AI-Driven Secure Network Authentication With Spatial Trust Validation

Preethi K[1], Srinithi S[2], Subavarshini S[3], Mrs.S.Sandhiya[4]
[1, 2, 3] Dept of Electronics and Communication Engineering,
[4]Assist prof, Dept of Electronics and Communication Engineering,
[1, 2, 3, 4] Kongunadu College of Engineering and Technology, Tholurpatti, India

Abstract- *This paper presents an AI-Driven Secure Network Authentication System with Spatial Trust Validation to enhance traditional login security using machine learning and Generative AI techniques. During registration, the system stores baseline authentication features including IP address and geolocation along with user credentials. During login, real-time IP and location data are compared with stored values to detect anomalies.An Intrusion Detection System based on the XGBoost algorithm analyzes behavioral features such as login frequency, IP deviation, geolocation variance, and failed attempts to classify access requests and generate a dynamic risk score. Suspicious activities trigger instant email alerts and are logged for analysis. Additionally, a Generative AI module provides adaptive security recommendations. The system establishes a smart and self-learning cyber security framework suitable for modern web applications.The integration of spatial validation with behavioral analysis significantly reduces unauthorized access risks. The proposed framework supports real-time monitoring and dynamic decision-making to strengthen overall network security. Experimental evaluation demonstrates improved detection accuracy and reduced false positives compared to conventional authentication systems.*

Keywords: AI-Driven Authentication, Secure Network Access, Spatial Trust Validation, Intrusion Detection System (IDS), XGBoost Algorithm, Behavioral Authentication, Geolocation Verification, IP Address Monitoring, Risk Scoring, Generative AI, Anomaly Detection, Real-Time Security Alerts, Cybersecurity Dashboard, Adaptive Security Framework.

I. INTRODUCTION

AI-Driven Secure Network Authentication with Spatial Trust Validation aims to provide a comprehensive, adaptive, and intelligent framework for securing network access with minimal unauthorized intrusion and maximum trust transparency. The system is designed to overcome the limitations of traditional authentication mechanisms that rely solely on static credentials such as usernames and passwords, which are highly vulnerable to credential theft, phishing, IP spoofing, and location-masking attacks.

The proposed system enhances security by integrating behavioral analytics, spatial trust validation, and machine learning-based intrusion detection into a unified framework. During user registration, baseline parameters such as IP address, geolocation, login frequency, and device characteristics are securely recorded. These parameters form a dynamic trust profile unique to each user. During login attempts, the system continuously compares real-time access information with the established baseline to evaluate trustworthiness.

By incorporating spatial trust validation, the system verifies whether the login location and IP address align with historical patterns. Any significant deviation, such as unusual geographic access or abnormal login behavior, triggers intelligent risk assessment mechanisms. This ensures that authentication is not solely dependent on correct credentials but also on contextual and behavioral consistency.

Overall, the system strengthens cybersecurity posture, enhances user trust, and provides a scalable solution suitable for modern web applications and enterprise environments operating in increasingly complex digital ecosystems.

The primary contributions of this work are summarized as follows: (1) Integration of Behavioral Analytics with Spatial Trust Validation : The system combines user behavior monitoring with real-time geolocation and IP verification to create a multi-dimensional authentication framework. (2) Machine Learning-Based Intrusion Detection:A predictive intrusion detection module using the XGBoost algorithm classifies login attempts based on behavioral and spatial deviations.

(3) Dynamic Risk-Based Authentication Mechanism:The framework evaluates login risk in real time and initiates additional verification procedures when anomalies are detected. (4) Generative AI-Based Security Recommendation Engine:The system provides intelligent,

context-aware preventive measures and adaptive security strategies upon identifying suspicious activities. (5) Automated Alert and Continuous Monitoring System:Suspicious login attempts trigger real-time alert and logging mechanisms, enabling proactive threat mitigation and administrative intervention.

II. LITERATURE SURVEY

Recent research in authentication systems highlights the transition from traditional credential-based security to intelligent, adaptive, and context-aware frameworks. With the rapid growth of satellite, wireless, IoT, and multimedia networks, researchers have focused on integrating physical-layer characteristics, biometrics, and AI-driven models to enhance authentication reliability.

Rui et al. [1] proposed a spatial channel-based authentication scheme for LEO satellites, utilizing channel impulse responses to generate unique spatial fingerprints for secure access. Dharmalingam and Tirumala [2] introduced a room-level voice authentication system using deep learning–based acoustic features to ensure scalable and privacy-preserving smart device security.Kalpana et al.

[3] developed a multimodal biometric authentication framework combining face, iris, and fingerprint recognition using Faster R-CNN, improving robustness against spoofing.Mahesh et al. [4] explored graphical password-based authentication to enhance usability and resistance to brute-force attacks.

Demirci et al. [5] applied deep learning to physical-layer authentication in XL-MIMO systems, generating transmitter fingerprints from channel state information. Li et al. [6] proposed a secure authentication and scheduling framework for 5G-enabled emergency vehicle systems, integrating contextual and cryptographic verification.Venkatraman et al. [7] introduced CNN-based video steganography for multi-factor authentication in multimedia environments.

Chen and Huang [8] developed an adaptive authentication architecture for the Beidou satellite network to ensure secure communication under dynamic conditions.Goki et al. [9] utilized Rayleigh backscattering fingerprints for optical network authentication, detecting unauthorized modifications. Xiao et al. [10] proposed an RF-based UAV identification framework using machine learning for real-time unauthorized access detection.

Overall, these studies demonstrate the effectiveness of spatial, biometric, and AI-driven authentication approaches. However, most existing solutions focus on domain-specific applications.

There remains a need for a unified authentication framework that integrates behavioral analytics, spatial trust validation, and machine learning–based intrusion detection for secure and adaptive network access, which the proposed work aims to address.

III. METHODOLOGY

A. System Architecture and Setup

The proposed AI-Driven Secure Network Authentication System is designed to provide dynamic and context-aware access control through behavioral analytics and spatial trust validation. The overall workflow of the system consists of user registration, baseline profile generation, real-time login monitoring, machine learning-based intrusion detection, and alert generation.

During the registration phase, user credentials along with contextual parameters such as IP address, geolocation, device information, and login time are securely captured and stored. These attributes form the baseline trust profile of the user. During login attempts, real-time access parameters are collected and compared against the stored baseline to evaluate authenticity and trustworthiness.

The system is implemented using a web-based interface integrated with a backend database and a machine learning module. Experimental evaluation is conducted by simulating both legitimate and malicious login attempts, including IP spoofing, location changes, repeated failed logins, and abnormal access frequency, to validate detection accuracy.

B. Data Acquisition and Profile Creation

The data acquisition module is responsible for collecting authentication-related parameters during both registration and login phases. Key attributes include: IP address, Geolocation (latitude and longitude), Device/browser information, Login timestamp, Login frequency.

During registration, these parameters are stored as a baseline authentication profile. Over time, the system updates the behavioral profile dynamically to reflect legitimate usage patterns. This adaptive profile formation enables continuous trust evaluation rather than static credential validation.

C. Feature Engineering

Relevant behavioral and spatial features including login frequency, IP deviation, geolocation variance, device changes, and failed login attempts are extracted and converted into structured inputs for analysis. These features represent the user's behavioral pattern over time.

D. Spatial Trust Validation

Spatial trust validation evaluates whether the current login attempt originates from a trusted geographical and network location. The system computes the distance between historical login coordinates and the current login location. Significant deviations beyond predefined thresholds trigger risk evaluation mechanisms.

IP address consistency is also verified to detect spoofing or unauthorized remote access. By combining geolocation deviation and IP analysis, the system establishes a spatial trust score that reflects contextual legitimacy.

E. Machine Learning-Based Intrusion Detection

The intrusion detection module is powered by the XGBoost algorithm. This supervised learning model classifies login attempts as legitimate or suspicious based on extracted behavioral and spatial features.

The training dataset consists of labeled login sessions categorized as normal or malicious. The model learns complex relationships between features such as IP deviation, login frequency, and device inconsistency.

During real-time authentication, the trained model generates a prediction score indicating the likelihood of unauthorized access.Performance metrics such as accuracy, precision, recall, and F1-score are used to evaluate the effectiveness of the classification model.

F. Risk Score Computation

A composite risk score is generated by combining machine learning prediction probability, spatial trust score, and behavioral similarity index. If the risk exceeds a predefined threshold, additional verification or access denial is triggered.A composite risk score is then generated by combining: Machine learning prediction probability, Spatial trust score, Behavioral similarity index. If the overall risk score exceeds a predefined threshold, the login attempt is marked as suspicious and subjected to additional verification or denial.

G. Adaptive Learning

The system incorporates an adaptive learning mechanism that updates user profiles based on confirmed legitimate activities. This prevents false alarms when users travel or change devices.

A generative AI-based recommendation engine provides context-aware security suggestions when suspicious activity is detected. These may include enabling multi-factor authentication, resetting passwords, or temporarily locking the account. This module transforms the system from reactive detection to proactive security guidance.

H. Alert Generation and Logging

The alert generation module is responsible for real-time notification and activity logging. When suspicious login behavior is detected, the system: Sends an automated email or dashboard alert to the administrator , Logs details such as username, IP address, location, timestamp, and risk score Records classification output for audit purposes

All authentication events are securely stored to maintain integrity and support forensic analysis. Real-time alerts enable immediate administrative intervention, while comprehensive logging ensures accountability and transparency in access control management.

Suspicious login attempts generate real-time alerts to administrators and are securely logged with details such as IP address, location, timestamp, and risk score. This ensures proactive monitoring and accountability.

4. EXISTING SYSTEM

Most existing authentication systems primarily rely on static credentials such as usernames and passwords or basic two-factor authentication (2FA) mechanisms. While these approaches are simple to implement and user-friendly, they remain vulnerable to modern cyber threats including phishing, credential stuffing, brute-force attacks, and password reuse exploits.

Biometric-only and One-Time Password (OTP)-based systems improve identity verification but can still be compromised through spoofing techniques, social engineering, SIM swapping, or device theft. These methods often operate as isolated verification layers without incorporating intelligent contextual validation.

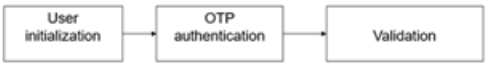

Figure 1. Block Diagram of exisiting system

Many traditional authentication frameworks do not consider dynamic parameters such as user location, IP address consistency, device trust level, login behavior, or temporal access patterns. The absence of AI-driven adaptive learning limits their ability to detect anomalies in real time or respond proactively to emerging threats.

As a result, conventional authentication systems continue to exhibit security gaps, limited scalability, and increased false acceptance or rejection rates in today's rapidly evolving digital environment.

V. PROPOSED SYSTEM

The proposed AI-Driven Secure Network Authentication System with Spatial Trust Validation enhances traditional credential-based authentication by integrating behavioral analytics, spatial verification, machine learning–based intrusion detection, and generative AI recommendations. Unlike conventional systems that rely only on usernames and passwords, the framework provides multi-layered, context-aware security for dynamic trust evaluation.

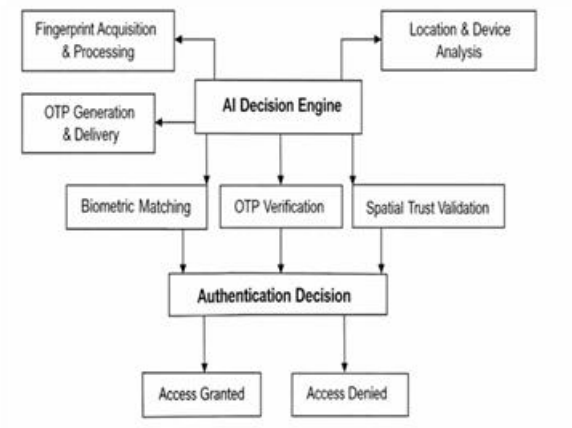

Figure 2. Block Diagram of proposed system

During user registration, credentials along with contextual parameters such as IP address, geolocation, device information, and login time are captured to create a baseline trust profile. During login, the system verifies credentials while simultaneously comparing current spatial and behavioral attributes with stored historical data.

A **Spatial Trust Validation Module** evaluates IP and location consistency, while the **Behavioral Analytics Module** monitors login frequency, failed attempts, and device changes. These features are analyzed using the XGBoost model, which assigns a real-time risk score and classifieslogin attempts as legitimate or suspicious.If the risk score exceeds a predefined threshold, automated responses such as access restriction, additional verification, and administrative alerts are triggered. A generative AI module further provides adaptive security recommendations based on detected anomalies.

Figure 3. Block Diagram of AI-Based Authentication System

Figure 4. Authentication Process Diagram

All authentication activities and alerts are displayed through a centralized dashboard for proactive monitoring. By combining spatial trust validation, behavioral analysis, and AI-driven detection, the system delivers a scalable, intelligent, and adaptive authentication framework suitable for modern enterprise and web environments.

VI. RESULTS AND DISCUSSION

The implementation of the proposed AI-Driven Secure Network Authentication System with Spatial Trust Validation demonstrated enhanced security performance compared to traditional credential-based mechanisms. During evaluation, the system accurately distinguished between legitimate and suspicious login attempts by analyzing

behavioral patterns and spatial parameters alongside user credentials. Login attempts from unfamiliar locations, unknown devices, or abnormal time patterns were detected in real time and assigned elevated risk scores.

The intrusion detection module powered by the XGBoost effectively classified anomalous activities such as repeated failed attempts and unusual login frequency with high accuracy. Automated alerts and logging ensured timely administrative intervention, while the generative AI module provided adaptive security recommendations to mitigate identified risks. The centralized dashboard further enhanced situational awareness by visualizing login trends, risk levels, and alert history.

The centralized dashboard enabled administrators to visualize system activity comprehensively, offering insights into login trends, risk distributions, and alert histories. This visualization facilitated proactive monitoring, enabling rapid response to anomalous behavior.

In scenarios simulating advanced intrusion attempts, the system demonstrated resilience by combining contextual verification, anomaly detection, and AI-guided recommendations, reducing the probability of unauthorized access.

The intrusion detection module, powered by the XGBoost algorithm, proved effective in classifying activities with high accuracy, dynamically generating risk scores that allowed prioritization of potential threats. Suspicious behaviors, such as repeated failed login attempts or deviations from typical login times, were successfully flagged, resulting in timely interventions. The generative AI recommendation engine further enhanced system responsiveness by providing adaptive security guidance tailored to detected patterns, ensuring that preventive measures were applied consistently and appropriately.

Figure 5. User Interface Dashboard

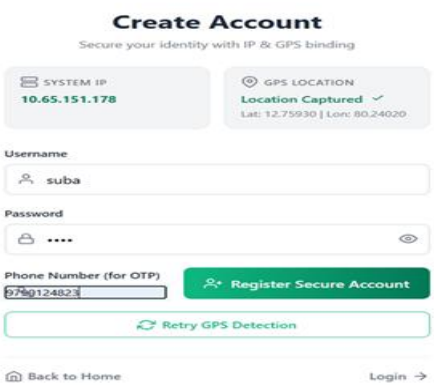

Figure 6. User Registration Interface

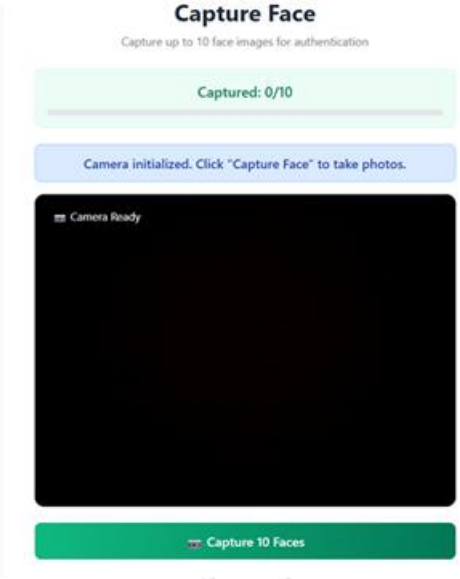

Figure 7. Face Capture During User Registration

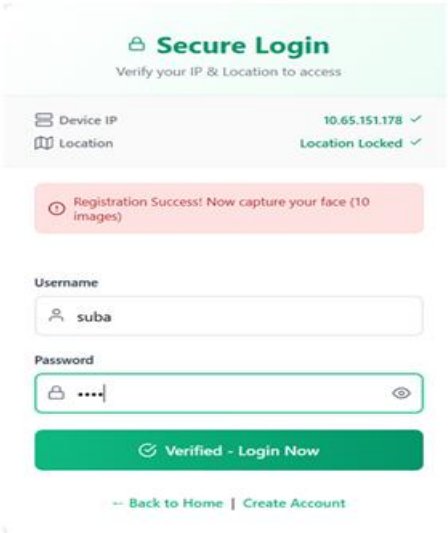

Figure 8. User Login Interface

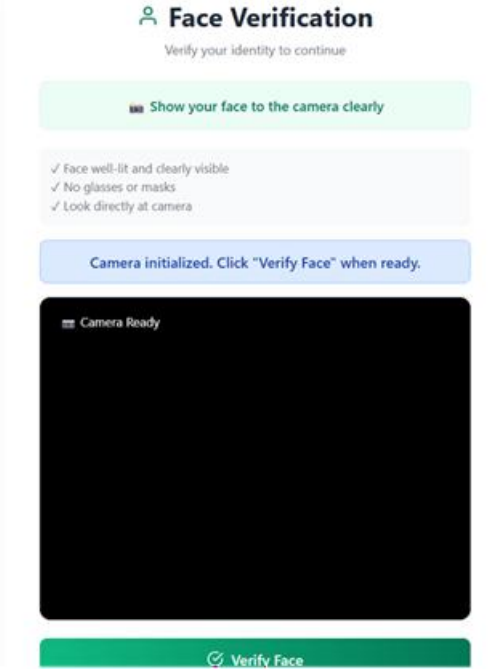

Figure 9. Facial Authentication in Login Process

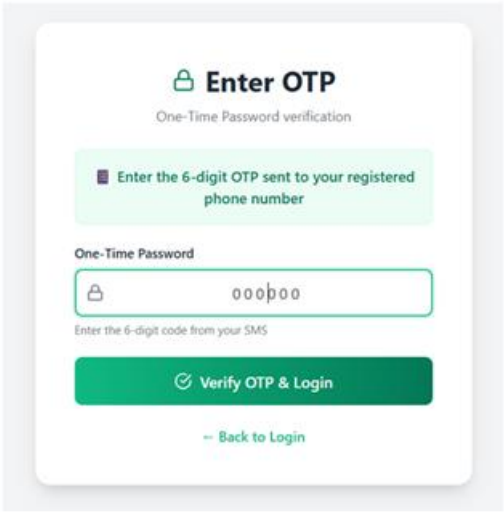

Figure 10. Secure OTP Verification Process

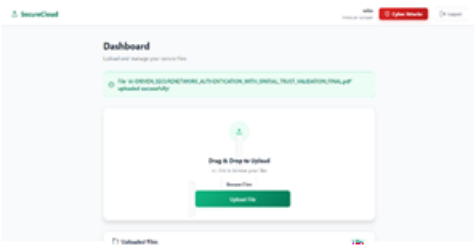

Figure 11. Dashboard After Successful Login

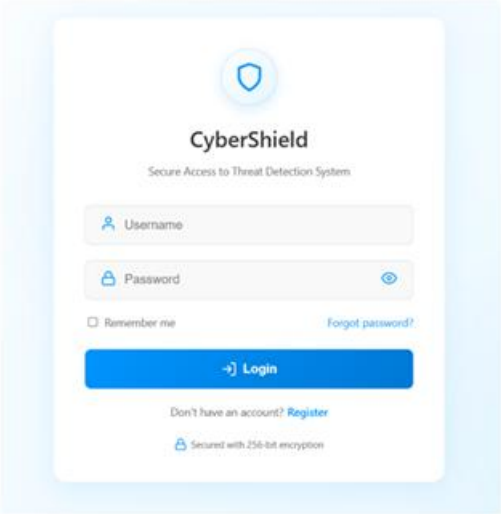

Figure 12. Cyber Security Login Page

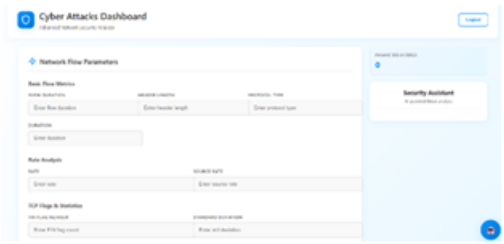

Figure 13. Cybersecurity Dashboard

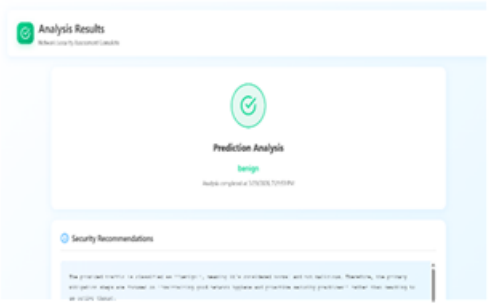

Figure 14. Cybersecurity Result Analysis (Attack/Threat Detection)

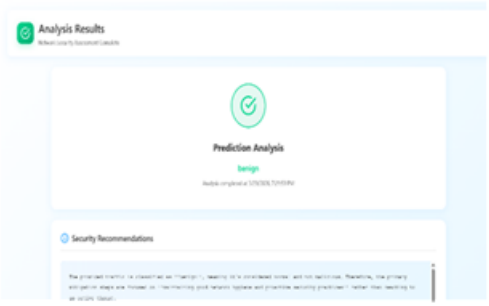

Figure 15.Security Recommendations for Protection

The proposed AI-based secure authentication and intrusion detection system successfully verifies users using multiple security layers, including face recognition, OTP

verification, and location-based validation.These results highlight the limitations of the password-based authentication and demonstrate the effectiveness of integrating behavioral analytics, spatial trust validation, and AI-driven risk assessment. The system's adaptive learning capability enables continuous refinement against evolving threats, transforming authentication into a dynamic, context-aware, and self-learning security framework suitable for modern enterprise and web environments.

VII. CONCLUSION

The proposed AI-driven Secure Network Authentication System with Spatial Trust Validation presents an advanced and adaptive approach to modern cybersecurity. By integrating behavioral analytics, spatial verification, machine learning, and generative AI, the system moves beyond traditional password-based authentication and establishes a multi-dimensional trust framework. It evaluates not only user credentials but also contextual parameters such as login behavior, device usage, IP address, and geolocation to ensure secure access. The intrusion detection module powered by XGBoost dynamically generates risk scores and accurately classifies suspicious activities, enabling timely intervention. Real-time anomaly detection combined with adaptive AI-driven recommendations strengthens proactive threat mitigation. The system transforms authentication from a static, reactive mechanism into an intelligent, self-learning, and context-aware security model. This framework significantly improves access reliability, reduces unauthorized intrusion risks, and provides a scalable solution suitable for modern enterprise and web-based environments.Overall, the system establishes a self-learning, intelligent, and adaptive cybersecurity framework that significantly enhances access reliability, security risks, and strengthens organizational resilience. By shifting authentication from a static, reactive process to a proactive, intelligent approach, this system exemplifies how AI-driven, context-aware solutions can redefine the security paradigm for modern web applications and enterprise networks, ensuring robust, continuous protection of digital assets.

REFERENCES

[1] Dharmalingam and P. Tirumala, "Voice Authentication at Scale: A Room Level Approach for Smart Devices," 2025 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 2025, pp. 1-5.

[2] J. Chen and F. Huang, "Research on Access Authentication Architecture Adapting to Beidou Communication Network," 2022 4th International Conference on Intelligent Control, Measurement and Signal Processing (ICMSP), Hangzhou, China, 2022, pp. 885-889.

[3] L. Venkatraman, S. Niksheetha, P. Ezhilarasi and S. Rajeshkannan, "Cipher Care : Multi-Authentication Video Steganography Powered by CNNs," 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 2024, pp. 1-6.

[4] L. Rui, J. Liu and M. Lu, "Security Authentication Scheme for Low Earth Orbit Satellites Based on Spatial Channel Characteristics," 2022 IEEE 8th International Conference on Computer and Communications (ICCC), Chengdu, China, 2022, pp. 396-400.

[5] P. Kalpana, S. R. Sitaraman, S. S. Harakannanavar, Z. Alsalami and S. Nagaraj, "Efficient Multimodal Biometric Recognition for Secure Authentication Based on Faster Region-Based Convolutional Neural Network," 2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON), Bengaluru, India, 2024, pp. 1-5.

[6] P. N. Goki, T. T. Mulugeta, N. Sambo, R. Caldelli and L. Potì, "Optical Network Authentication through Rayleigh Backscattering Fingerprints of the Composing Fibers," GLOBECOM 2022 - 2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 2022, pp. 2146-2150.

[7] S. Demirci, L. Afeef and H. Arslan, "Deep Learning-Enhanced Physical Layer Security in XL-MIMO: A Visibility Region-Based Authentication Framework," 2025 33rd Signal Processing and Communications Applications Conference (SIU), Sile, Istanbul, Turkiye, 2025, pp. 1-4.

[8] S. Li et al., "Efficient Vehicle Secure Scheduling and Access Authentication Scheme for 5G-Integrated Emergency Rescue Scenario," in IEEE Transactions on Intelligent Transportation Systems, vol. 26, no. 11, pp. 21004-21023, Nov. 2025.

[9] Y. Xiao et al., "RF-Based Identification Framework Against Unauthorized UAV Networking in Low-Altitude Economy," in IEEE Transactions on Network Science and Engineering, vol. 13, pp. 6538-6555.

[10] Y. Mahesh, P. Sirivarshini, C. Kavya and D. B. Naik, "Image-Based Authentication: Strengthening Security with Graphical Passwords," 2025 IEEE 17th International Conference on Computational Intelligence and Communication Networks (CICN), Goa, India, 2025, pp. 920-926.