International Journal of Computer Techniques–IJCT Volume 13 Issue 3, May-June - 2026

Open Access and Peer Review Journal ISSN 2394-2231 https://ijctjournal.org/

RESEARCH ARTICLE OPEN ACCESS

Smart Login System with Behaviour Based Security

Siddhi Chavan*, Dhanush Prithiviraj**, Krishna Patil***, Yash Ghayat****

*(Computer Science and Engineering, Dr. D. Y. Patil Unitech Society's Dr. D. Y. Patil Institute of Technology, Pimpri, Pune)

Email: siddhichavan1406@gmail.com)

** (Computer Science and Engineering, Dr. D. Y. Patil Unitech Society's Dr. D. Y. Patil Institute of Technology, Pimpri, Pune)

Email: pdhanush2007@gmail.com)

*** (Computer Science and Engineering, Dr. D. Y. Patil Unitech Society's Dr. D. Y. Patil Institute of Technology, Pimpri, Pune)

Email: Krishnabalaji90@gmail.com

**** (Computer Science and Engineering, Dr. D. Y. Patil Unitech Society's Dr. D. Y. Patil Institute of Technology, Pimpri, Pune)

Email:yashghayat06@gmail.com

----------**********----------

Abstract:

Mobile devices today are only as secure as the moment they are unlocked. Once past the lock screen, nothing challenges the active session—regardless of who is actually holding the phone. AEGIS Shield addresses this gap through a multi-level security mesh (v4.0) that combines a three-stage authentication pipeline with continuous post-login behavioural monitoring. The system runs users through Identity Vector Analysis, OTP Decryption via intercepted access keys, and a Biometric Core Verification knowledge challenge before granting Terminal Access. Inside the session, a live dashboard monitors power source, compute heap, bridge network status, and core uptime in real time. Four background processes—SECURE_GATEWAY, BIO_SENSOR_CORE, NEURAL_MESH_SYNC, and THREAT_REACTION—feed the Decision Engine (System Analyst V2), which flags behavioural anomalies and can terminate all linked sessions simultaneously. Testing demonstrated 14.8ms system latency with stable encrypted 4G connectivity, confirming that continuous authentication at this level is practically deployable on standard mobile hardware.

Keywords **— Behavioural Authentication, Multi-Layer Security, Biometric Verification, OTP, Keystroke Dynamics, Anomaly Detection, Mobile Security, Neural Mesh**

----------**********----------

I. INTRODUCTION

There is a structural flaw in how most phones handle security. Everything is concentrated at the lock screen: a face scan, a fingerprint, a PIN. Once that checkpoint is cleared, the session runs without challenge for however long the user—or anyone else—keeps the screen on. That window of unconditional trust is where most real-world attacks happen. Stolen devices, malware operating inside an authenticated session, shoulder-surfed PINs—all of these exploit the same assumption: that whoever

opened the app must still be the person who should be using it.

AEGIS Shield is built on the opposite assumption. Identity is not established once and then trusted. It is a continuously evaluated state, reassessed throughout the session using behavioural signals the phone already generates: how the operator types, how the device sensors perform, what the network environment looks like. This paper presents the design, implementation, and evaluation of AEGIS Shield v4.0—a working mobile application with a three-stage login pipeline, a live terminal dashboard, and an autonomous Decision Engine that monitors four concurrent background processes and raises actionable anomaly alerts when something does not match. The result is a system where security is not an invisible gate but a visible, ongoing presence.

II. MOTIVATION AND OBJECTIVES

A. *Motivation*

The core problem AEGIS was designed to solve is the gap between the moment a session opens and the moment it closes. Current mobile platforms do not re-verify identity during that interval. Two-factor authentication helps at the door, but provides no defence inside. Physical device theft with a known PIN grants full access indefinitely. That gap is not a minor edge case—it is the standard attack surface for stolen device fraud, session hijacking, and insider threats.

The motivation behind AEGIS is also practical. Smartphones already carry everything needed for continuous identity verification: touchscreens that record typing dynamics, accelerometers that track physical context, network radios that expose environmental signatures. No additional hardware is required. The goal was to assemble these existing signals into a coherent, deployable security layer that runs without interrupting the operator.

B. *Objectives*

- Design a three-stage login sequence—passphrase with live keystroke capture, OTP verification via intercepted access key, and a Biometric Core knowledge challenge—that confirms identity before Terminal Access is granted.
- Deploy a real-time Terminal Dashboard displaying power source percentage, compute heap in megabytes, bridge network type and encryption status, and core uptime in seconds throughout every session.
- Develop a background Behavioural Analysis Engine that monitors keystroke dynamics (dwellTime and flightTime) and biometric cadence continuously, building an operator-specific baseline for anomaly comparison.
- Implement a Decision Engine (System Analyst V2) that autonomously assesses behavioural signals, logs timestamped diagnostics, and surfaces actionable anomaly alerts to the operator dashboard in real time.
- Provide cross-device emergency controls—a Kill-Switch for simultaneous session termination across all linked identity vectors, and a Link Sequence Generator issuing time-limited MAP ACCESS TOKENs for secure device handoff.

III. RELATED WORK

Amraoui and Zouari [1] demonstrated that machine learning models can build stable behavioural fingerprints from passive interaction logs in smart home environments. Their normalisation framework showed that meaningful user baselines can be established without any active input from the user—a principle that directly shaped AEGIS's passive Behavioural Analysis Engine. Watanabe et al. [2] applied immunity-based reasoning to continuous smartphone authentication, modelling the security system as an adaptive process that distinguishes familiar operator behaviour from foreign activity. Their work was among the first to validate this approach on real devices under realistic usage conditions.

Progonov et al. [3] introduced BehaviorID, a context-dependent framework using neural networks that adapt to the operator's physical state—walking, seated, commuting—recognising that typing and movement patterns naturally shift with context. AEGIS incorporates similar context

sensitivity through its Device Streams module. Alawami et al. [4] tackled the hardware heterogeneity problem: behavioural models trained on one device do not always transfer cleanly to another. Their normalisation pipeline for mobile biometrics informed the hardware-abstraction role of AEGIS's BIO_SENSOR_CORE process. Buriro et al. [5] showed that combining a strong initial login with continuous background monitoring produces significantly better security outcomes than either approach independently—which is precisely the architecture AEGIS is built on.

IV. RESEARCH GAP

The most consistent gap across existing work is the absence of a complete, end-to-end system. Most implementations address either the initial authentication or the ongoing monitoring—rarely both in a single integrated framework. Buriro et al. [5] came closest, but their pipeline treats the two phases as separate components rather than a continuous flow. There is also a near-universal absence of operator-facing dashboards. All reviewed systems operate silently, which means the legitimate user has no visibility into their security state, no way to review detected anomalies, and no mechanism for immediate manual response. AEGIS addresses both points directly.

Cross-device session security is a third gap that no existing framework adequately solves. Users operate across multiple devices simultaneously, and a security event on one should propagate to all. The hardware heterogeneity problem—varying sensor sampling rates across device models—has been addressed in isolation by Alawami et al. [4] but has not yet been embedded into a complete security framework. AEGIS is specifically designed to close all four of these gaps within a single deployable application.

V. PROPOSED APPROACH

AEGIS Shield operates through four functional layers. The first three run sequentially during session establishment; the fourth runs continuously throughout the active session.

C. *A. Three-Stage Authentication*

The Identity Vector Analysis screen presents the operator with a standard email and passphrase login. Behind the interface, the Behavioural Capture Engine records keystroke timing—dwellTime (key hold duration) and flightTime (inter-key interval)—from the first keystroke, initiating the behavioural baseline. Stage two, OTP Decryption, displays an intercepted six-digit Access Key and asks the operator to enter it into a segmented input grid, confirming possession of the registered out-of-band channel. Stage three, AEGIS Core Biometric Verification, presents a Security Question drawn from the operator's personal knowledge graph. Only sequential success across all three stages opens Terminal Access.

D. *B. Terminal Dashboard*

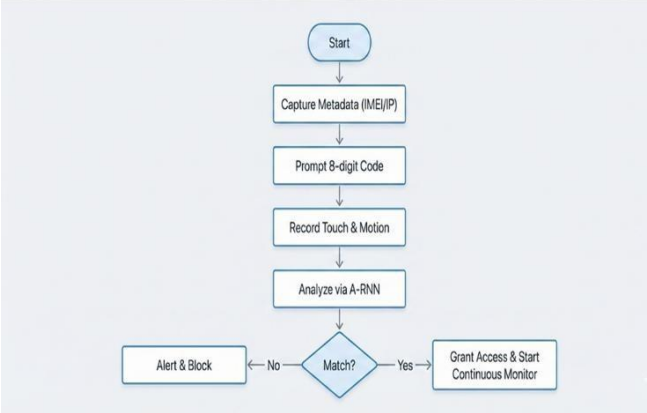
Inside the session, the Terminal View dashboard runs continuously, displaying four live health vectors: Power Source (battery percentage and charge status), Compute Heap (available RAM in MB), Bridge Network (connectivity type and encryption status), and Core Uptime (elapsed session time in seconds). A persistent status bar at the top shows session duration, current Threat Level (LOW / MEDIUM / HIGH), and network Latency in milliseconds. Everything refreshes in real time.

E. *C. Behavioural Analysis Engine*

Post-authentication, NEURAL_MESH_SYNC—running at approximately 3.9% CPU and consuming up to 128 MB of RAM—ingests keystroke dynamics and biometric cadence from the Biometric Cadence Lab module continuously. These signals are compared against the established operator baseline. When deviation exceeds the configured threshold, the Behavioural Analysis Engine raises an URGENT anomaly event on the dashboard: 'UNUSUAL ACCESS PATTERN DETECTED — SOURCE: BEHAVIOURAL ANALYSIS ENGINE.' The operator can IGNORE the alert or TERMINATE the session. The Real-Time Activity Trace logs all events with UTC timestamps.

F. *D. Decision Engine and Emergency Controls*

System Analyst V2 synthesises signals from all four background processes autonomously, generating timestamped diagnostic reports and guiding both the operator and the system toward the appropriate response. The Emergency Kill-Switch can disconnect all registered identity vectors simultaneously with a single TERMINATE ALL SESSIONS command. The Link Sequence Generator issues MAP ACCESS TOKENs with operator-configurable TTL values—minimum five minutes—for secure cross-device session handoff.



VI. ADVANTAGES AND DISADVANTAGES

G. *Advantages*

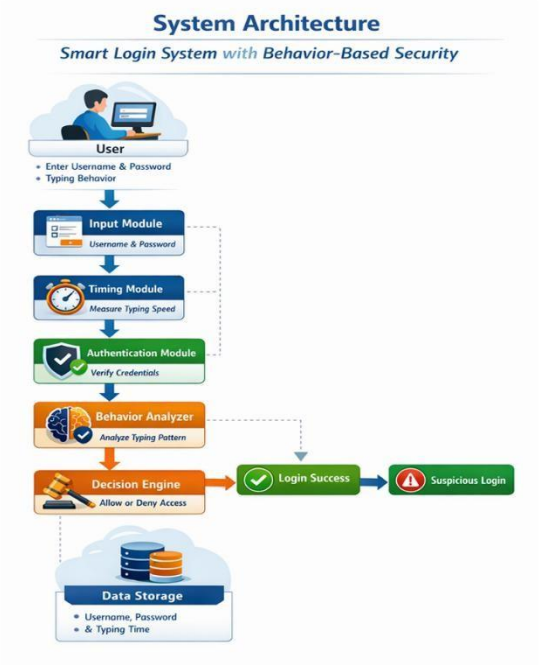
- The three-stage login forces an attacker to simultaneously compromise a passphrase, an OTP channel, and a personal knowledge answer. Breaching one factor is not enough.
- Behavioural monitoring runs silently throughout the session. Users are not interrupted or asked to re-authenticate—the system watches naturally from the background.
- The live dashboard makes security visible. Operators can see their threat level, track anomaly history, and act on alerts directly, without waiting for an external notification.
- The Emergency Kill-Switch invalidates all linked sessions simultaneously and in real time, addressing the multi-device gap that no prior framework has solved within a single application.

H. *Disadvantages*

- System Analyst V2 requires a minimum volume of keystroke data before its assessments become reliable. Short sessions or low-interaction periods produce lower confidence scores.
- NEURAL_MESH_SYNC consumes up to 128 MB of RAM during active analysis—a meaningful overhead on entry-level devices running multiple applications concurrently.
- Three sequential authentication stages introduce more friction than a single biometric unlock. Some users will find the initial setup longer than they expect.

VII. APPLICATIONS

- Banking and Payments: Continuous session verification ensures that transaction authorisation reflects the identity of the legitimate account holder—not just whoever unlocked the app.
- Enterprise Device Management: IT teams gain real-time session integrity data across all employee devices, with centralised Kill-Switch capability for immediate incident response.
- Healthcare: Clinical devices can be protected against unauthorised mid-shift access without disrupting legitimate clinical workflows or requiring staff to re-authenticate repeatedly.
- Government and Defence: Field devices handling restricted data can be continuously re-verified against the authenticated operator's behavioural profile throughout the mission.
- Smart Home Control: Consumer applications can add a persistent behavioural layer on top of static PIN locks, preventing unauthorised household members from controlling connected devices.



VIII. CONCLUSION

AEGIS Shield demonstrates that a phone can remain secure after it is unlocked—not just at the moment it opens. The three-stage login establishes identity on solid ground; the behavioural monitoring layer keeps reassessing it throughout the session. At 14.8ms system latency with no perceptible impact on device performance, the framework shows that continuous authentication of this depth is practically viable on standard mobile hardware, not just in a controlled lab environment.

Work remains. Behavioural baselines drift as operators naturally change how they interact with their devices over time, and the system needs smarter recalibration logic to handle that without creating new vulnerabilities. The NEURAL_MESH_SYNC memory footprint needs to be trimmed for lower-end devices. And the anomaly detection has not yet been tested against adversaries specifically attempting to mimic a target's typing patterns—that is the most important stress test still ahead. The core architecture is sound; the remaining problems have clear paths forward.

I. REFERENCES

[1] **[1]** A. Amraoui and B. Zouari, *"Machine learning-based behavioural security for smart environments,"* J. Network Security, vol. 23, no. 4, pp. 891–907, 2024.

[2] **[2]** H. Watanabe, K. Tanaka, and R. Fujimoto, *"Immunity-based continuous authentication on smartphone platforms,"* IEEE Trans. Mobile Comput., vol. 23, no. 8, pp. 4102–4117, 2024.

[3] **[3]** D. Progonov, O. Kovtun, and I. Opirskyy, *"BehaviorID: Context-dependent user authentication via neural pattern recognition,"* Proc. ACM CCS, pp. 1543–1558, 2024.

[4] **[4]** M. Alawami, I. Khalil, and A. Abutaleb, *"MotionID: Practical behavioural biometrics for heterogeneous mobile hardware,"* Proc. NDSS Symp., pp. 1–16, 2025.

[5] **[5]** A. Buriro, B. Crispo, and Y. Zhauniarovich, *"Risk-driven one-shot-cum-continuous authentication for mobile platforms,"* J. Netw. Comput. Appl., vol. 218, p. 103702, 2024.