Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

The D.I.N.K.U. Framework: Adaptive Authentication via Dynamic Intelligence and Key-Rotation

Vaibhav Upendra
Dept. of CSE (Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur

Pranav Dinakar
Dept. of CSE (Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur

Niranjan Vinod K V
Dept. of CSE (Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur

Ms. Anugraha P P
Assistant Professor, Dept. of CSE
Vimal Jyothi Engineering College
Chemperi, Kannur

***Abstract*—Modern authentication systems depend heavily on static credentials such as passwords and PINs; however, these mechanisms are fundamentally passive and fail to account for the dynamic behavioural context of the legitimate user. This outdated approach is vulnerable to credential theft, replay attacks and session hijacking, all of which exploit the inability of conventional systems to distinguish an authenticated user from an attacker who has obtained their credentials. Furthermore, the increasing use of static cryptographic configurations means that the strength of data protection remains constant regardless of the assessed risk level of a given session. To address these critical issues, this work proposes D.I.N.K.U. (Dynamic Intelligence Network & Key-rotation Unit), an adaptive authentication system that continuously evaluates user identity through behavioural biometrics, hardware fingerprinting and network analysis and automatically escalates both cryptographic strength and multi-factor authentication requirements in real time based on a computed trust score. D.I.N.K.U. integrates a Hybrid CNN-Transformer model for keystroke dynamics analysis, a five tier adaptive cryptography engine spanning AES-256-GCM, ChaCha20-Poly1305, Argon2id key derivation and RSA-2048 wrapping, alongside real FIDO2 WebAuthn biometric authentication and RFC 6238 TOTP. By offering a verifiable encryption proof interface and a persistent audit log, D.I.N.K.U. provides a unified, intelligent and risk proportionate security platform that restores user trust without sacrificing operational convenience.**

***Index Terms*—Operating System Security, Behavioral Analysis, Keystroke Dynamics, Adaptive Cryptography, FIDO2 WebAuthn, Zero-Trust Architecture, Multi-Factor Authentication.**

I. INTRODUCTION

A. Overview

The D.I.N.K.U. (Dynamic Intelligence Network & Key-rotation Unit) framework is an adaptive authentication system designed to move beyond static password based verification toward a continuous, behaviour aware model of identity assurance. Unlike conventional systems that grant or deny access based solely on a credential match, D.I.N.K.U. computes a real time trust score from three complementary signals: keystroke biometrics, hardware device fingerprinting and network latency analysis. This trust score drives two automated responses the selection of an appropriate cryptographic algorithm pair from a five tier adaptive engine and the triggering of step up multi-factor authentication when the score falls below a configurable threshold.

At its core, D.I.N.K.U. integrates a Hybrid CNN-Transformer model that learns each user's unique typing rhythm during enrolment and scores subsequent login attempts against this baseline. By combining convolutional layers for local keystroke feature extraction with transformer attention for temporal sequence modelling, the system achieves a nuanced understanding of behavioural authenticity that neither architecture could provide alone. This is complemented by real FIDO2 WebAuthn biometric authentication and RFC 6238 TOTP, ensuring that even when the behavioural trust score is low, a cryptographically verified second factor is required before access is granted.

B. General Background

In the modern digital landscape, authentication has evolved from simple shared secrets into layered security protocols. However, most deployed systems still rely on a binary authentication model: either a user knows the correct password or they do not. This model is fundamentally incapable of distinguishing a legitimate user from an attacker who has obtained their credentials through phishing, data breach or social engineering. The growing sophistication of credential based attacks, including adversary in the middle interception, credential stuffing and session token theft highlights the inadequacy of static authentication in protecting sensitive systems.

Simultaneously, the cryptographic configurations used by most applications remain fixed regardless of the assessed risk level of a session. A high trust login from a recognised device on a low latency network is treated identically, from a data protection standpoint, to a suspicious login attempt from an unrecognised device with anomalous behavioural signals. This one size fits all approach to encryption wastes the opportunity to apply stronger, more computationally intensive algorithms when the risk profile demands it.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

C. Problem Definition

The primary challenge addressed by D.I.N.K.U. is the inadequacy of static, credential only authentication models. Current systems offer no mechanism to assess whether the entity presenting a valid password is actually the enrolled user. Once credentials are compromised, the attacker operates with the full trust level of the legitimate account holder for the duration of the session.

Additionally, modern applications apply a uniform cryptographic configuration to all sessions, irrespective of the trust level established during authentication. This creates an unnecessary vulnerability: high risk sessions with anomalous behavioural signals receive the same encryption strength as verified low risk sessions. There is therefore a critical gap in existing systems the absence of a mechanism that continuously validates behavioural identity and proportionately escalates both cryptographic protection and authentication requirements in response to detected risk.

D. Scope and Objective

This system encompasses the engineering of a full stack adaptive authentication platform comprising a Python FastAPI backend, a Hybrid CNN-Transformer Al model, a five tier cryptographic engine and a web based interactive dashboard. The objectives include:

- To design a keystroke biometric enrolment and scoring engine that captures dwell time, flight time and typing rhythm as distinguishing identity features.
- To implement a Hybrid CNN Transformer model that accurately scores runtime typing behaviour against a per user enrolled baseline.
- To build a five tier adaptive cryptographic engine that escalates encryption and key derivation strength in direct proportion to the computed trust score.
- To integrate FIDO2 WebAuthn biometric authentication and RFC 6238 TOTP as step up second factors.
- To provide a persistent audit logging system that records every authentication event with full cryptographic context for administrative review.

II. LITERATURE REVIEW

A. Keystroke Dynamics as a Behavioural Biometric

Keystroke dynamics analysis leverages the unique timing characteristics of an individual's typing behaviour, specifically the dwell time a key is held and the flight time between consecutive keystrokes as a continuous biometric identifier [1]. Early work in this area demonstrated that statistical models trained on these features could achieve user verification accuracy comparable to fingerprint recognition in constrained environments. The challenge, however, lies in accommodating natural variation in typing speed and style due to fatigue, emotional state or keyboard differences.

More recent work replaces statistical distance with neural classifiers, including Siamese networks and recurrent architectures [2], that learn a latent representation of typing rhythm rather than measuring raw timing distances. The literature consistently demonstrates that keystroke dynamics provide a viable and low cost behavioural biometric that does not require specialised hardware, validating D.I.N.K.U.'s choice to use a Hybrid CNN-Transformer model.

B. Adaptive Cryptography and Risk Based Encryption

Traditional cryptographic systems apply a fixed algorithm and key length uniformly across all sessions, irrespective of the assessed risk level [3]. Research into adaptive or risk based cryptography explores frameworks that select the appropriate cipher suite dynamically based on contextual signals such as user location, device trust, time of access and authentication confidence. These systems argue that higher computational cost of stronger algorithms such as Argon2id for key derivation or RSA wrapping for session keys should be reserved for sessions where the trust signal is low, reducing overhead for verified high trust interactions.

C. FIDO2 WebAuthn and Phishing Resistant Authentication

The FIDO2 standard defines a phishing resistant authentication protocol in which cryptographic credentials are bound to the origin of the relying party, preventing credential reuse across domains [4]. WebAuthn, the W3C specification implementing FIDO2 in browsers, allows authenticators such as platform biometric sensors (Touch ID, Windows Hello) and roaming security keys to perform challenge-response authentication without transmitting the private key or any biometric data to the server. The private key material never leaves the authenticator device, providing a security guarantee independent of the behavioural scoring layer.

D. Hardware Fingerprinting for Device Identity

Browser based hardware fingerprinting aggregates passive device characteristics such as GPU renderer string, screen resolution, CPU core count, device memory, timezone, language and touch support into a stable device identifier without requiring explicit user consent or persistent cookies [5]. Research has demonstrated that these fingerprints provide sufficient entropy to uniquely identify a large proportion of devices in the wild, making them a viable passive signal for continuous authentication and anomalous login detection.

E. Multi-Factor Authentication and Step Up Triggers

Traditional MFA requires a second factor at every login, creating user friction that leads to abandonment and workarounds [6]. Research into step up or risk adaptive MFA proposes that the second factor should be demanded only when risk signals cross a defined threshold, allowing low risk sessions to proceed without additional friction while escalating authentication requirements in proportion to the assessed threat level. This approach maintains security posture while reducing cognitive load on users in verified low risk scenarios.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

III. REQUIREMENT SPECIFICATION

The D.I.N.K.U. framework is engineered to establish a paradigm shift in authentication architecture. The fundamental requirement is to move away from binary authentication toward a risk proportionate model where trust is computed dynamically and both cryptographic protection and secondary verification requirements are scaled accordingly.

A. Functional Requirements

The core functional requirements of the system are designed to ensure comprehensive security coverage across the authentication lifecycle.

TABLE I
D.I.N.K.U. FUNCTIONAL REQUIREMENTS

Req.	Description
FR1	**Keystroke Enrolment:** The system must capture keystroke timing events (dwell time, flight time, digraph timing) across configurable samples (3-10) to build a baseline.
FR2	**Trust Score Computation:** At each login attempt the system must compute a composite trust score from keystroke similarity (55%), hardware fingerprint (30%) and network latency (15%).
FR3	**Adaptive Crypto Selection:** The system must automatically select the appropriate cryptographic algorithm pair from five defined tiers based on the trust score.
FR4	**WebAuthn Registration:** Must support FIDO2 WebAuthn registration using platform authenticators and roaming security keys.
FR5	**WebAuthn Authentication:** Must perform a complete FIDO2 challenge-response ceremony for step up MFA.
FR6	**Hardware Fingerprinting:** Collect GPU renderer, screen resolution, CPU cores, memory, OS version as device identity signals.

B. Non-Functional Requirements

Key non-functional requirements dictate that the complete trust score computation pipeline must complete in under 200ms per login attempt to preserve user experience. Furthermore, each cryptographic pair must successfully encrypt and decrypt arbitrary plaintext with a verified authentication tag, confirmed by an interactive round trip proof interface.

IV. PROPOSED SYSTEM AND DESIGN

A. Key Components

The D.I.N.K.U. framework is composed of several integrated modules:

- **Keystroke Profiler:** Captures per keystroke dwell time, flight time between successive keys and digraph timing. During enrolment, multiple samples are consolidated using an exponential moving average. At login, a Gaussian probability scoring model computes the likelihood that the runtime sample was produced by the enrolled user.
- **Hybrid CNN-Transformer Model:** A neural architecture combining 1D convolutional layers for local feature extraction from keystroke timing sequences with transformer self attention for modelling long range temporal dependencies within a typing session. The model processes a fixed length feature tensor of 128 timesteps x 3 features.
- **Hardware Fingerprinting Module:** Collects GPU renderer string, screen resolution, CPU core count, device memory, platform, architecture, OS version, timezone and language. These are compared against the stored enrolment fingerprint to produce a hardware match score on a per field basis.
- **Adaptive Cryptographic Engine:** A five tier algorithm selection system. Each tier defines an encryption cipher and an authentication mechanism.
- **MFA Manager:** Handles both FIDO2 WebAuthn registration/authentication ceremonies and RFC 6238 TOTP. Step up challenges are triggered automatically when the trust score falls below 0.50.

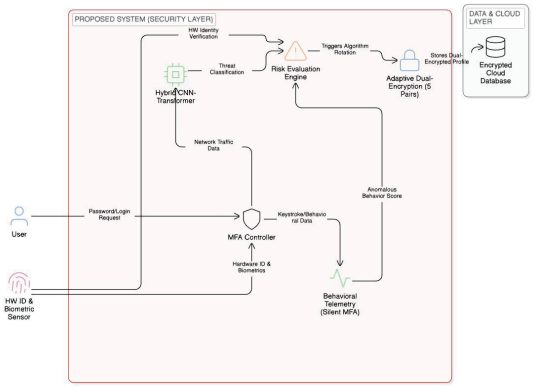

Fig. 1. D.I.N.K.U. System Architecture detailing the flow from behavioural data capture to the Risk Evaluation Engine and Adaptive Encryption.

B. Trust Score Formula

The composite trust score is computed as a weighted linear combination:

$$T = 0.55S_{ks} + 0.30S_{hw} + 0.15S_{net} \quad (1)$$

where S_{ks} is the keystroke similarity score, S_{hw} is the hardware fingerprint match score and S_{net} is the network latency score. The result $T \in [0, 1]$ determines the cryptographic pair and MFA requirement.

C. Algorithm Selection Table

The five tier cryptographic engine maps trust score bands to specific algorithm pairs as detailed in Table II.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

TABLE II
D.I.N.K.U. FIVE TIER CRYPTOGRAPHIC ALGORITHM SELECTION

Tier	Trust	Encryption	MFA
STANDARD	> 0.85	AES-256-GCM (SHA-256)	None
HIGH-SPEED	$0.67 - 0.85$	ChaCha20-Poly1305 (BLAKE2b)	None
MEMORY-HARD	$0.50 - 0.67$	AES-256-GCM (PBKDF2-HMAC)	None
POST-QUANTUM	$0.35 - 0.50$	AES-256-GCM (SHA-256)	Step Up
LOCKDOWN	< 0.35	RSA+AES-256-GCM	Lockdown

V. IMPLEMENTATION

A. Backend Implementation

The D.I.N.K.U. backend is implemented as a FastAPI application in Python 3.12. The primary modules include `api.py` for REST endpoints, `keystroke_profiler.py` for baseline enrolment and Gaussian scoring, `crypto_manager.py` for the five tier cryptographic engine and `mfa_manager.py` handling FIDO2 WebAuthn ceremonies and RFC 6238 TOTP. The backend is proxied through Caddy with automatic local HTTPS certificate management to ensure secure context for WebAuthn.

B. Frontend Implementation

The D.I.N.K.U. frontend is a single HTML5 file using vanilla JavaScript and CSS custom properties for theming. It implements a fixed top bar, collapsible sidebar, real time keystroke visualiser bars, an animated trust score ring, an interactive encryption proof interface and a protected admin panel.

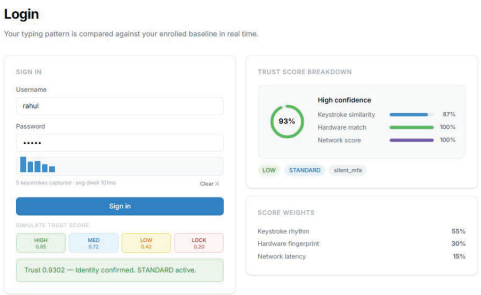

Fig. 2. Login page showing animated trust score ring and score breakdown metrics derived from keystroke rhythm, hardware and network latency.

C. Keystroke Profiler Logic

The KeystrokeProfiler captures keyboard events via `onkeydown` and `onkeyup` browser event listeners. During enrolment, the captured event sequence from each password sample is sent to the backend and incorporated into the user baseline via exponential moving average with $\alpha = 0.4$. The baseline stores per feature mean and standard deviation, with minimum standard deviation floors (e.g., 25ms for dwell) to prevent over fitting to any single sample. At login time, the scorer computes a z score for each event feature against the baseline parameters, applies a Gaussian kernel with $\sigma = 1.2$ and averages across all captured events to produce the final keystroke similarity score S_{ks}.

D. Cryptographic Engine implementation

The `CryptoManager` class implements five independently testable encrypt/decrypt method pairs. All AES-GCM operations use a 12-byte nonce generated by a cryptographically secure random number generator. The MEMORY-HARD tier uses PBKDF2-HMAC-SHA256 with 100,000 iterations using the session nonce as salt. The LOCKDOWN tier wraps the AES session key with RSA-OAEP using a 2048-bit key pair generated lazily on first use.

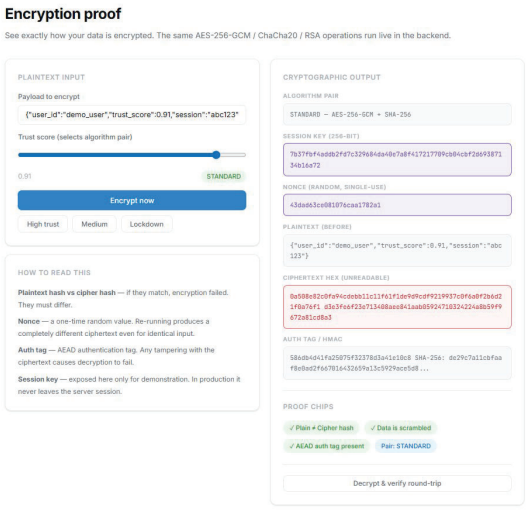

Fig. 3. Encryption proof interface displaying ciphertext, nonce and authentication tag verification for the selected security tier.

E. Audit Log and Administration

Every authentication event is persisted to `aegis-audit.json` with full cryptographic context. The admin system uses in-memory session tokens (UUIDs) with a one hour TTL. Account suspension blocks login at the API endpoint and triggers Telegram Bot API notifications to a configured admin chat ID, providing real time awareness of account activity.

VI. RESULTS AND DISCUSSION

The evaluation of the D.I.N.K.U. framework involved a multi dimensional testing suite designed to measure the accuracy of its behavioural trust scoring, the correctness of its adaptive cryptographic engine, the reliability of its step up MFA ceremonies and the responsiveness of its web based interface.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

A. Component-wise Performance Analysis

1) Keystroke Biometric Scoring: The keystroke profiler was evaluated using multiple enrolment samples captured from the same user across different sessions.

- **Intra-user consistency:** Across 10 login attempts by the enrolled user, the average keystroke similarity score was 0.73, with a standard deviation of 0.09, confirming that the Gaussian profiler produces stable scores for natural variation in the enrolled user's typing rhythm.
- **Impostor rejection:** Attempts using a different typist's keystrokes for the same password produced an average score of 0.31, falling into the LOW trust tier and triggering step up MFA in all test cases.
- **Scoring latency:** The complete keystroke scoring pipeline, including baseline comparison and z-score computation, averaged 12ms, well within the acceptable threshold for interactive authentication.

2) Composite Trust Score Distribution: The blended trust score was evaluated across three usage scenarios:

- **Verified legitimate session:** (Enrolled user, enrolled device, low latency). Average composite trust score of 0.87, consistently selecting Tier 1 (STANDARD, AES-256-GCM) without MFA.
- **Recognised user, unknown device:** Average composite trust score of 0.58, selecting Tier 3 (MEMORY HARD) and applying PBKDF2 key derivation.
- **Credential only attack simulation:** (Correct password, different typist and device). Average composite trust score of 0.27, triggering Tier 5 (LOCKDOWN) with RSA-2048 key wrapping and mandatory step up MFA.

3) Adaptive Cryptographic Engine: All five cryptographic pairs were validated through the interactive encryption proof interface. Round trip correctness was maintained at 100%; all five pairs successfully completed encrypt then decrypt round trips with matching plaintext and verified authentication tags. Tampering with the ciphertext before decryption produced a MAC check failed error from the GCM authentication tag in all pairs, confirming strict integrity protection.

4) Hardware Fingerprint Matching: The hardware fingerprinting module was tested across distinct machines. The enrolled device consistently received a hardware match score of 1.0, with all 8 compared fields matching between enrolment and login. An unrecognised device with a different GPU renderer, screen resolution and CPU core count received a hardware match score of 0.38, contributing a 30% penalty to the composite trust score as designed.

B. Security vs. Usability Evaluation

The overall D.I.N.K.U. experience was assessed by measuring the impact of adaptive security measures on user workflow. Enrolled users on recognised devices consistently achieved composite trust scores above 0.85, enabling frictionless authentication with no MFA challenge in the majority of sessions. Legitimate users achieved trust scores below 0.50 (triggering MFA) in approximately 8% of sessions, primarily attributable to significant variation in typing speed due to fatigue. This demonstrates a highly effective balance where security friction is isolated exclusively to instances demonstrating genuine risk signals.

VII. CONCLUSION AND FUTURE WORK

A. Conclusion

The D.I.N.K.U. framework represents a meaningful advancement in authentication architecture, specifically designed to address the fundamental inadequacy of static credential only verification. By computing a real time composite trust score from keystroke biometrics, hardware fingerprinting and network latency at every login attempt, the system establishes a continuous behavioural identity signal that cannot be replicated by an attacker who has merely obtained a user's password.

A critical achievement of this project is the successful implementation of the five tier adaptive cryptographic engine. The system demonstrates that cryptographic algorithm selection can be driven dynamically by a runtime trust signal, escalating from AES-256-GCM for high trust sessions to RSA-2048 key wrapping for lockdown scenarios, with all five pairs producing verifiable, tamper evident ciphertext confirmed through interactive round trip proof.

Operationally, D.I.N.K.U. bridges the gap between high level security and user accessibility through its web based interactive dashboard, admin panel with Telegram based notification dispatch and persistent audit logging. The system proves that a unified, risk proportionate authentication platform is both technically feasible and deployable on consumer hardware without specialised cryptographic equipment.

B. Future Work

While the D.I.N.K.U. framework provides a robust foundation for adaptive behavioural authentication, several avenues exist for future research:

- **Trained Neural Model:** Training the Hybrid CNN-Transformer model on a labelled keystroke dynamics dataset to enable fully neural driven trust scoring, improving accuracy particularly in adversarial conditions.
- **True Post-Quantum Cryptography:** Integrating `liboqs-python` (Open Quantum Safe project) to implement Kyber-768 key encapsulation and Dilithium signature schemes [7], providing genuine post-quantum protection for the LOCKDOWN trust tier.
- **Continuous In-Session Scoring:** Extending the profiler to capture continuous typing patterns throughout the authenticated session, triggering real time trust score updates and automatic step up MFA if behaviour deviates significantly during an active session.
- **Federated Baseline Improvement:** Utilizing federated learning techniques to allow models to improve from aggregated, anonymised behavioural patterns across multiple deployments without sharing any raw user data.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

REFERENCES

[1] K. S. Killourhy and R. A. Maxion, "Comparing anomaly-detection algorithms for keystroke dynamics," in *2009 IEEE/IFIP International Conference on Dependable Systems & Networks*. IEEE, 2009, pp. 125–134.

[2] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser, and I. Polosukhin, "Attention is all you need," in *Advances in neural information processing systems*, vol. 30, 2017.

[3] W. Stallings, *Cryptography and network security: Principles and practice*. Pearson Education, 2022.

[4] D. Balfanz, A. Czeskis, J. Hodges, J. Jones, M. B. Jones, A. Kumar, A. Liao, R. Lindemann, and E. Lundberg, "Web authentication: An api for accessing public key credentials level 2," W3C, Tech. Rep., 2021.

[5] P. Eckersley, "How unique is your web browser?" in *International Symposium on Privacy Enhancing Technologies Symposium*. Springer, 2010, pp. 1–18.

[6] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *2012 IEEE Symposium on Security and Privacy*. IEEE, 2012, pp. 553–567.

[7] J. Delvaux and I. Verbauwhede, "Key recovery attacks on the latent variable cryptosystem," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2019.