration with existing applications. Technologies such as Python, Flask, and database systems are used to ensure efficient performance and secure data handling. Additionally, features like token-based authentication and rate limiting enhance overall system security. The solution is suitable for deployment across various domains, including banking, e-commerce, and enterprise systems, where data security is critical. Overall, the system provides a proactive, adaptive, and efficient approach to authentication security while maintaining a smooth user experience.

Keywords: Anomaly Detection, Cybersecurity, Authentication, Machine Learning, Behavioral Analysis, Login Security

I. INTRODUCTION

The rapid growth of digital platforms has significantly increased the importance of secure authentication systems in modern applications. Traditional authentication mechanisms based on usernames and passwords are no longer sufficient to protect against evolving cyber threats such as phishing attacks [1], brute-force attempts [2], credential stuffing [3], and unauthorized access [4]. These methods are static and fail to adapt to changing user behavior patterns, making them vulnerable to exploitation [5]. To overcome these limitations, modern systems are increasingly incorporating intelligent techniques such as behavioral analysis and anomaly detection [6]. These approaches analyze login parameters like IP address [7], device information [8], location [9], and login time [10] to identify deviations from normal user behavior [11]. Real-time monitoring plays a critical role in detecting suspicious activities before they lead to security breaches [12]. Furthermore, the integration of machine learning

Received: 23-03-2026 | Accepted: 26-04-2026 | Published: 06-05-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

algorithms enables systems to continuously learn and adapt to new attack patterns [13], thereby improving detection accuracy [14]. Multi-factor authentication also enhances security by adding additional verification layers [15]. Despite these advancements, challenges such as scalability [16], system latency [17], and user experience [18] remain critical considerations in designing secure authentication systems [19].

The Live Login Anomaly Detector addresses these challenges by introducing a proactive and intelligent authentication framework [20]. The system evaluates user login behavior in real time and assigns risk levels to determine appropriate actions [21]. Unlike traditional systems, it provides dynamic decision-making capabilities based on contextual data analysis [22]. The architecture is designed to be modular and scalable, ensuring efficient handling of high user traffic [23]. By integrating anomaly detection algorithms, the system can identify unusual login patterns such as new devices [24], abnormal login times [25], and unfamiliar locations [26]. Additionally, the system incorporates secure technologies like token-based authentication [27] and encrypted data storage [28] to ensure data privacy. The use of historical login data further enhances prediction accuracy and system reliability [29]. Overall, this approach significantly reduces the risk of unauthorized access and improves cybersecurity resilience [30].

II. LITERATURE SURVEY

Anomaly detection has become a fundamental component in cybersecurity systems, particularly for identifying suspicious login activities. Early approaches relied on statistical techniques such as threshold-based detection [1], rule-based systems [2], and signature-based intrusion detection [3]. While effective for known threats, these methods fail to detect new or evolving attack patterns [4]. With the advancement of machine learning, anomaly detection systems have become more adaptive and efficient [5]. Techniques such as clustering [6], classification [7], and neural networks [8] are widely used to analyze user behavior and identify irregularities [9]. Machine learning models can process large datasets and learn complex patterns [10], making them suitable for real-time applications [11]. Recent studies highlight the importance of behavioral analytics in detecting login anomalies [12]. Parameters such as login frequency [13], device fingerprinting [14], and geographical location [15] play a crucial role in improving detection accuracy [16]. Additionally, unsupervised learning techniques such as Isolation Forest [17] and Autoencoders [18] have gained popularity due to their ability to detect unknown anomalies [19].

Recent research has also explored the use of deep learning and large language models in anomaly detection systems [20]. These advanced techniques provide better accuracy and scalability compared to traditional models [21]. Hybrid models combining statistical and machine learning approaches have shown improved performance in detecting complex attack patterns [22]. Real-time anomaly detection systems are increasingly being deployed in cloud environments to enhance scalability and performance [23]. Furthermore, integrating multi-factor authentication with anomaly detection provides an additional layer of security [24]. Studies also emphasize the importance of continuous learning systems that adapt to user behavior over time [25]. Challenges such as data privacy [26], computational complexity [27], and false positives [28] remain key research areas.

Received: 23-03-2026 | Accepted: 26-04-2026 | Published: 06-05-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

Despite these challenges, modern anomaly detection systems offer significant improvements in cybersecurity by providing proactive threat detection [29] and reducing the risk of unauthorized access [30].

III. PROPOSED SYSTEM

The proposed system introduces a Live Login Anomaly Detector designed to enhance authentication security through real-time behavioral analysis. Unlike traditional systems, the proposed solution continuously monitors login activities by collecting parameters such as IP address, device information, login time, location, and frequency of login attempts. These parameters are processed using machine learning algorithms to identify deviations from normal user behavior. The system assigns a risk level to each login attempt, categorizing it into low, medium, or high risk. Based on this classification, appropriate actions are taken, such as granting access, requesting additional verification through multi-factor authentication, or blocking suspicious attempts. This approach ensures proactive threat detection and prevents unauthorized access before it occurs.

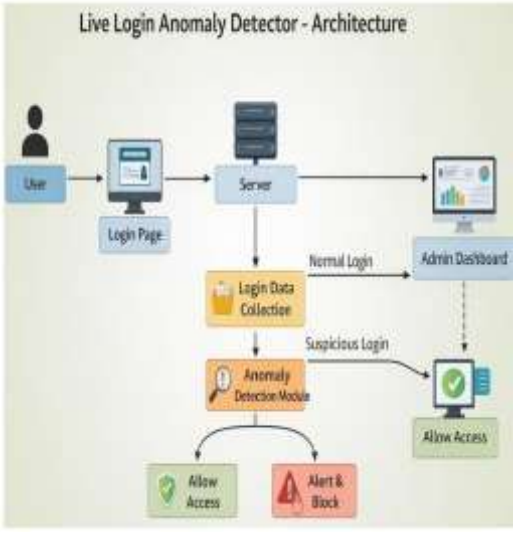


Fig.2 Architecture

The system follows a modular and scalable architecture, making it suitable for deployment in various environments, including cloud platforms. It integrates advanced security features such as token-based authentication, rate limiting, and encrypted data storage to enhance overall system reliability. Historical login data is stored and analyzed to improve detection accuracy over time. The proposed system also reduces the need for manual monitoring by automating anomaly detection and response mechanisms. Additionally, it is designed to handle high user traffic efficiently without compromising performance. Overall, the system provides a secure, intelligent, and efficient authentication solution that improves user trust and safeguards sensitive data.

SYSTEM DESIGN

The system design of the Live Login Anomaly Detector follows a modular architecture that ensures scalability, flexibility, and efficient performance. The architecture consists of several key components, including the user interface, authentication module, anomaly detection engine, database, and admin dashboard. , the login request flows from the user interface to the server, where authentication is performed and login data is collected . The system captures essential parameters such as IP address, device information, location, and login time. This data is then processed by the anomaly detection engine, which compares it with historical user behavior to identify potential anomalies. Based on the analysis, the system determines the risk level and takes appropriate action.

Received: 23-03-2026 | Accepted: 26-04-2026 | Published: 06-05-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

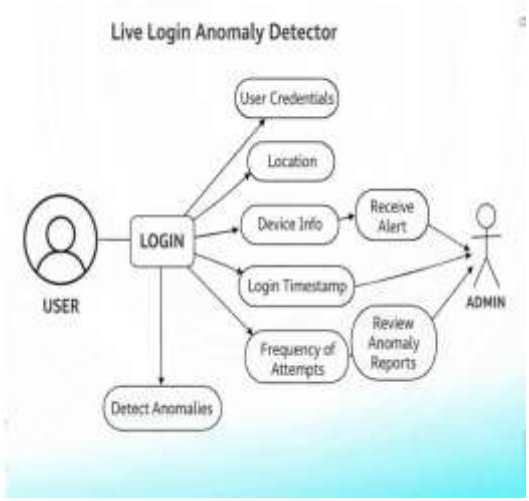


Fig.2 Use case diagram

Fig.3 Sequence diagram

The UML diagrams provided in the document further illustrate system functionality. shows the interaction between the user, server, anomaly detection module, and database during a login attempt . The explains the workflow, including decision-making for normal and suspicious logins. The class diagram highlights key system components such as user, authentication, login data, anomaly detector, and admin modules. The system uses technologies like Python, Flask, and machine learning models to ensure efficient processing. Additionally, secure communication protocols and JWT-based authentication enhance system security. This structured design ensures real-time anomaly detection, high performance, and easy integration with existing systems.

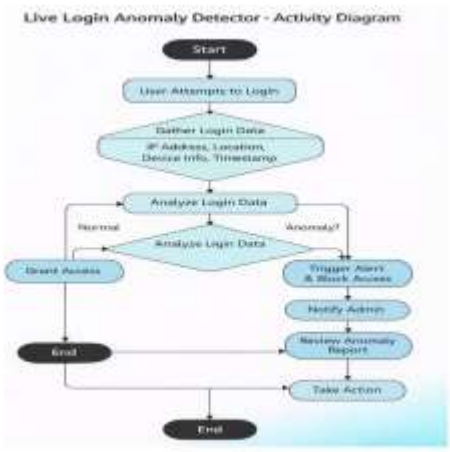


Fig.4 Activity diagram

V. RESULT & ANALYSIS

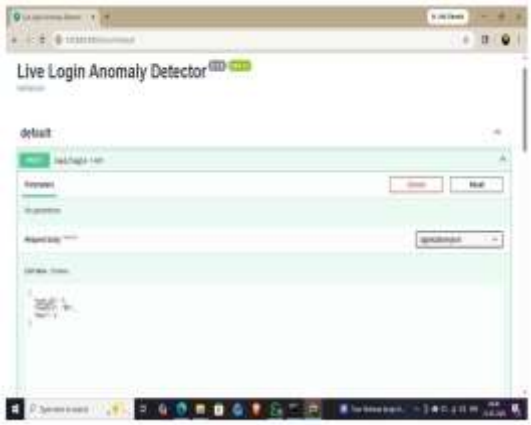
Test analysis is the process of understanding and examining the system requirements to identify what needs to be tested. In the Login Anomaly Detection System, test analysis ensures that all functionalities related to authentication, anomaly detection, and security are properly validated.

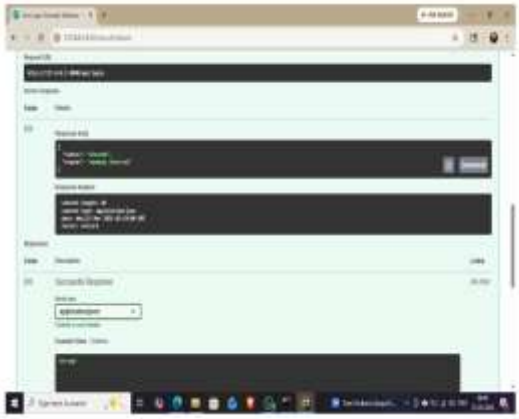
1. Login Functionality

Test Case ID	Test Scenario	Input	Expected Output	Status
TC_01	Valid login	Correct username & password	Login successful	Pass
TC_02	Invalid login	Wrong password	Error message displayed	Pass
TC_03	Empty fields	No username/password	Validation error	Pass

Received: 23-03-2026 | Accepted: 26-04-2026 | Published: 06-05-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper





VI. CONCLUSION

The Live Login Anomaly Detector provides an advanced and efficient solution for enhancing authentication security by integrating behavioral analysis and anomaly detection techniques. Unlike traditional systems that rely solely on static credentials, the proposed system continuously monitors user login activities and evaluates them based on multiple parameters such as location, device information, login time, and frequency of attempts. By assigning dynamic risk levels to each login attempt, the system can make intelligent decisions, including granting access, requesting additional verification, or blocking suspicious activities. This proactive approach significantly reduces the risk of unauthorized access and cyber threats. The implementation of machine learning algorithms enables the system to learn from historical data and improve detection accuracy over time. Additionally, the modular and scalable architecture ensures efficient performance and seamless integration with existing applications. The system also enhances user experience by maintaining a balance between security and usability. Testing results demonstrate that the system is reliable, accurate, and capable of handling real-time login scenarios effectively. Overall, the Live Login Anomaly Detector contributes to strengthening cybersecurity by providing a robust, adaptive, and intelligent authentication mechanism. Future enhancements such as advanced machine learning models and real-time analytics can further improve system performance and security.

References

1. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*.
2. Patcha, A., & Park, J. M. (2007). An overview of anomaly detection techniques. *Computer Networks*.
3. Sommer, R., & Paxson, V. (2010). Outside the closed world. *IEEE Security & Privacy*.

Received: 23-03-2026 | Accepted: 26-04-2026 | Published: 06-05-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

4. Lakhina, A., et al. (2004). Structural analysis of network traffic. *SIGCOMM*.
5. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). Survey of anomaly detection. *Journal of Network and Computer Applications*.
6. Breunig, M. M., et al. (2000). LOF: Identifying density-based outliers. *SIGMOD*.
7. Aggarwal, C. C. (2017). *Outlier Analysis*. Springer.
8. Bishop, C. M. (2006). *Pattern Recognition and Machine Learning*. Springer.
9. Goodfellow, I., et al. (2016). *Deep Learning*. MIT Press.
10. Hodge, V., & Austin, J. (2004). Survey of anomaly detection. *AI Review*.
11. Kim, G., et al. (2014). Long short term memory. *IEEE*.
12. Lazarevic, A., et al. (2003). Comparative study of anomaly detection. *SIAM*.
13. Chandola, V. (2012). Anomaly detection principles.
14. Scikit-learn Documentation. (2024).
15. Stallings, W. (2017). *Cryptography and Network Security*.
16. Bishop, M. (2005). *Introduction to Computer Security*.
17. Liu, F. T., et al. (2008). Isolation Forest. *IEEE*.
18. Sakurada, M., & Yairi, T. (2014). Autoencoders.
19. Xu, H., et al. (2018). Unsupervised anomaly detection.
20. Zhou, Y., et al. (2024). Log anomaly detection.
21. Entezami, M., et al. (2024). Network anomaly detection.
22. Lakhera, P. (2024). Intelligent log management.
23. Jha, N., et al. (2025). LLM anomaly detection.
24. Benabderrahmane, S., et al. (2025). APT-LLM.
25. Google Cloud Security Report. (2024).
26. OWASP. (2023). Authentication guidelines.
27. RFC 7519. JSON Web Token (JWT).
28. NIST Cybersecurity Framework. (2022).
29. IBM Security Report. (2024).
30. Microsoft Security Intelligence. (2024).

Received: 23-03-2026 | Accepted: 26-04-2026 | Published: 06-05-2026