Ms. Akanksha Patil. 14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

AI-Powered Remote Work Fraud Detection System

[1] Ms. Akanksha Patil, [2] Aryan Gole, [3] Harsh Pokharkar, [4] Sanika Surve

Abstract- Due to the rise of remote work, ensuring employee accountability and performance has become increasingly challenging. This has also increased cases where employees misuse work hour using keyboard jigglers, auto-clickers, or embedded chips that simulate activity, allowing employees to appear active without actually working. This project presents an AI-driven system to detect such fraudulent behavior by analyzing keystroke dynamics, mouse movement patterns, and system activity logs. The goal is to build this system to detect such behavioural data including typing speed, key press duration, inter- key delay, mouse trajectory, and interaction timing to build a unique profile for each user. These behavioural patterns are then analyzed using machine learning algorithms to detect anomalies that indicate potential fraudulent activity. The System can keep the track of what people are actually doing on their devices in real time like how someone types or moves the mouse, the system can tell the work is being done by real person or just by using an automation tool. This project aims to improve transparency in remote job roles and promote honest work culture.

Keywords: Remote Work, keyboard jigglers, Automation Device, Keystroke dynamics.

I. INTRODUCTION

The rapid digital transformation of workplaces, accelerated by the COVID-19 pandemic, has significantly reshaped the global employment structure. Remote work has evolved from a temporary solution into a mainstream operational model adopted across industries [1]. While this shift has improved flexibility, reduced operational costs, and enhanced work-life balance, it has also introduced challenges in monitoring employee productivity and maintaining organizational accountability [2]. In remote environments where direct supervision is limited, organizations increasingly rely on digital monitoring systems to evaluate employee activity, yet verifying whether this activity reflects genuine productivity remains difficult.

A major concern in remote work settings is the misuse of automation tools designed to simulate user activity. Tools such as keyboard jigglers, auto- clickers, and activity simulators can generate artificial keystrokes or mouse movements to bypass inactivity detection systems. As a result, users may appear active without performing meaningful work, creating challenges similar to those observed in behavioral authentication systems [2], [3]. Most existing monitoring systems rely on simple indicators such as keystroke counts, mouse movements, or login duration [4]. However, these systems lack behavioural intelligence and cannot reliably distinguish natural human interaction from repetitive automated patterns. To address this limitation, this research proposes an AI-driven remote work fraud detection system based on behavioural biometrics, which analyzes user interaction patterns and detects anomalies to identify suspicious activity [5].

II. LITERATURE SURVEY

Behavioral biometrics and computer vision are two important areas of Artificial Intelligence used in the proposed remote work fraud detection system. Behavioral biometrics analyzes how users interact with devices such as keyboards and mice. Each individual has unique typing speed, key press duration, and mouse movement patterns that can help distinguish genuine activity from automated tools like keyboard jigglers or macros. Computer vision verifies the physical presence of employees using face recognition through a webcam. Combining both approaches improves reliability because relying on a single technique may fail to detect certain types of fraud.

Panda and Tripathy proposed a keystroke dynamic–based approach for detecting unusual user behavior using machine learning techniques [1]. Their system analyzes typing features such as key press duration and delay between keystrokes to perform

continuous user authentication. However, the study mainly focuses on identifying users rather than detecting automation tools.

Irbaz *et al.* developed a real-time face recognition system to track remote employees using deep learning models [2]. The system periodically verifies the employee's identity through webcam-based face recognition. Although it confirms physical presence, it does not determine whether meaningful work activity is being performed.

Labayen *et al.* proposed a multimodal biometric system combining face recognition and voice analysis for online exam authentication [3]. While this approach improves identity verification, it is mainly designed for short-duration examination environments rather than long working hours.

Tiong and Lee introduced a deep learning–based system using RNN and LSTM models to detect cheating behavior in online exams [4]. Similarly, Sumaiya *et al.* proposed an automated invigilation system using face recognition, eye tracking, and screen recording to monitor exam environments [5]. These systems focus on exam integrity rather than detecting automation-based fraud in remote work scenarios.

III. METHODOLOGY

Secure Background Session Initialization

When an employee logs into the system, a secure session is created that links the employee's identity with their device using encrypted keys. After successful authentication, a background monitoring service automatically starts and runs throughout the work session. The system periodically checks whether this service is active. If the service is stopped or interrupted, an alert is immediately sent to the server to prevent monitoring tampering Testing and Implementation

Behavioural Activity Monitoring

The system continuously analyzes keyboard and mouse interactions to study behavioral patterns. For keyboard activity, features such as key press duration and the time interval between keystrokes are recorded. Mouse monitoring includes movement speed, direction changes, and cursor paths. Human activity typically shows irregular patterns, while automation tools produce repetitive behavior. The system also verifies which application is active during input activity to identify suspicious actions.

Visual Presence Verification

To confirm the presence of the employee, the system uses webcam-based face detection. At regular intervals, the camera checks for a visible face and matches it with the registered user to ensure the correct person is present.

Fraud Detection and Decision Making

The system combines data from keyboard, mouse, and face verification to evaluate activity authenticity. An integrity score is calculated, and suspicious sessions are flagged. Instead of storing raw recordings, the system generates summarized activity reports for monitoring and audit purposes while maintaining privacy.

IV. PROPOSED SYSTEM

The proposed architecture is designed to monitor employee activity securely while detecting fraudulent behavior in remote work environments. The system consists of five main components: Frontend Interface, Client Agent, Backend Services, AI/ML Processing Module.

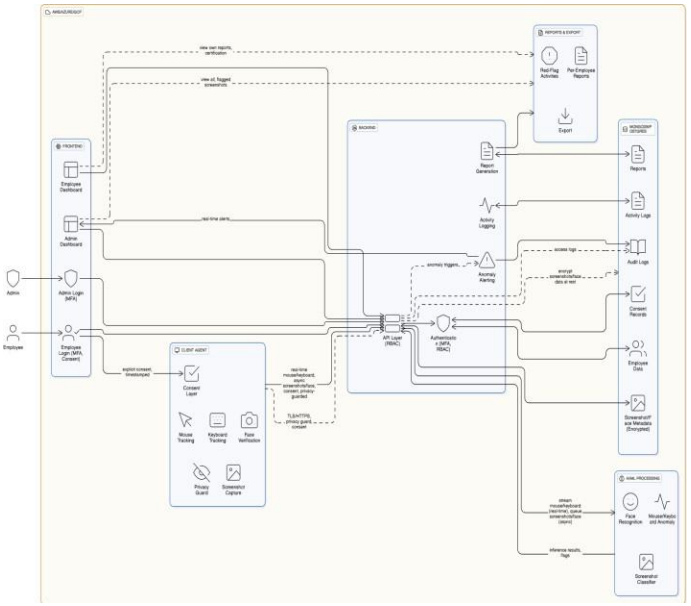


Figure: System Architecture

Frontend Layer (Employee and Admin Dashboard

The frontend provides user interfaces for both employees and administrators. Employees log in through a secure authentication process with Multi- Factor Authentication (MFA) and provide explicit consent before monitoring begins. Employees can view their activity reports and certifications through the employee dashboard. Administrators access the admin dashboard to monitor employee activities, view alerts, and review flagged screenshots or suspicious behaviors in real time.

Client Agent (Activity Monitoring Module)
The sensing module continuously monitors the scalp environment when activated by the user. The sensor captures temperature and humidity values and sends them to the microcontroller for analysis. The sensing operation can be manually enabled or disabled using a dedicated button, allowing the user to control when measurements are taken. This approach ensures power efficiency and avoids unnecessary data collection.

Backend Services
The backend acts as the central processing unit of the system. It contains an API layer with Role-Based Access Control (RBAC) and authentication mechanisms to manage secure communication between components. The backend performs activity logging, anomaly alerting, and report generation. If suspicious patterns are detected, alerts are generated and sent to the admin dashboard.

AI/ML Processing Module
The AI/ML module analyzes incoming behavioral data. It performs face recognition to verify employee presence and mouse/keyboard anomaly detection to identify automation tools or unusual behavior patterns. A screenshot classifier may also analyze captured images to detect suspicious activity.

Data Storage Layer
The system stores data securely using databases such as MongoDB or PostgreSQL. Stored information includes activity logs, reports, audit logs, employee data, consent records, and encrypted screenshot metadata. This ensures traceability while maintaining data privacy.

Reporting and Export Module
The reporting module generates per-employee reports and red-flag activity summaries. Administrators can export these reports for auditing, performance monitoring, or compliance purposes.

V. RESULT ANALYSIS

The implemented system successfully demonstrates the functionality of the proposed AI-based Remote Work Fraud Detection System.

Account Creation Interface
Employees enter personal details such as name, email, contact number, username, and password. The system also requires uploading a photo, document, and ID card for identity verification. This ensures that only verified users can access the monitoring system.

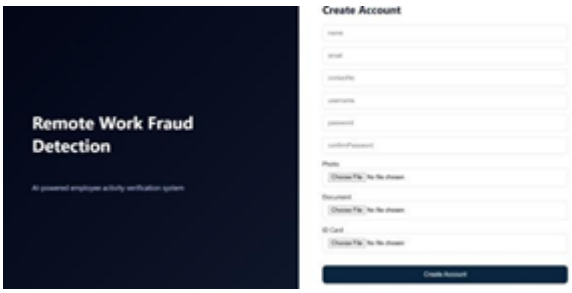


Figure 2: Account creation

Work monitoring
The system continuously monitors keyboard typing patterns, mouse movements, and active screen usage to identify productive behavior.

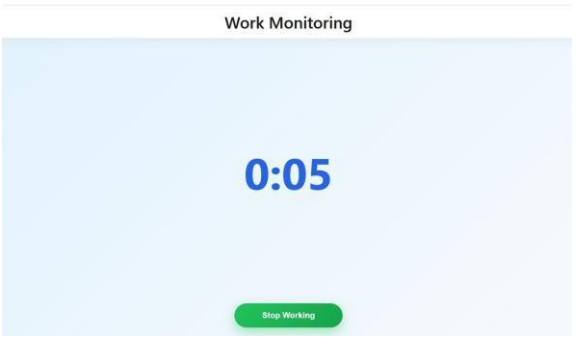


Figure 3: Work monitoring

Employee Work Report Dashboard
It summarizes metrics such as total work time, wasted time, and efficiency percentage. A pie chart visually represents the distribution between productive work time and wasted time, helping administrators evaluate employee performance.

Figure 4: Work report

Typing activity proof
The system detects unusual typing patterns such as gibberish or random keystrokes, which may indicate the use of automation tools or unnatural activity. Each detected event is logged with a timestamp for verification.

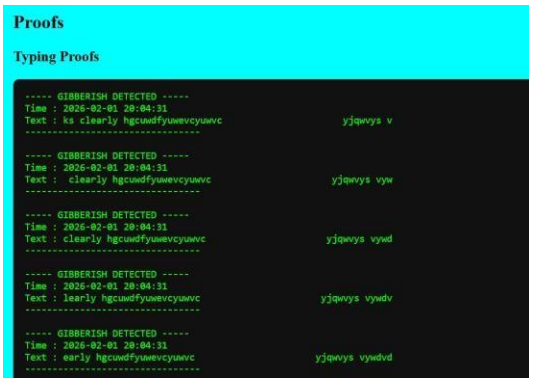


Figure 5: Typing proof

Face Verification Proof

This screenshot shows webcam-based face capture used for presence verification. The system periodically captures images to confirm that the actual employee is present in front of the device during working hours.

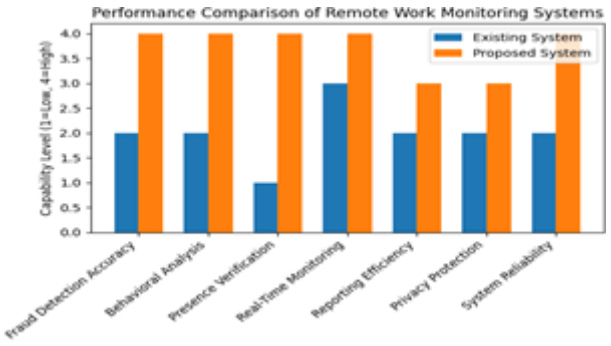
Figure 6: Face verification

Screen Activity Proof

This screenshot represents periodic screen captures taken by the system. These images provide evidence of the employee's active workspace and help verify that meaningful work is being performed. Screen proofs are stored for audit and monitoring purposes.

Figure 7: Screen proof

VI. SYSTEM COMPARISON



The graph presents a comparative analysis between the existing remote work monitoring systems and the proposed AI-based remote work fraud detection system across several important performance parameters. The parameters considered include fraud detection accuracy, behavioral analysis capability, presence verification, real-time monitoring, reporting efficiency, privacy protection, and system reliability.

From the graph, it can be observed that existing systems show moderate performance because they mainly rely on basic activity indicators such as login time or simple keyboard and mouse activity tracking. These methods are limited and can be easily manipulated using automation tools like keyboard jigglers or auto-clickers.

In contrast, the proposed system demonstrates significantly higher capability across most parameters. This improvement is due to the integration of behavioral biometrics (keystroke dynamics and mouse movement analysis) and computer vision- based face verification. These technologies allow the system to detect automated behavior more accurately while ensuring that the actual employee is present during work sessions.

Overall, the graph highlights that the proposed system provides better accuracy, stronger monitoring capability, improved reliability, and enhanced transparency, making it a more effective solution for detecting fraud in remote work environments.

VII. SCOPE OF RESEARCH

This research focuses on developing an AI-based system to detect fraudulent activities in remote work environments. The system analyzes behavioral biometrics such as keystroke dynamics, mouse movement patterns, and face verification to differentiate genuine human activity from automated tools like keyboard jigglers or auto-clickers. The research aims to improve employee accountability, enable real-time monitoring, and generate meaningful activity reports while maintaining user privacy. The proposed approach can be applied in organizations that use remote or hybrid work models to ensure transparency, prevent

misuse of work hours, and support fair performance evaluation.

VIII. CONCLUSION

The growth of remote work has increased the risk of employees misusing work hours through automation tools. This paper proposed an AI-powered fraud detection system that combines behavioral biometrics, including keystroke dynamics, mouse movement patterns, and computer vision-based presence verification. By integrating multiple monitoring methods, the system can effectively distinguish genuine human activity from automated behavior. Experimental results show that the system provides accurate detection, real-time monitoring, and meaningful reporting while maintaining user privacy. Overall, the proposed solution improves transparency and accountability in remote work environments and supports fair performance evaluation in modern organizations.

IX. FUTURE SCOPE

Although the proposed system successfully detects automation-based fraud using behavioral monitoring and visual verification, several enhancements can be explored in future work to further improve detection accuracy and system intelligence. A weighted fusion layer can be incorporated to intelligently combine outputs from keyboard behavior analysis, mouse activity patterns, and visual presence verification, enabling the system to generate a more adaptive and reliable integrity score. Additionally, advanced liveness-detection techniques may be integrated into the visual verification module to ensure that the detected face belongs to a real user rather than a static image or prerecorded video. Another important improvement involves applying Shannon entropy–based analysis to mouse movement behavior. In some situations, automated bot-generated mouse activity may exhibit movement frequencies similar to human interaction, making detection difficult using basic variance-based methods. Entropy analysis can help measure the randomness and complexity of mouse trajectories, allowing the system to better distinguish genuine human control from automated scripts. These enhancements would strengthen the robustness of the framework and move the system toward a more intelligent and adaptive remote work fraud detection solution.

X. DISCUSSION

The implementation of the proposed AI-based Remote Work Fraud Detection System shows clear improvements over traditional activity monitoring methods. Conventional systems mainly rely on simple indicators such as login time or basic keyboard and mouse activity, which can easily be manipulated using automation tools. In contrast, the proposed system analyzes behavioral biometrics such as keystroke dynamics and mouse movement patterns to distinguish genuine human activity from automated behavior. The integration of webcam- based face verification further ensures that the actual employee is present during work sessions. This combination of behavioral analysis and visual verification improves the reliability of fraud detection. Additionally, the system generates summarized activity reports and alerts for administrators, enabling better monitoring while maintaining user privacy. Overall, the proposed system provides a more accurate and practical solution for detecting fraudulent activities in remote work environments.

XI. ACKNOWLEDGEMENT

It is a privilege for our team to have worked under the guidance of Ms Akanksha Patil ma'am during this project. We have greatly benefited from her valuable advice and constant support. We sincerely express our gratitude for her encouragement, patience, and assistance throughout the completion of this work. Her suggestions have greatly enhanced the quality of our project.

REFERENCES

1. M. S. Irbaz, M. A. Al Nasim, and R. E. Ferdous, "Real- Time Face Recognition System for Remote Employee Tracking," Preprint, Jul.2021. [Online]. Available: arXiv:2107.07576.
2. M. Labayen, R. Vea, J. Fl´orez, N. Aginako, and B. Sierra, "Online Student Authentication and Proctoring System Based on Multimodal Biometrics Technology," IEEE Access, vol. 9, pp. 72398–72415, 2021.
3. L. C. O. Tiong and H. J. Lee, "E-cheating Prevention Measures: Detection of Cheating at Online Examinations Using Deep Learning Approach – A Case Study," Journal of LaTeX Class Files, Jan. 2021.
4. N. Sumaiya et al., "Automated Invigilation System for Detection of Suspicious Activities During Examination," IRJET, vol. 10, no. 4, Apr.2023.
5. P. Panda and A. Tripathy, "Detecting Fraudulent Pattern through Key Stroke Dynamics using Machine Learning Algorithm," in Proc. ASSIC,2024

Author's Details

1. Assistant Professor, Computer Engineering, Pillai HOC College Of Engineering and Technology (Autonomous), Ms. Akanksha Patil, Maharashtra, India, akankshapatil@mes.ac.in
2. Student, Computer Engineering, Pillai HOC College of Engineering and Technology (Autonomous), Mr. Aryan Sanjay Gole, Maharashtra, India, swarupsg23hcompe@student.mes.ac.in
3. Student, Computer Engineering, Pillai HOC College of Engineering and Technology (Autonomous), Mr. Harsh Anil Pokharkar, Maharashtra, India, harshap23hcompe@student.mes.ac.in
4. Student, Computer Engineering, Pillai HOC College of Engineering and Technology (Autonomous), Ms. Sanika Vishvnath Surve, Maharashtra, India, sanikavs23hcompe@student.mes.ac