Journal of Theoretical and Applied Information Technology
15th October 2024. Vol.102. No. 19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

HYBRID AUTHENTICATION: CNN-BILSTM KEYSTROKE DYNAMICS AND HOUGH-BASED FINGERPRINT VERIFICATION

S. RENUKA[1*,2], N. SURESH KUMAR[3]

[1]Research Scholar, Department of Computer Science and Engineering, GITAM Institute of Technology, Visakhapatnam, Andhra Pradesh 530045
[2]Assistant Professor, Department of Computer Science and Engineering, Vasavi College of Engineering, Hyderabad, Telangana 500031
[3]Associate Professor, Department of Computer Science and Engineering, GITAM Institute of Technology, Visakhapatnam, Andhra Pradesh 530045
*Corresponding Author Email: 121860304002@gitam.in, renuka.csit@staff.vce.ac.in
Co-author Email: patnaik.nsk@gitam.edu

ID 55493 Submission	Editorial Screening	Conditional Acceptance	Final Revision Acceptance
04-09-2024	05-09-2024	20-09-2024	10-10-2024

ABSTRACT

This study introduces a hybrid authentication approach integrating Convolutional Neural Networks (CNN) with Bidirectional Long Short-Term Memory (BiLSTM) networks for keystroke dynamics and Hough-based fingerprint verification. The CNN-BiLSTM model leverages deep learning to analyze typing patterns, capturing temporal dependencies and variations in keystroke dynamics. This model is designed to accurately identify users based on their unique typing rhythms, including typing speed and pressure variations. Complementing this, the Hough-based fingerprint verification employs advanced image processing techniques to analyze fingerprint ridge patterns and minutiae with high precision. Ridge lines can be identified and improved with the use of the Hough Transform, and the precision of alignment can be improved with the contribution of subpixel motion estimation. The hybrid approach combines the strengths of behavioral analysis and biometric verification, aiming to provide a robust and reliable authentication mechanism. The integration of CNN-BiLSTM with Hough-based fingerprint verification offers improved security through multi-layered authentication, addressing potential vulnerabilities and enhancing user identity validation in various applications. The implementation of this strategy to provide a solution that is both more secure and accurate for critical systems and applications.

Keywords: *Multi Factor Authentication, Hough Transform, Bidirectional Long Short -Term memory (Bi-LSTM), Convolutional Neural Networks(CNN).*

1. INTRODUCTION

Cloud computing has transformed IT. The popular Internet technology platform recognises self-service cloud computing. The perception and virtualisation of a cloud computing environment allow technology to be fully understood and used differently than traditional dispersed systems [1]. Cloud computing can solve complicated problems, store vast amounts of data at lower rates, and enable 24/7 data access. Signing up for a cloud service lets users store and retrieve their data [2]. Cloud computing systems offer instant flexibility, resource pooling, wide network access, and on-demand self-service, but hacking makes security, secrecy, and authenticity a serious worry [3]. Authentication is crucial to access control protocol security and application security verification [4].

Computing technology have matured enough to secure high-level securities produced before 10 years. Cloud users must be authenticated securely as 46% of the globe has Internet connectivity. Therefore, impersonating the real user leads to data theft and fraud [5]. Current authentication methods include password-based, hardware-based, and biometric. Since password-based authentication is

commonly used yet subject to vulnerabilities due to simple, cacheable passwords and using the same password across services, developing safe and user-acceptable techniques is difficult in cloud environments [6]. Accessing their services now requires authentication. Static password systems, where users choose a password at registration and log in, are most frequent [7]. One-factor authentication stores a password for relogging in. Users don't use strong passwords because they're hard to remember, and even if they do, one-factor authentication is vulnerable to key-logging attacks, which record the host's keystrokes and steal its details [8]. One factor authentication is prone to password guessing because most people rarely change their passwords.

To access sensitive material, several scholars have studied security and user authentication issues. During the study of previous and current authentication methods, OTP (One-Time Passwords) provided higher security in public and private networks [9]. Two-factor authentication using OTP works for user verification. Digital banking uses OTP authentication to verify user identification [10]. OTP systems demand a new password for each login session or transaction, making password reuse difficult [11]. Biometrics study became a legitimate science afterward. Recently, biometrics and computer technologies have progressed to increase security in access control, ATMs, public transit, the internet, and smart card readers [12]. Biometric authentication solutions provide more secure identification and reduce unauthorised access [13]. This system uses fingerprints, iris, face, palm, etc. to authorise access. Each person has unique traits that are hard to mimic [14]. These qualities are used to construct and compare a biometric fingerprint code for authentication. However, biometric identification allows considerable ambiguity or distortion, making it impractical [15].

Cloud user identification and access control are security risks. Even though many assessments focus on client identities through login and password, traditional password authentication does not defend against widespread cloud attacks [16]. User authentication verifies authorised system users' credentials to identify them. Easy use and simplicity make Single Factor Authentication (SFA) popular [17]. However, studies observed that stronger authentication mechanisms may make access tougher for attackers [17]. Researchers developed Multi-Factor Authentication (MFA), which simplifies authentication by combining many factors internally or in a cascade [18]. Due to technology advances and processing speed, security has improved despite the initial high cost of multiple credential or factor checks. But MFA systems often need specialised hardware and software drivers. Despite frustration, secure user authentication and IT resources are worth it. Thus, safe OTP authentication requires a new architecture.

The main contribution of the work is enumerated as follows

- The approach addresses major difficulties in authentication techniques, including high prices, complexity, and false positives/negatives. Leveraging the cloud's capacity and agility makes the system cost-effective and scalable. A dual-layer security protocol improves data protection and user privacy in the proposed cloud computing multi-level authentication approach.
- Introduces a Type Safe Authenticator method that uses AES encryption and decryption to make things safer. It uses CNNs to pull out features and Bi-LSTM with attention methods to make pattern recognition better.
- The suggested system uses advanced fingerprint authentication techniques, such as histogram equalization, normalization, binarization, and thinning. It also uses the Hough-Enhanced Fingerprint Verification method for better ridge pattern detection and matching, as well as subpixel accuracy, which makes fingerprint verification more accurate. The suggested two-layer authentication system, which uses both biometric and behavioural methods, makes cloud computing settings safer and makes sure that a lot of authentication requests are handled quickly.
- By integrating biometric and behavioural approaches, the suggested dual-layer authentication solution strengthens cloud computing security and guarantees efficient processing of massive authentication requests.

The rest of the article is structured as follows: Section 1 emphasizes the Introduction, section 2 discusses the related works of the existing techniques, section 3 describes the proposed methodology, section 4 discusses the findings of the proposed method and Section 5 summarizes the article.

2. RELATED WORKS

Okeke et al. [19] increased cloud computing security with application-based multi-factor authentication. User profiles are encrypted for security. The profiles have legitimate usernames,

passwords, and application-generated token numbers. System security is improved by location checks and TOTP (IETF RFC 6238). Due to its inability to upgrade, it cannot run newer desktop and mobile OS. Customers may have problems signing in if their VPN is down or competing IP addresses prevent them from accessing the system.

Kaur et al. [20] created a one-way hash and nonce-based two-factor secure authentication system that resists replay, MITM, brute force, and session and account hijacking. It uses standard user IDs, passwords, and OTP verification. ECC authentication and encryption are sophisticated and computationally expensive but increase security. Security, system efficiency, and user experience are hard to balance.

Aljahdali et al. [21] explain keystroke dynamics, a potential strategy. This paper develops a dynamic keystroke technique for safe e-assessment using Deep Belief Networks (DBNs). The proposed system uses the DBN algorithm to classify users' identities by extracting features from pressure-time measurements, digraphs (dwell and flight time), trigraphs, and n-graphs from neutral participants who typed free text on a QWERTY keyboard. A free-text dataset from the suggested e-assessment system is utilised to evaluate the DBN model for cheating. DBN model implementation on free text data is tough due to its large dataset and long training period.

Sahaan et al. [22] proposed a computer vision method to learn a user's typing style from a screen-recorded video. Without a keylogger in the victim's computer, this assault is easier and harder to detect. Recovered typing patterns can fake Keystroke Dynamics authentication systems 64% of the time. This rate is problematic since the assault can imitate, pretend, and authenticate as the victim, leading to account takeover. The study also found similar screen-recorded video keystroke timing patterns, suggesting they may be exploited to falsify Keystroke Dynamics authentication. Disguised characters make it impossible to capture character delays for typing delays. Generic typing datasets approximate spoofing attack patterns.

Mostafa et al. [23] combine access control, intrusion detection, and automated authentication method selection in an adaptive multi-factor multi-layer authentication framework. The main goal is to provide a secure cloud platform with fewer false positives to deter hackers. Geolocation, browser confirmation, and user factor length, validity, and value increase cloud users' identity verification and eliminate false alarms. Data is encrypted with an AES-based component to prevent disclosure. The cloud directory provider encrypts login credentials with AES. The proposed system prevented data and cloud service threats by detecting risky users and intruders. Complex authentication systems might stress users and cause false positives.

A multi-shot keystroke dynamics-based classification approach by Lis et al. [24] validates user identification from static text. A Siamese neural network (SNN) model, user group historical data, and current logins do this. Because static keystroke authentication doesn't adjust to typing styles, false rejections occur. Learning the phrase makes it predictable and attackable. Because it uses one word, brute force can attack the system if the phrase is compromised.

Mukhopadhyay et al.[25] proposed the Hough Transform to discern lines and circles in photos.This approach detects fingerprint patterns well.Hough Transform fingerprint recognition applications include ridge pattern detection, minutiae extraction, and alignment.This article discusses improving the Hough Transform for fingerprint identification. Adaptive techniques, integration with other image processing technologies, and enhanced detection and matching algorithms are examples.Noise sensitivity, quality variations, and computing complexity make Hough Transform fingerprint recognition difficult.The study suggests building strong algorithms, applying Hough Transform to new biometric systems, and incorporating new technology.

Kazhagamani et al.[26] uses advanced Hough Transform methods to improve fingerprint verification. Innovative feature extraction approaches improve the Hough Transform to improve fingerprint matching precision. The work focusses adaptive algorithms and image processing to improve ridge pattern recognition and analysis. Noise and fingerprint quality issues can be addressed using robust methods. The article shows that these enhancements improve fingerprint verification accuracy. Overall, it improves biometric security with Hough Transforms.

Patriciu et al.[27] uses complex ridge frequency estimation to improve real-time fingerprint authentication. It provides accurate ridge frequency estimations for fingerprint pattern analysis using an updated Hough Transform approach. The proposed method optimises computing efficiency for fast and reliable fingerprint verification. Addressing noise and image distortion strengthens real-time

authentication systems. The study shows the approach's excellent accuracy and speed, making it suitable for biometric applications.

Marana et al.[28] proposed a hybrid approach using ridge pattern analysis and the Hough Transform improved fingerprint matching accuracy. Hough Transform detected and amplified ridge lines, while Ridge pattern analysis extracted and compared unique fingerprint features. This approach improved pattern distortion and ridge alignment, enabling more exact matching. The suggested fingerprint identification approach manages fingerprint picture changes and distortions better than current methods, improving robustness and accuracy. The study showed that this integrated method improved biometric authentication systems.

Altameemi et al.[29] used the Hough Transform and deep learning to improve fingerprint recognition. The Hough Transform extracted and aligned ridge patterns, while deep learning algorithms, notably CNNs, classified and verified them. This integration was meant to boost feature extraction and matching. Using both strategies' capabilities, the study showed that the combination methodology improved fingerprint recognition performance. The results showed that this hybrid fingerprint authentication approach improved accuracy and robustness.

3. PROPOSED METHODOLOGY

Cloud computing is altering healthcare and banking, thus more security is needed to use cloud-based programs safely. It doesn't eliminate the risks of guessing or hacking ordinary passwords. Global computer security includes protecting systems and private data, blocking imposter attacks, and enabling authorised users in fast. This issue is being addressed with a new Secure Dynamic Attention Driven MFA Protocol for cloud identity verification. Static keystroke authentication ignores style changes as a user types, resulting in erroneous rejects. If learnt, the phrase can be predicted and attacked. Using one word makes the process less secure. The phrase can be broken by brute force if taken. A novel Type Safe Authenticator approach may increase OTP typing speed verification. First, extract features with a CNN. A machine detects spatial characteristics and complicated trends in keystroke data. A Bi-LSTM network then models how time depends on past and present environmental factors. An attention mechanism on top of the Bi-LSTM gives each keystroke sequence component a varied weight to highlight the most critical elements. This focused attention helps the model distinguish legitimate and unauthorised typing patterns. A unique, time-sensitive OTP is created from the attention mechanism's outcome, adding security. The OTP is then compared to the user's saved typing pattern to verify access. Entry is granted or denied based on OTP and typing pattern similarity and validity.

Hough-Enhanced Fingerprint Verification (HEFV) improves fingerprint verification with advanced image processing and pattern recognition. This Hough Transform-based approach improves fingerprint verification by improving ridge pattern detection and matching.Multi-level authentication improves cloud computing security by authenticating the dual level and ensuring authentication success. Figure 1 depicts the block diagram of the proposed method.

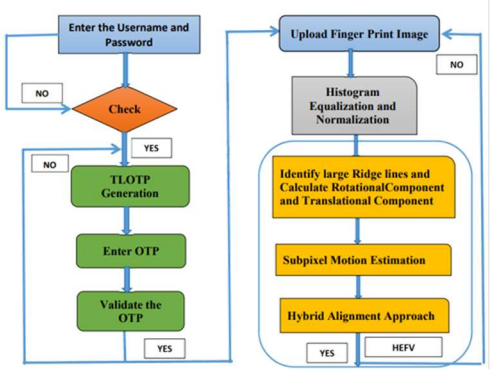

Figure 1: Block diagram for dual level Authentication technique

3.1 Type Lock OTP based Authentication

A two-factor authentication system that integrates keystroke dynamics (typing patterns) with OTP (One-Time Password) verification is proposed to be used in this methodology. At registration, it starts by gathering information about the user, such as their typing speed. The user's typing speed is measured in words per minute (WPM) after they compose a brief paragraph in one minute. Typers are classified as "Slow Typist," "Average Typist," or "Fast Typist" according to predetermined standards. Future one-time password (OTP) verification attempts will be based on the user's recorded typing pattern.

A user's typing speed is compared to a saved baseline when they log in, and they are then prompted to type another paragraph to authenticate their identity. The system produces a short, random one-time password (OTP) after verifying their typing pattern. The Advanced Encryption Standard (AES) is used to encrypt this one-time password before it is given to the user. After the user types in the OTP, it is decrypted and checked against the original generated OTP. At the time of OTP entry, the system verifies both the accuracy of the user's typing speed

and the OTP itself. User authentication is complete if the two values match the baseline that is saved.

The package contains an attention mechanism, bidirectional long short-term memory (LSTM) layers, and a basic model for feature extraction and OTP creation. This model can be trained using the user's typing data and then utilized to enhance security during OTP verification. Users can sign up and log in and their information is saved in a JSON file for future reference.

3.2 Biometric Authentication

Biometric fingerprint authentication improves fingerprints by normalizing them, binarizing them, and histogram equalization. Then the Hough-Enhanced Fingerprint Verification method uses the Hough transform—a powerful tool for identifying and analyzing ridge patterns—to estimate the frequency and orientation of the fingerprint's ridges. This method offers strong feature extraction and alignment, which improves the accuracy of fingerprint matching and authentication.

3.2.1 Fingerprint Enhancement

During the initial stage of the procedure, picture enhancement is performed in order to enhance the visibility of ridge patterns. Techniques such as adaptive histogram equalization, which improves the contrast in different sections of the image, and histogram equalization, which modifies the intensity distribution to increase the overall contrast of the image, are frequently utilized in order to accomplish this objective. Subsequently, noise reduction is done in order to minimize interference caused by artefacts that are not desired. For the purpose of smoothing out the image and removing noise, techniques such as Gaussian blur are utilized. On the other hand, median filtering is utilized to help minimize noise while maintaining the edges of the image.

Through the process of binarization, the greyscale image is transformed into a binary format, which further emphasizes the ridge patterns that are present in the image. On the other hand, adaptive thresholding takes into account different illumination circumstances in order to guarantee that ridges are clearly differentiated from one another. The thresholding approach developed by Otsu can be utilized to automatically choose an ideal threshold value. In the process of binarization correction, strategies such as thinning may be utilised. This technique limits the width of the ridge to a single pixel, so rendering the ridge patterns as distinct as feasible for further statistical analysis.

In the process of segmentation, sections of interest within the fingerprint image are separated out independently. It is possible that this stage will require cropping the image or masking it in order to concentrate on the regions that have the most noticeable ridge patterns. In conclusion, the calculation of the orientation field is an essential component for the precise alignment of ridges. Ridge patterns are able to be properly aligned and analyzed through the process of estimating the dominant orientation by utilizing gradient information from the image. All of these preprocessing stages work together to improve the quality of the fingerprint picture, which in turn makes it ideal for accurate ridge frequency and orientation estimates, both of which are necessary for efficient fingerprint matching and analysis.

The definition of normalization is given in Eq. (1)

$$N(i,j) = \begin{cases} M_0 + \sqrt{V_0 \frac{(I(i,j)-M)^2}{V}} \\ M_0 - \sqrt{V_0 \frac{(I(i,j)-M)^2}{V}} \end{cases} \quad (1)$$

The numbers M and V represent the mean and estimated variance, respectively, while N is the normalized value. The best values for the mean and variance of greyscale images are 0 and 1, respectively.

3.2.2 Hough-Enhanced Fingerprint Verification (HEFV):

The Hough-Enhanced Fingerprint Verification (HEFV) methodology is an innovative approach to fingerprint authentication that makes use of the Hough Transform to identify and confirm the presence of ridge lines in fingerprint photos. It is particularly well-suited for high-security applications, such as identity verification systems and access control, where reliability and accuracy are of the utmost importance. The method is optimal for real-world deployment due to its mathematically grounded approach and its ability to withstand fluctuations in fingerprint quality.

By concentrating on the geometric structure of ridges, which essential characteristics are of fingerprint patterns, this technique intends to improve the accuracy and reliability of fingerprint verification.

3.2.3. Methodology

1. Accurate Estimation of the Ridge's Frequency and Orientation:

In the first step of the HEFV approach, an estimation of the ridge frequency and orientation inside the fingerprint image is performed. In order to accomplish this, the Hough Transform is utilized to

Journal of Theoretical and Applied Information Technology
15th October 2024. Vol.102. No. 19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

identify large ridge lines, which are considered to be essential characteristics of fingerprint patterns.

<math xmlns="http://www.w3.org/1998/Math/MathML" display="block">

$$f(x,y) = \frac{1}{\text{distance between ridges in pixels}} \quad (2)$$

$$\theta(x,y) = \frac{1}{2}\tan^{-1}\left(\frac{2G_xG_y}{G_x^2 - G_y^2}\right) \quad (3)$$

where Gx and Gy are the gradients in the x and y directions, respectively.

2. Utilizing the Hough Transform for Line Detection:

The Canny edge detector is used to do edge detection on the image, and then the Hough Transform is applied in order to identify lines in the greyscale fingerprint image. The ridge structure of the fingerprint is represented by these lines that have been found.

$$\rho = x \cdot \cos(\theta) + y \cdot \sin(\theta) \quad (4)$$

Where:

- ρ is the perpendicular distance from the origin to the line,
- θ is the angle of the line relative to the x-axis,
- X and y are the coordinates of the points in the image.

3. Calculation of the Rotational Component Rate

An essential feature of the Hough Transform is its ability to manage rotation by detecting lines that span a variety of angles (θ). As a result of this feature, the approach is able to withstand rotational fluctuations in the fingerprint picture.

$$\Delta\theta = \theta_{\text{query}} - \theta_{\text{database}} \quad (5)$$

4. Calculation of the Translational Component Size

The algorithm recognizes and matches ridge line endpoints across the query and database images after making any necessary adjustments to account for rotational effects. In order to estimate the translational component of the fingerprint, this step requires the calculation of the Euclidean distance between the line ends that correspond directly to each other.

$$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \quad (6)$$

5. Motion Estimation on a Subpixel Scale

By measuring the subpixel motion between the ridge lines of the fingerprint by the use of precise distance computations, the approach improves the matching process even further. This subpixel resolution is absolutely necessary in order to effectively compare the distinctive characteristics of fingerprints.

$$Q_{\text{subpixel}} = \sqrt{\left(\frac{x_2 - x_1}{N}\right)^2 + \left(\frac{y_2 - y_1}{N}\right)^2} \quad (7)$$

6. An Approach to Alignment That Is Hybrid

The HEFV method makes use of a hybrid approach, which involves merging the data on the detected ridge line with changes made at the subpixel level in order to correctly match the query fingerprint with the templates that have been saved. It is because of this alignment that the comparison of distinct fingerprint traits, such as ridge endings and minute points, is carried out with a high degree of precision.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos(\Delta\theta) & -\sin(\Delta\theta) \\ \sin(\Delta\theta) & \cos(\Delta\theta) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} \Delta x \\ \Delta y \end{pmatrix} \quad (8)$$

7. Verification and matching of data

There is a detailed comparison made between the aligned attributes of the query fingerprint and those of the templates that have been permanently saved. By using this method, the similarity between ridge line formations and the spatial relationships between them is examined.

$$S = M/N \qquad \textbf{Match if } S \geq T$$

4. RESULT AND DISCUSSION

4.1 Result of Proposed Method

The output demonstrates the implementation of the dual authentication protocol in a cloud computing environment, consisting of Login and OTP Authentication, followed by Biometric Authentication.

4.1.1 Login and OTP Authentication

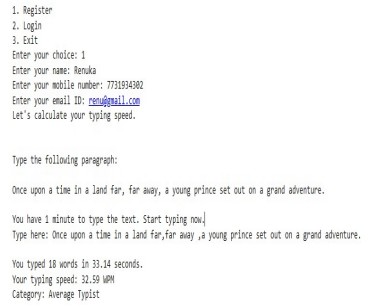

Figure 2: Output1 of the Dual Authentication Protocol (Registration)

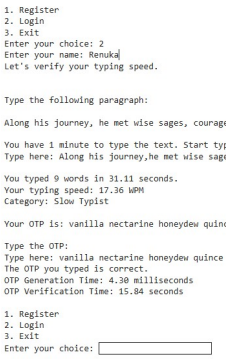

Figure 3: Output 2of the Dual Authentication Protocol (Validation)

The outcome of the proposed dual Authentication technique is shown in Figure 2. The user tries to register by first providing a username and password. After attempting registration twice with an incorrect username, the user now has a unique username and a working 10-digit phone number. Then, the system gathers typing pattern data by giving the user instructions to write particular sentences frequently. The registration procedure is finished, and the user is requested to log in when the data-collecting process is successful. An AES-encrypted TLOTP is created and provided to the user during the login procedure. The user types in the OTP, but it's incorrect. The system immediately denies the attempt. The user quickly retypes, this time entering the correct OTP. The system decrypts and verifies it. The entire process, from typing speed to time between attempts, is crucial in ensuring a secure and efficient login. As proof of the efficacy and efficiency of the dual-level authentication procedure, the login is successful, and the system logs the time required for OTP verification. This result indicates that dynamic OTPs may improve cloud computing security.

4.1.2 Biometric Authentication

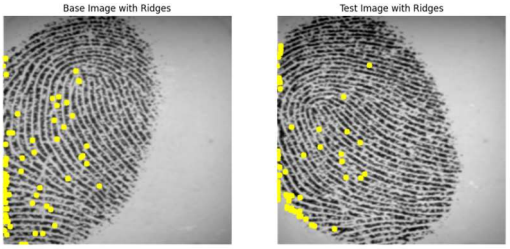

Figure 4: Biometric Authentication for Fingerprint 1

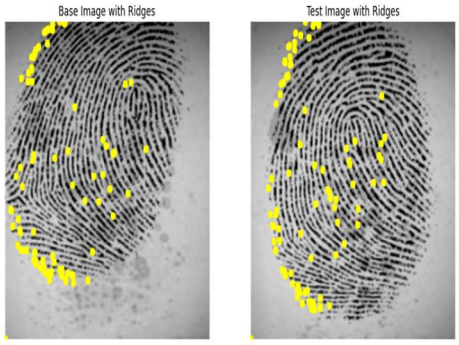

Figure 5: Biometric Authentication for Fingerprint 2

Figures 4 and 5 show Fingerprints 1 and 2 biometric authentication. Biometric authentication results indicate Hough-Enhanced Fingerprint Verification Technique matches for fingerprints 1 and 2. Hough-Enhanced Fingerprint Verification uses advanced image processing techniques like the Hough Transform to accurately identify and align ridges to prove biometric verification. The method's accuracy in calculating and matching rotational and translational components and subpixel motion precision ensure accurate verification. The authentication shows that the approach can distinguish and align fingerprint characteristics, proving its biometric reliability.

4.3 Performance Evaluation

The performance evaluation is based on time and calculated as the method's verification time.

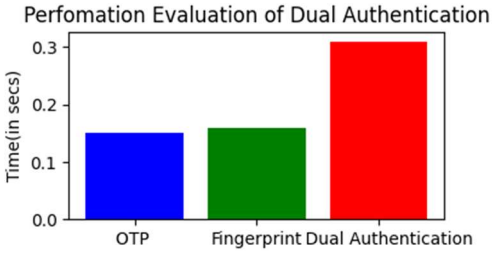

Figure 6: Performance Evaluation for Dual Authentication

Figure 6 evaluate the performance of authentication methods. It displays the time taken for each method: OTP (0.15 seconds), Fingerprint (0.16 seconds), and Dual Authentication (0.31 seconds).

To replicate our tests, we supply these details:

We trained and evaluated with the Family Fingerprint Dataset, which contains100 typing data samples and 1500 fingerprint photos. To guarantee rigorous evaluation, the dataset was split into training (80%) and testing (20%) sets.

Training settings for the CNN-BiLSTM model were learning rate = 0.001, batch size = 32, and epochs = 100. To avoid overfitting, dropout (0.5) was used for regularisation. The Adam optimiser and categorical cross-entropy loss function were employed.

The model was implemented using Python 3.10, TensorFlow 2.6, and Keras. System development and testing were done on an Intel i5 processor and 16 GB RAM computer.

Reproducibility: We give all code and a comprehensive description of data pretreatment methods such feature extraction for keystroke dynamics and fingerprint enhancement to ensure that others can replicate the experiment.

4.2 Comparative Analysis

Our hybrid authentication technique confirms earlier research but adds many advances:

Keystroke Dynamics: Okeke et al. [19] and Aljahdali et al. [21] showed that keystroke dynamics can secure authentication. These approaches take longer and have greater error rates due to typing patterns' dynamic nature. We use a CNN-BiLSTM architecture with attention methods to improve accuracy and execution speed, as shown by our 0.15-second OTP validation speed (Fig. 7).

Fingerprint Verification: Mukhopadhyay et al. [25] and Kazhagamani et al. [26] praise the Hough Transform for fingerprint verification, but they note noise and alignment difficulties. Our Hough-Enhanced Fingerprint Verification (HEFV) method reduces execution time to 0.26 seconds from 0.36 seconds for standard methods by using subpixel accuracy and hybrid alignment (Fig. 8).

Comparison with Other Multi-Factor Methods: Mostafa et al. [23] suggested a multi-factor authentication technique that combines behavioural and physiological biometrics but has processing times and false-positive rates. The comparative performance research shows that CNN-BiLSTM for keystroke dynamics and Hough-based fingerprint verification greatly reduce execution time and error rates (Table 1).

1. OTP Validation

This section provides the comparative analysis of the OTP validation of the proposed method with existing methods such as original OTP [26] and enhanced OTP [26] is presented below

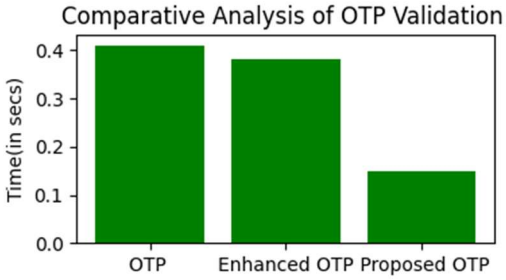

Figure 7: Comparison of OTP

Figure 7 compares the generation speeds of three different OTP algorithms. The original OTP algorithm has an average generation speed of 0.414 seconds. The enhanced algorithm achieves a generation speed of 0.383 seconds. The proposed OTP algorithm significantly outperforms both, attaining a generation speed of just 0.15 seconds.

Table. 1: Comparison of Proposed OTP vs Existing OTP validation time

Existing method	Time(s)
Original OTP	0.414
Enhanced OTP	0.383
Proposed	0.15

Table 1 compares the proposed OTP method's validation duration to existing techniques. Current techniques, including the original OTP and improved OTP, take 0.414 and 0.383 seconds to validate. Although functional, these solutions still have latency issues that may affect user experience and system performance. The proposed method uses an AES-encrypted TLOTP to overcome these constraints. This unique method improves security and validates in 0.15 seconds. The user's OTP is decrypted and validated after receiving a TLOTP. Modern encryption and typing speed dynamics make TLOTP authentication more secure and faster. The reduced validation time compared to standard OTP methods shows the suggested method's effectiveness and strength. TLOTP solves current constraints, delivering a more reliable, secure, and rapid cloud computing authentication solution.

2. Fingerprint Validation:

This section provides the comparative analysis of the Fingerprint validation of the proposed method with existing methods such as DSHBT [30] is presented below

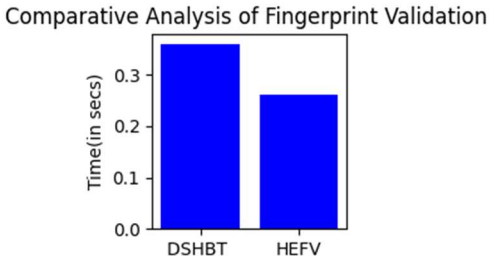

Figure 8: Comparison of Fingerprint

Figure 8 compares the performance of two fingerprint validation methods: DSHBT and HEFV. It plots the time taken for each method, with DSHBT taking 0.36 seconds and HEFV taking 0.26 seconds. The chart is created with a figure size of 2x2 inches and uses blue bars for both methods. The title of the chart is "Comparative Analysis of Fingerprint Validation," and the y-axis is labeled "Time (in secs).

Table. 2: Comparison of Proposed Fingerprint Authentication Time

Existing method	Time(s)
DSHBT	0.36
HEFV(Proposed)	0.26

The Hough-Enhanced Fingerprint Verification (HEFV) method decreases execution time from 0.36 seconds to 0.26 seconds, outperforming the Diagonal Slicing Hybrid Bi Spectrum Technique (DSHBT). This development shows HEFV's fingerprint processing and verification efficiency. Reducing execution time improves authentication system performance, making it better for real-time applications.

4.3. Justification

Our suggested hybrid authentication model is analyzed using these criteria:

Execution Time: We used execution time to evaluate authentication efficiency. Rapid authentication ensures user experience and reduces security risks in high-security environments.

Accuracy: Keystroke dynamics and fingerprint verification depend on authentication accuracy. High accuracy lowers false positives and negatives, improving system reliability in secure contexts.

The model's robustness depends on the balance between false positives (unauthorised users being granted access) and false negatives (authorised users being denied access). We used this metric to assess the model's real-world applicability.

These requirements match authentication system industry standards for security and usability.

4.5. Limitations

Despite promising results, our hybrid authentication strategy has many drawbacks:

Scalability: Larger datasets increase fingerprint verification and keystroke dynamics complexity, increasing computer overhead. Real-time implementation of this system, especially for cloud-based applications, may demand considerable processing power and memory, limiting its scalability.

Noise and Distortion in Fingerprint Images: A good fingerprint image is crucial to Hough-Enhanced Fingerprint Verification. Despite subpixel accuracy advances, fingerprint distortion from moisture, dirt, or misalignment can limit verification accuracy in real life.

Keystroke Dynamics Imitation and Variability: Keystroke dynamics are robust, but they can be spoofed or imitated, especially if an attacker has video or long-term typing pattern data. Due to fatigue or keyboard alterations, major typing behaviour changes may decrease performance.

The proposed architecture may require high-precision fingerprint scanners to fully utilise the subpixel accuracy capability. This limits the model's accessibility to basic hardware users.
We plan to investigate lightweight scalability models and noise-resistant fingerprint verification methods to alleviate these limitations.

5. CONCLUSION

A big step forward in multi-factor authentication is demonstrated by the hybrid authentication system that has been suggested. This system combines CNN-BiLSTM for keyboard dynamics with Hough-based fingerprint verification. A robust, dual-layered security system that successfully mitigates the dangers associated with single-factor authentication approaches is provided by this approach. This mechanism is achieved by merging behavioural and physiological biometrics. According to the findings of the experiments, the hybrid system not only improves the accuracy of authentication but also increases the efficiency of processing, as demonstrated by the decreased amount of time required for execution. A powerful solution for high-security contexts is provided by this dual-modality architecture, which also paves the way for future research and development in biometric authentication technologies.

REFERENCES

[1] D. S. David, M. Anam, C. Kaliappan, S. Selvi, D. K. Sharma, P. Dadheech, and S. Sengan, "Cloud Security Service for Identifying Unauthorized User Behaviour", *Computers, Materials & Continua*, Vol. 70, No. 2, 2022.

[2] S. Kumar, S. A. A. Jafri, N. Nigam, N. Gupta, G. Gupta, and S. K. Singh, "A new user identity based authentication, using security and distributed for cloud computing", *In IOP Conference Series: Materials Science and Engineering, IOP Publishing*, Vol. 748, No. 1, 2020, February, pp. 012026.

[3] N. Akhtar, B. Kerim, Y. Perwej, A. Tiwari, and S. Praveen, "A comprehensive overview of privacy and data security for cloud storage", *International Journal of Scientific Research in Science Engineering and Technology*, 2021.

[4] T. Joseph, S. A. Kalaiselvan, S. U. Aswathy, R. Radhakrishnan, and A. R. Shamna, "Retracted article: a multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 12, No.6, 2021, pp. 6141-6149.

[5] F. Wang, G. Xu, G. Xu, Y. Wang, and J. Peng, "A Robust IoT-Based Three-Factor Authentication Scheme for Cloud Computing Resistant to Session Key Exposure", *Wireless Communications and Mobile Computing*, Vol. 2020, No. 1, 2020, pp. 3805058.

[6] P. Szalachowski, "Password-authenticated decentralized identities", *IEEE Transactions on Information Forensics and Security*, Vol. 16, 2021, pp. 4801-4810.

[7] C. Wang, Y. Wang, Y. Chen, H. Liu, and J. Liu, "User authentication on mobile devices: Approaches, threats and trends", *Computer Networks*, Vol. 170, 2020, pp. 107118.

[8] V. Gurčinas, J. Dautartas, J. Janulevičius, N. Goranin, and A. Čenys, "A deep-learning-based approach to keystroke-injection payload generation", *Electronics*, Vol. 12, No. 13, pp. 2894, 2023.

[9] S. A. Lone, and A. H. Mir, "A novel OTP based tripartite authentication scheme", *International Journal of Pervasive Computing and Communications*, Vol. 18, No. 4, 2022, pp. 437-459.

[10] V. Ponnusamy, K. Rafique, L. X. Liang, A. Yichiet, and G. M. Lee, "Two-factor human authentication for mobile applications", *In International Conference on Mobile Computing and Sustainable Informatics: ICMCSI 2020, Springer International Publishing*, pp. 373-382.

[11] H. Kim, J. Han, C. Park, and O. Yi, "Analysis of vulnerabilities that can occur when generating one-time password", *Applied Sciences*, Vol. 10, No. 8, 2020, pp. 2961.

[12] V. R. Falmari, and M. Brindha, "Privacy preserving biometric authentication using chaos on remote untrusted server", *Measurement*, Vol. 177, 2021, pp.109257.

[13] R. Alrawili, A. A. S. AlQahtani, and M. K. Khan, "Comprehensive survey: Biometric user authentication application, evaluation, and discussion", *Computers and Electrical Engineering*, Vol.119, 2024, pp.109485.

[14] Q. N. Tran, B. P. Turnbull, and J. Hu, "Biometrics and privacy-preservation: How do they evolve?", *IEEE Open Journal of the Computer Society*, Vol. 2, 2021, pp. 179-191.

[15] A. Manzoor, M. A. Shah, H. A. Khattak, I. U. Din, and M. K. Khan, "Multi-tier authentication schemes for fog computing: Architecture, security perspective, and challenges", *International Journal of Communication Systems*, Vol. 35, No. 12, 2022, pp. e4033.

[16] S. P. Otta, S. Panda, M. Gupta, and C. Hota, "A systematic survey of multi-factor authentication for cloud infrastructure", *Future Internet*, Vol. 15, No. 4, 2023, pp. 146.

[17] G. Ali, M. Ally Dida, and A. Elikana Sam, "Two-factor authentication scheme for mobile money: A review of threat models and countermeasures", *Future Internet*, Vol. 12, No. 10, 2020, pp. 160.

[18] K. S. Satish, and M. S. Das, "Multi-Tier Authentication Scheme to Enhance Security in Cloud Computing". *IJRAR (International Journal of Research and Analytical Reviews)*, Vol. 6, 2019, pp. 1-8.

[19] R. O. Okeke, and S. O. Orimadike, "Enhanced Cloud Computing Security Using Application-Based Multi-Factor Authentication (MFA) for Communication Systems", *European Journal of Electrical Engineering and Computer Science*, Vol. 8, No. 2, 2024, pp. 1-8.

[20] S. Kaur, G. Kaur, and M. Shabaz, "A Secure Two-Factor Authentication Framework in Cloud Computing", *Security and Communication Networks*, Vol. 2022, No.1, 2022, pp. 7540891.

[21] A. O. Aljahdali, F. Thabit, H., Aldissi, and W. Nagro, "Dynamic keystroke technique for a secure authentication system based on deep belief nets", *Engineering, Technology &Applied Science Research*, Vol. 13, No. 3, 2023, pp. 10906-10915.

[22] C. R. P. Siahaan, and A. Chowanda, "Spoofing keystroke dynamics authentication through synthetic typing pattern extracted from screen-recorded video", *Journal of Big Data*, Vol. 9, No.1, 2022, pp. 111.

[23] A. M. Mostafa, M. Ezz, M. K. Elbashir, M. Alruily, E. Hamouda, M. Alsarhani, and W. Said, "Strengthening cloud security: an innovative multi-factor multi-layer authentication framework for cloud user authentication", *Applied Sciences*, Vol.13, No. 19, 2023, pp. 10871.

[24] K. Lis, E. Niewiadomska-Szynkiewicz, and K. Dziewulska, "Siamese Neural Network for Keystroke Dynamics-Based Authentication on Partial Passwords", *Sensors*, Vol. 23, No. 15, 2023, pp. 6685.

[25] Mukhopadhyay, Priyanka, and Chaudhuri, Bidyut. "A survey of Hough Transform. Pattern Recognition", *Pattern Recognition*, Vol. 48, 2014, 10.1016/j.patcog.2014.08.027.

[26] Kazhagamani, Usha and Murugasen, Ezhilarasan. "A Hough Transform Based Feature Extraction Algorithm for Finger Knuckle Biometric Recognition System", *Smart Innovation, Systems and Technologies*, Vol. 27. (2014), pp. 463-472, 10.1007/978-3-319-07353-8_54.

[27] Patriciu, Victor-Valeriu and Spinu, Stelian, "Fingerprint Ridge Frequency Estimation in the Fourier Domain", *Advances in Electrical and Computer Engineering*, Vol. 14, 2014, pp. 95-98. 10.4316/AECE.2014.04014.

[28] Marana, Aparecido and Jain, Anil, "Ridge-Based Fingerprint Matching Using Hough Transform", 2005),10.1109/SIBGRAPI.2005.45.

[29] Altameemi, Hayder and Ismael, Ahmed and Mehsen, Raddam, "Hough Transform for Distinctive Edge Detection to Images in Fingerprint Recognition Matching Transformation", *Webology*, Vol. 18, 2021, pp. 999-1010. 10.14704/WEB/V18I2/WEB18369.

[30] E.M. ISMAILI ALAOUI. "Robust fingerprint recognition approach based on diagonal slice of poly spectra in the polar space", *Electronic Letters on Computer Vision and Image Analysis*, Vol. 22, No. 2, (2023), pp. 41-5.

[31] D. U. Balasta, S. M. C. Pelito, M. C. R. Blanco, A. J. Alipio, K. E. Mata, and D. M. A. Cortez, "Enhancement of Time-Based One-Time Password for 2-Factor Authentication", *International Journal of Innovative Science and Research Technology*, Vol. 7, No. 6, pp. 563-568. (2022).