InSight Bulletin: A Multidisciplinary Interlink International Research Journal
Peer Reviewed International, Open Access Journal.
ISSN : 3065-7857 / Website: https://ibrj.us / Volume-3, Issue-1 / January - 2026

Original Article

Secure AI-Driven Behaviour-Based Access Control (BBAC) for Real-Time Data Breach Prevention

Pranav Mali[1], Ishita Baghel[2]
[1,2]Department of Computer Science, Ashoka Center for Business and Computer Studies, Nashik, Maharashtra, India

Manuscript ID:
IBMIIRJ -2026-030120

Submitted: 07 Dec. 2025

Revised: 11 Dec. 2025

Accepted: 06 Jan. 2026

Published: 31 Jan. 2026

ISSN: 3065-7857

Volume-3

Issue-1

Pp. 109-111

January 2026

Correspondence Address:
Pranav Mali, Department of Computer Science, Ashoka Center for Business and Computer Studies, Nashik, Maharashtra, India
Email: malipranav4747@gmail.com

OPEN ACCESS

Quick Response Code:

Web. https://ibrj.us

DOI: 10.5281/zenodo.18950491

DOI Link:
https://doi.org/10.5281/zenodo.18950491

Creative Commons

Abstract

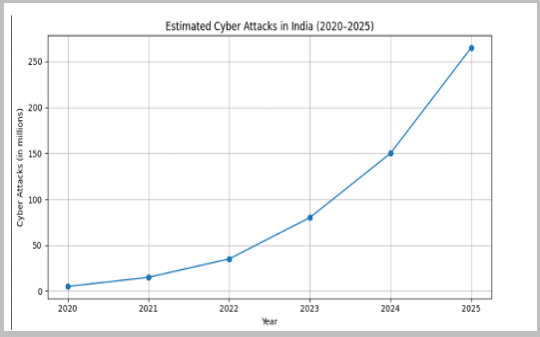
As cloud computing and digital services continue to expand, cybersecurity threats are becoming more advanced and destructive. Traditional security methods based on fixed credentials, predefined rules, and slow response times often fail to detect attackswhere hackers use valid user credentials. To address this issue, this paper presents an AI-powered Behaviour-Based Access Control (BBAC) system that continuously tracks user activity and identifies unusual behaviour in real time. By learning each user's normal activity patterns, the system can automatically end suspicious sessions and reset compromised credentials before major damage occurs.This approach provides a proactive and self-healing security layer, making it highly effective for modern software platforms, cloud services, and enterprise environments.

Keywords: *Artificial Intelligence, Behaviour-Based Access Control, Anomaly Detection, Data Breach Prevention, Cybersecurity, Zero Trust, Self-Healing System.*

Introduction

In recent years, cyberattacks have become far more advanced, evolving from simple external breaches to more complex threats involving stolen credentials and insider misuse. Despite organizations investing heavily in security tools like firewalls, multi-factor authentication, and intrusion detection systems, large-scale data breaches continue to occur. These incidents reveal an important flaw in traditional security approaches, [1] once an attacker gains access to valid credentials often through phishing, social engineering, or insider threats it becomes extremely difficult for existing systems to tell the difference between a legitimate user and an intruder. This allows malicious activities to go unnoticed for long periods.To tackle this challenge, our research introduces an AI-driven Behaviour-Based Access Control (BBAC) system. [2] Unlike traditional methods that focus only on verifying identity during login, BBAC keeps an eye on user activity throughout thesession. It learns how each user normally interacts with systems and identifies unusual patterns that might indicate a security threat. [3] When suspicious behaviour is detected, the system can automatically take action such as limiting access or asking for additional verification. By moving from one-time authentication to continuous behavioural monitoring, BBAC provides a stronger, more adaptive layer of protection against modern cyberattacks.

Diagram-1



Cyberattack in India (approximate, 2020–2025)
Data collected from- TOI, NCRB, CERT-In, Check Point Research, etc.

How to cite this article:
Mali, P., & Baghel, I. (2026). Secure AI-Driven Behaviour-Based Access Control (BBAC) for Real-Time Data Breach Prevention. InSight Bulletin: A Multidisciplinary Interlink International Research Journal, 3(1), 109–111. https://doi.org/10.5281/zenodo.18950491

1. **Proposed BBAC System Overview**

The proposed Behaviour-Based Access Control (BBAC) system acts as an intelligent, adaptive security layer that can easily integrate into existing software platforms or function as a standalone middleware. Unlike traditional systems that rely only on fixed access rules or one-time authentication, BBAC continuously monitors user activity after login. It observes how users interact with applications and data in real time and gradually learns their normal behaviour patterns. [4] This allows the system to make dynamic access decisions and quickly detect any suspicious actions, enhancing security while ensuring a seamless experience for legitimate users.

2. **Architecture Diagram Explanation**

The architecture of the Behaviour-Based Access Control (BBAC) system is made up of several interconnected modules that work together to provide real-time protection.

a. **User Interface / Client Layer**

This layer represents the end users who access applications, servers, or cloud services.

b. **Authentication & Authorization Layer**

It handles standard login methods such as passwords, multi-factor authentication (MFA), or tokens. Once the user is verified, control is handed over to the BBAC module.

c. **Behaviour Monitoring Module**

This component continuously tracks user activity parameters like login time, session length, device information, access frequency, and data volume.

d. **AI Behaviour Analysis Engine**

Powered by machine learning, this engine compares real-time user behaviour with established baselines to detect any unusual or suspicious activity.

e. **Decision & Response Module**

Based on the AI engine's analysis, this module decides whether to allow, restrict, or terminate a user's access session.

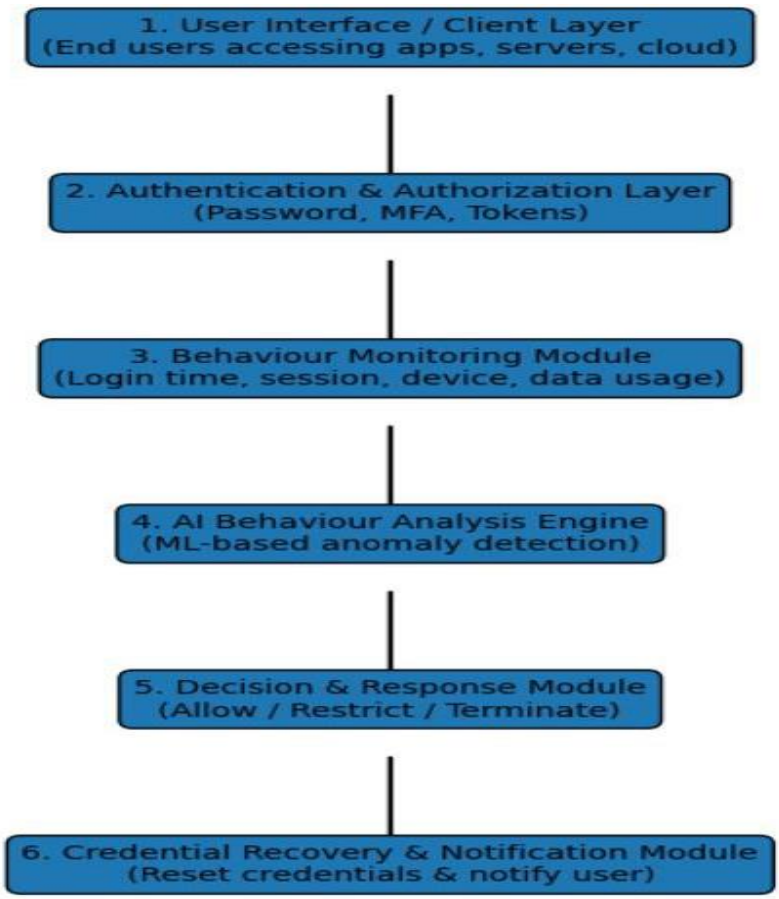
f. **Credential Recovery & Notification Module**

If any compromise is detected, this module automatically resets credentials and securely notifies the rightful user.

g. **Logging & Audit Module**

All system events are recorded here for compliance, auditing, and continuous learning purposes.

Diagram-2



Together, these modules create a scalable, automated, and adaptive security framework suitable for diverse software environments.

Working of the Proposed BBAC System

In the beginning, the system watches how each user normally behaves like when they log in, what actions they take, and how much data they access. Using this information, it builds a personal "behaviour profile" for every user. When the user is active, the system keeps checking their actions in real time and compares them with this normal behaviour profile. If everything looks normal, access continues smoothly. [11] But if the system notices something unusual like a sudden large download or an odd login attempt it quickly ends the session and resets the user's credentials to prevent misuse. [12] The AI keeps learning and updating these behaviour profiles over time, so it stays accurate even if a user's habits change, ensuring both strong security and flexibility.

Key Parameters Difference Table-1

Parameter	Existing Security Systems	Proposed AI-Driven BBAC System
Detection Method	Rule-based, signature-based	AI-based behavioural analysis
Response Time	Delayed (minutes to hours)	Real-time (seconds)
Handling Valid Credentials	Weak (fails if credentials are valid)	Strong (detects abnormal behaviour even with valid credentials)
Automation & Recovery	Manual intervention required	Fully automated self-healing
Adaptability	Static, requires manual updates	Adaptive and continuously learning

Discussion

[13] Recent analyses of major data breaches reveal that attackers often use valid login credentials and can stay hidden within systems for a long time. [14] Most existing security setups only alert administrators after the damage such as data theft hasalready occurred. The proposed Behaviour-Based Access Control (BBAC) system overcomes this limitation by continuously monitoring and validating user behaviour, allowing it to detect and respond to suspicious activity in real time without waiting for human intervention. [15] Although challenges like false alerts and user privacy concerns may arise, these issues can be managed by fine-tuning detection thresholds and applying privacy-focused data handling methods. This ensures a balance between strong security and user trust

Conclusion

This paper introduced an AI-powered Behaviour-Based Access Control (BBAC) system designed to reduce the risk of large-scale data breaches in modern software environments. By continuously monitoring user behaviour and responding automatically when something unusual happens, the system helps detect threats faster and limit potential damage. Unlike traditional security methods, BBAC takes a proactive and adaptive approach that aligns with zero-trust security principles. It can even recover credentials automatically when a threat is detected, making it a smart, self-healing solution. Future improvements will aim to make the system even more accurate, reduce false alerts, and ensure that user privacy is always protected.

Acknowledgment

The authors express their sincere gratitude to the Department of Computer Science, Ashoka Center for Business and Computer Studies, Nashik, for providing the necessary support and resources to complete this research. They also thank their mentors and peers for their valuable guidance and encouragement throughout the study.

Financial support and sponsorship

Nil.

Conflicts of interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Refrences

1. Mitnick, Kevin D., and William L. Simon. The art of intrusion: the real stories behind the exploits of hackers, intruders and deceivers. John Wiley & Sons, 2009.
2. Kumarasinghe, Jayampathini. "Improving the B App to Improve CustomerExperience and Operational Efficiency: From the Perspectives of User Engagement, Functionality, and Security." (2024).
3. Jiang, Meng, Peng Cui, and Christos Faloutsos. "Suspicious behavior detection: Current trends and future directions." IEEE intelligent systems 31.1 (2016): 31-39.
4. Ghadge, Nikhil. "Enhancing threat detection in Identity and Access Management (IAM) systems." International Journal of Science and Research Archive 11.2 (2024): 2050-2057.
5. Kaiser, Tamanna, Rafa Siddiqua, and Md Main Uddin Hasan. A multi-layer security system for data access control, authentication, and authorization. Diss. Brac University, 2022.
6. Atterer, Richard, Monika Wnuk, and Albrecht Schmidt. "Knowing the user's every move: user activity tracking for website usability evaluation and implicit interaction." Proceedings of the 15th international conference on World Wide Web. 2006.