Journal Homepage: www. ijarpr.com ISSN: 3049-0103 (Online)

International Journal of Advance Research Publication and Reviews

Vol 02, Issue 10, pp 106-115, October 2025

Behaviour Biometrics Enhanced Security Layer of Windows Authentication and Remote Access Sessions

Miss Hetvi Gosai.[1], Ami M. Mehta[2]

[1] *PG Scholar, Computer Science Engineering/ Information Technology Department, Dr. Subhash University, Junagadh, India*

[2] ***Assistant Prof Professor,*** *Computer Science Engineering/ Information Technology Department, Dr. Subhash University, Junagadh, India*

ABSTRACT

Endpoint security has become a critical concern in safeguarding enterprise infrastructures against advanced and persistent cyber threats. Traditional antivirus solutions are no longer sufficient to defend against ransomware, fileless malware, and living-off-the-land (LotL) attacks [7], [10], [18]. Endpoint Detection and Response (EDR) systems have emerged as a vital Défense mechanism, providing real-time monitoring, behavioural analytics, and automated response [1], [4], [12]. However, challenges such as high false-positive rates, limited artificial intelligence (AI) adaptability, and inadequate detection of stealthy attacks persist [9], [17], [25]. To address these limitations, this study explores the integration of behavioural biometrics-driven continuous authentication with EDR frameworks, enhancing security in remote work environments [3], [11], [20]. By capturing user-specific behavioural traits such as keystroke dynamics and mouse movements, and combining them with AI and Zero Trust architectures, the proposed approach strengthens anomaly detection, minimizes false alerts, and ensures adaptive Défense [14], [22], [30].

Keywords: Endpoint Detection and Response (EDR), Extended Detection and Response (XDR) ,Behavioural Biometrics, Continuous Authentication, Keystroke Dynamics, Mouse Dynamics, Zero Trust Architecture, Artificial Intelligence (AI) in Cybersecurity, Machine Learning (ML) for Threat Detection, Fileless Malware, normally Detection, Remote Work Security, Enterprise Cybersecurity

1.Introduction

The rapid digitization of business processes, coupled with the expansion of remote and hybrid work environments, has significantly increased the attack surface for enterprises [11], [20], [27]. Cybercriminals now employ sophisticated techniques such as advanced persistent threats (APTs), fileless malware, and LotL attacks that can easily bypass traditional security solutions [10], [18], [26].

According to recent industry reports, global cybercrime damages are expected to exceed $10 trillion annually by 2025, emphasizing the urgent need for more robust endpoint security mechanisms [14], [30].Endpoint Detection and Response (EDR) has evolved as a next-generation Défense system, moving beyond signature-based antivirus by incorporating behavioural analytics, machine learning, and automated remediation [1], [4], [12].

EDR tools continuously monitor endpoint activities, enabling real-time detection of anomalies and rapid response to active threats [8], [15], [21]. Unlike traditional defences, EDR can identify fileless and insider attacks through advanced telemetry analysis [6], [16], [22]. However, despite their efficiency, EDR systems still face critical challenges such as

false positives, scalability issues, and limited integration with adaptive frameworks like Zero Trust and Extended Detection and Response (XDR) [8], [20], [28].

One promising enhancement to EDR is the integration of behavioural biometrics, a technology that leverages unique human behavioural patterns (e.g., keystroke dynamics, mouse movement, and touchscreen interactions) for continuous authentication [2], [7], [19]. Unlike static credentials or physical biometrics, behavioural biometrics operate passively and unobtrusively, enabling persistent monitoring without compromising user experience [5], [13], [22].

In remote work scenarios, this approach can provide an additional trust layer to endpoint Défense by continuously verifying user legitimacy while reducing reliance on single-point authentication [3], [11], [20].The convergence of EDR with behavioural biometrics, supported by AI-driven models and Zero Trust architectures, offers a proactive Défense mechanism capable of addressing stealthy attack vectors and minimizing false alerts [9], [17], [25].

This study investigates the potential of such an integrated approach for enterprise endpoint protection, aiming to enhance anomaly detection, improve resilience against advanced threats, and ensure compliance with modern data privacy standards [16], [24], [31].

2. Literature Review

Table 1 – *Literature Review*

No	Publisher/Year	Title of Paper	Research Objective	Methods	Limitations
1	IEEE Trans. on Info Forensics and Security, 2024	Continuous authentication using keystroke and mouse dynamics fusion in enterprise systems	Improve continuous authentication using keystroke and mouse fusion	Experimental evaluation on enterprise datasets	Limited to enterprise scenarios
2	J. Info Security and Applications, 2023	Zero Trust integration with endpoint detection and response for hybrid work environments	Explore Zero Trust integration with EDR in hybrid environments	Case studies and simulations	Focused on hybrid work only
3	ACM Trans. on Privacy and Security, 2024	Adversarial machine learning attacks and defenses in endpoint security models	Analyze adversarial attacks and defenses in EDR models	Theoretical analysis and experiments	Limited model types studied
4	Future Generation Computer Systems, 2024	Behavioral biometrics for frictionless multi-factor authentication in cloud workplaces	Implement behavioral biometrics for MFA in cloud	Simulation and prototype implementation	Cloud-specific, not generalizable
5	Expert Systems with Applications, 2023	Explainable AI for endpoint detection: Improving trust in automated threat response systems	Enhance trust via explainable AI in endpoint detection	Design and testing of XAI models	Limited dataset diversity

6	Computers & Security, 2023	Privacy-preserving behavioral biometrics for compliance with GDPR in enterprise networks	Enable privacy-preserving behavioral biometrics for GDPR compliance	Algorithm design and testing	Focus on GDPR regions only
7	J. Computer Virology and Hacking Techniques, 2024	Dataset challenges for benchmarking EDR and behavioral analytics tools	Identify challenges in EDR benchmarking datasets	Dataset analysis and review	Limited datasets reviewed
8	J. Network and Computer Applications, 2025	Cross-platform endpoint protection using behavioral biometrics in Windows and Linux systems	Evaluate cross-platform behavioral biometrics protection	Experimental evaluation on Windows/Linux	Limited OS coverage
9	J. Cybersecurity Research and Practice, 2024	A comparative study of XDR and EDR solutions in mitigating advanced persistent threats	Compare XDR vs EDR for APT mitigation	Comparative analysis	Focus on selected vendors only
10	Pattern Recognition Letters, 2023	Mouse dynamics for anomaly detection in online examination and enterprise authentication	Use mouse dynamics for anomaly detection	Experimental studies in exam/enterprise setup	Dataset size limited
11	IEEE Access, 2024	AI-enhanced threat hunting in Zero Trust endpoint environments	Enhance threat hunting with AI in Zero Trust	AI algorithm implementation	Limited real-world deployment tested
12	Int. J. Info Management Data Insights, 2024	Scalable behavioral biometric authentication for large enterprise deployments	Enable scalable behavioral authentication	Prototype deployment on enterprise scale	May not generalize to small organizations
13	Knowledge-Based Systems, 2025	Federated learning for endpoint anomaly detection with privacy preservation	Apply federated learning for anomaly detection while preserving privacy	Federated learning experiments	Communicati on overhead issues
14	Human-Centric Computing and Info Sciences, 2024	Balancing usability and security in continuous behavioral authentication systems	Optimize usability-security tradeoff	User study and simulations	Limited sample size

15	ACM Computing Surveys, 2024	A survey on the integration of Zero Trust architecture with AI-driven endpoint detection	Survey integration of Zero Trust with AI for endpoint security	Literature review	Survey may miss latest unpublished studies
16	J. Cybersecurity and Privacy, 2024	Behavioral biometrics for continuous authentication in remote work environments	Implement behavioral biometrics in remote work authentication	Simulation and evaluation	Limited to remote work setup
17	Computers & Security, 2023	Keystroke dynamics and mouse movement analysis for anomaly detection in endpoint security	Use keystroke and mouse analysis for anomaly detection	Experimental evaluation	Dataset size may be limited
18	Int. J. Info Security, 2024	AI-driven behavioral profiling for proactive threat detection in remote access systems	Develop AI behavioral profiling for proactive threat detection	Algorithm design and testing	Limited network environments tested
19	J. Network and Computer Applications, 2024	Integrating behavioral biometrics with adaptive security policies for resilient cybersecurity	Combine behavioral biometrics with adaptive policies	Policy simulation and analysis	Focus on specific policy scenarios
20	Big Data and Cognitive Computing, 2023	Advanced behavioral analytics for user authentication and anomaly detection in enterprise networks	Apply behavioral analytics for authentication and anomaly detection	Analytics framework testing	Limited network types
21	Int. J. Info Technologies & Security, 2025	Detection of behavioural baseline deviation in endpoint usage through mouse dynamics analysis	Detect deviations in endpoint behavior using mouse dynamics	Mouse dynamics experiments	Limited to desktop usage
22	IET Biometrics, 2022	Intrusion detection using mouse dynamics	Detect intrusions via mouse behavior patterns	Experimental evaluation	Small user sample

23	J. Medical Systems, 2022	User authentication method based on keystroke dynamics and mouse dynamics in hybrid scenes	Combine keystroke and mouse for hybrid authentication	Simulation experiments	Limited hybrid environment coverage
24	ACM Computing Surveys, 2024	Mouse dynamics behavioural biometrics: A survey	Survey mouse dynamics for behavioral biometrics	Literature survey	Survey may not include unpublished methods
25	Expert Systems with Applications, 2025	Cognitive behavioural characteristics identification for cybersecurity	Identify cognitive-behavioral traits for security	Experimental and cognitive analysis	Focus on selected cognitive models
26	J. Cybersecurity, 2025	AI-based cybersecurity frameworks for 7G-enabled virtual therapy platforms	Develop AI frameworks for 7G virtual therapy security	Framework design and simulation	Limited to 7G virtual therapy context
27	Expert Systems with Applications, 2021	An approach to detect user behavior anomalies within touchscreen-based systems	Detect anomalies in touchscreen-based systems	Experimental evaluation	Focused on touchscreen devices only
28	CrowdStrike Blog, 2023	AI-powered behavioral analysis in cybersecurity	Overview of AI behavioral analysis	Case studies and examples	Non-peer-reviewed blog content
29	Int. J. Strategic Marketing Practice, 2024	Consumer Behavior Analysis in the Age of Big Data for Effective Marketing Strategies	Analyze consumer behavior using big data	Data analytics and case studies	Marketing-focused, not cybersecurity
30	Fortinet Cybersecurity Glossary, 2024	Artificial Intelligence (AI) in Cybersecurity	Define AI applications in cybersecurity	Conceptual overview	High-level overview, not empirical

No Publisher/Year Title of Paper Research objective Methods Limitations

2.1 Research Gap:

1. AI/ML Integration Limitations

Existing EDR solutions rely heavily on static detection and limited machine learning models, which are often ineffective against zero-day and polymorphic attacks [7], [15], [23]. Research lacks adaptive frameworks that continuously evolve with threat landscapes [11], [20], [27].

2. Insufficient Detection of Fileless& LotL

Fileless malware and LotL techniques bypass traditional defenses by exploiting legitimate system processes. Few frameworks provide robust, real-time detection mechanisms for these stealthy attack vectors [10], [18], [26].

3. High False Positive Rates

Many EDR systems generate excessive false alerts, leading to alert fatigue and reduced efficiency of security operation centers [9], [17], [25]. Optimized AI-driven methods to balance accuracy and efficiency are still underexplored [19], [22], [30].

4. Lack of Standardized Datasets

Benchmarking and comparative evaluation of EDR solutions remain inconsistent due to the absence of publicly available, standardized datasets for endpoint activity and behavioral biometrics [11], [21], [30].

5. Limited Integration with Zero Trust & XDR

While Zero Trust and XDR frameworks offer holistic protection, research on their seamless integration with EDR and behavioral biometrics is minimal, leaving a gap in unified, multi-layered defense strategies [8], [20], [28].

6. Privacy & Compliance Concerns

Continuous behavioral monitoring raises data privacy and compliance challenges, particularly under GDPR and other global regulations [16], [24], [31]. More research is needed to establish privacy- preserving behavioral analytics models.

7. Scalability in Large Enterprises

Most studies on behavioral biometrics and EDR integration focus on small or controlled environments. Large-scale enterprise deployments face scalability challenges, including high data volume, latency in anomaly detection, and increased resource consumption [6], [12], [19].

8. Adaptive Adversarial Evasion

Attackers increasingly use adversarial machine learning techniques to manipulate or bypass AI/ML- driven security systems. Research into robust EDR models resilient against adversarial evasion is still limited [14], [22], [25].

9. Cross-Platform and Hybrid Environment Challenges

Remote work often involves a mix of Windows, Linux, macOS, and mobile devices. Current EDR and biometric systems show limited cross-platform consistency, reducing effectiveness in hybrid environments [5], [13], [21].

10. User Experience vs. securityTrade-off

Continuous authentication via behavioural biometrics must balance security and usability. Existing solutions often increase false re-authentication prompts or latency, which may hinder user productivity [2], [7], .

11. Insufficient Explainability of AI Models

Many AI-driven EDR and biometric systems operate as “black boxes,” making it difficult for security teams to understand, trust, and validate detection decisions. Research on explainable AI (XAI) in endpoint security is still emerging [9], [17], [30].

12. Integration with Cloud and Edge Computing

As enterprises shift workloads to the cloud and adopt edge computing, EDR and behavioural biometrics face challenges in distributed environments, including data synchronization, latency, and heterogeneous security policies [20], [27], [29].

3. Future Enhancements

Although significant progress has been made in Federated Learning (FL), Blockchain, Homomorphic Encryption (HE), and Post-Quantum Cryptography (PQC) for IoT Intrusion Detection Systems (IDS), several open challenges remain that present opportunities for future research.

Although significant progress has been made in Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), Artificial Intelligence (AI)/Machine Learning (ML), and Behavioral Biometrics, several open challenges remain that present opportunities for future research:

Adversarial-Resilient AI Models: Current AI/ML algorithms used in EDR are vulnerable to adversarial attacks, where malicious inputs are designed to evade detection. Future research should focus on building robust and explainable AI models capable of resisting adversarial manipulation and ensuring transparency in decision-making [9], [17], [25].

Multimodal Behavioral Biometrics: While keystroke dynamics and mouse movements have been widely studied, future systems should incorporate multimodal behavioral traits (e.g., touchscreen patterns, voice interaction, and cognitive response times) to improve accuracy and reduce false positives in continuous authentication [2], [8], [19].

Integration with Zero Trust and XDR: Current deployments often operate in isolation. A unified framework integrating EDR with Zero Trust architectures and XDR can enable holistic visibility across endpoints, networks, and cloud ecosystems, significantly improving proactive defense [8], [20], [28].

Privacy-Preserving Analytics: Continuous monitoring raises data privacy concerns, particularly under GDPR and global regulations. Techniques such as Federated Learning (FL), Homomorphic Encryption (HE), and Differential Privacy should be adapted for endpoint and behavioral biometric data to ensure compliance while maintaining system effectiveness [16], [24], [31].

Scalability in Enterprise and Remote Environments: As organizations increasingly adopt hybrid work models, endpoint solutions must scale across heterogeneous platforms (Windows, Linux, macOS, mobile devices). Future research should focus on designing lightweight, resource-efficient models for large-scale enterprise deployments [6], [12], [19]..

3.2 Research Objectives

1. **Comprehensive Review of EDR Evolution**

To analyze the progression of endpoint defense mechanisms from traditional antivirus to behavior-driven EDR and Extended Detection and Response (XDR), highlighting their strengths and limitations [1], [4], [12].

2. **Evaluation of EDR Against Modern Threats**

To investigate the effectiveness of EDR solutions in detecting and mitigating ransomware, fileless malware, and living-off-the-land (LotL) attacks through real-time behavioral analytics [6], [16], [22].

3. **Integration of Behavioral Biometrics**

To design and implement continuous authentication mechanisms using keystroke dynamics, mouse movement analysis, and other behavioral patterns as an additional trust layer for endpoint security [2], [7], [19].

4. **Application of AI and Machine Learning**

To explore AI/ML-driven anomaly detection models for reducing false positives and enhancing adaptability of EDR systems against stealthy and polymorphic attacks [9], [17], [25].

5. Zero Trust and XDR Synergy

To develop strategies for combining EDR with Zero Trust architectures and XDR solutions, thereby enabling multi-layered, holistic security coverage across endpoints, networks, and cloud systems [8], [20], [28].

6. Privacy-Preserving Data Collection

To ensure that behavioral data used for continuous authentication is collected, stored, and processed in compliance with data privacy regulations while maintaining detection effectiveness [16], [24], [31].

7. Enterprise Deployment Guidelines

To propose a framework for deploying behavioral biometrics-driven continuous authentication in organizational IT infrastructure, particularly in remote and hybrid work environments [11], [20], [27].

4. Conclusion

Endpoint Detection and Response (EDR) has significantly strengthened enterprise security by moving beyond signature-based antivirus to real-time monitoring, automated response, and behavioral analytics. This evolution has made it more effective in identifying advanced threats such as ransomware, fileless malware, and insider attacks.

However, EDR still faces limitations, including false positives, difficulty in detecting stealthy LotL techniques, and the absence of standardized datasets for benchmarking. These gaps reduce accuracy and hinder consistent evaluation of solutions across enterprises.

The integration of behavioral biometrics introduces a valuable enhancement. By leveraging keystroke dynamics, mouse movements, and other user-specific patterns, continuous authentication can provide an additional trust layer without disrupting user experience. When combined with AI/ML-driven analytics and Zero Trust frameworks, EDR becomes more adaptive, scalable, and resilient against evolving attacks.

In summary, the future of endpoint security lies in developing integrated, AI-enhanced, and privacy-preserving EDR systems that incorporate behavioral biometrics and extend into XDR ecosystems. This unified approach can deliver stronger anomaly detection, reduced false alerts, and continuous verification, ensuring enterprise protection in an increasingly digital and remote-first world.

5.References

1. Sharma, Ankit, Priya Singh, and Ravi Kumar. "Behavioral biometrics for continuous authentication in remote work environments." Journal of Cybersecurity and Privacy 5.3 (2024): 211-225.
2. Patel, Mehul, et al. "Keystroke dynamics and mouse movement analysis for anomaly detection in endpoint security." Computers & Security 112 (2023): 102577.
3. Kumar, Rohit, and Neeraj Arora. "AI-driven behavioral profiling for proactive threat detection in remote access systems." International Journal of Information Security 22.2 (2024): 145-162.
4. Singh, Priya, and Anil Rane. "Integrating behavioral biometrics with adaptive security policies for resilient cybersecurity." Journal of Network and Computer Applications 205 (2024): 103477.
5. Ebrahimi, Pejman, et al. "Advanced behavioral analytics for user authentication and anomaly detection in enterprise networks." Big Data and Cognitive Computing 8.1 (2023): 55.

6. Asgarov, Kamran N. "Detection of behavioural baseline deviation in endpoint usage through mouse dynamics analysis." International Journal on Information Technologies & Security 17.3 (2025): 95-104.

7. Antal, M. "Intrusion detection using mouse dynamics." IET Biometrics 8.6 (2022): 369-376.

8. Wang, X., et al. "User authentication method based on keystroke dynamics and mouse dynamics in hybrid scenes." Journal of Medical Systems 46.3 (2022): 1-10.

9. Khan, S., et al. "Mouse dynamics behavioural biometrics: A survey." ACM Computing Surveys 57.4 (2024): 1-35.

10. Orun, A. "Cognitive behavioural characteristics identification for cybersecurity." Expert Systems with Applications 189 (2025): 115-130.

11. Jayanthiladevi, A. "AI-based cybersecurity frameworks for 7G-enabled virtual therapy platforms."Journal of Cybersecurity 5.2 (2025): 75-85.

12. Martín, A. G., et al. "An approach to detect user behavior anomalies within touchscreen- based systems." Expert Systems with Applications 169 (2021): 114-125.

13. CrowdStrike. "AI-powered behavioral analysis in cybersecurity." CrowdStrike Blog, 6 Sep. 2023.

14. Williams, John. "Consumer Behavior Analysis in the Age of Big Data for Effective Marketing Strategies." International Journal of Strategic Marketing Practice 6.2 (2024): 36-46.

15. Orun, A. "Cognitive Behavioral Characteristics Identification for Cybersecurity." Expert Systems with Applications 189 (2025): 115-130.

16. Fortinet. "Artificial Intelligence (AI) in Cybersecurity." Fortinet Cybersecurity Glossary. Published 2024.

17. LexisNexis Risk Solutions. "What is Behavioral Biometrics? LexisNexis Risk Solutions. Published 2024.

18. Li, Y., Chen, X., and Zhao, H. "Continuous authentication using keystroke and mouse dynamics fusion in enterprise systems." IEEE Transactions on Information Forensics and Security 19.2 (2024): 785-798.

19. Gupta, R., and Bansal, V. "Zero Trust integration with endpoint detection and response for hybrid work environments." Journal of Information Security and Applications 75 (2023): 103542.

20. Ahmed, M., et al. "Adversarial machine learning attacks and defenses in endpoint security models." ACM Transactions on Privacy and Security 27.1 (2024): 1-28.

21. Chatterjee, S., and Prakash, A. "Behavioral biometrics for frictionless multi-factor authentication in cloud workplaces." Future Generation Computer Systems 151 (2024): 254-269.

22. Zhao, L., et al. "Explainable AI for endpoint detection: Improving trust in automated threat response systems." Expert Systems with Applications 220 (2023): 119758.

23. Banerjee, P., and Dutta, S. "Privacy-preserving behavioral biometrics for compliance with GDPR in enterprise networks." Computers & Security 113 (2023): 102621.

24. Novak, J., and Keller, M. "Dataset challenges for benchmarking EDR and behavioral analytics tools." Journal of Computer Virology and Hacking Techniques 20.1 (2024): 33-49.

25. Tran, H., et al. "Cross-platform endpoint protection using behavioral biometrics in Windows and Linux ystems." Journal of Network and Computer Applications 210 (2025): 103630.

26. Silva, R., and Costa, L. "A comparative study of XDR and EDR solutions in mitigating advanced persistent threats." Journal of Cybersecurity Research and Practice 14.2 (2024): 89-104.

27. Park, J., and Lee, S. "Mouse dynamics for anomaly detection in online examination and enterprise authentication." Pattern Recognition Letters 167 (2023): 65-73.

28. Verma, K., and Joshi, D. "AI-enhanced threat hunting in Zero Trust endpoint environments." IEEE Access 12 (2024): 55438-55452.

29. Ranjan, A., and Mehta, R. "Scalable behavioral biometric authentication for large enterprise deployments." International Journal of Information Management Data Insights 4.1 (2024): 100198.

30. Oliveira, P., and Martins, J. "Federated learning for endpoint anomaly detection with privacy preservation." Knowledge-Based Systems 285 (2025): 111379.