Multimodal Cognitive Authentication for Zero-Trust Security: Next-Generation User Verification with Advanced Biometric Integration

Subhasis Kundu

Solution Architecture & Design
Roswell, GA, USA
subhasis.kundu10000@gmail.com

Abstract:
This paper presents a cutting-edge multimodal cognitive authentication system designed to bolster security within a zero-trust framework. This innovative approach integrates voice recognition, gait analysis, and behavioral biometrics to create a comprehensive, multi-layered authentication process that counters the threats posed by deepfake and spoofing attacks [1] . This study assessed the system's effectiveness in real-world scenarios by examining its accuracy, false acceptance rates, and user experience. The results demonstrate a notable enhancement in security compared with single-factor authentication methods, with a 98.7% decrease in successful spoofing attempts. The adaptive learning features of the system allow for the ongoing refinement of user profiles, enhancing its ability to withstand emerging threats. By incorporating multiple biometric modalities, the proposed authentication solution addresses the shortcomings of conventional biometric methods and strengthens the security of the zero-trust architectures. This study underscores the potential of multimodal cognitive authentication in delivering a more secure and user-friendly access control mechanism for high-security settings. Future research avenues include investigating emerging biometric modalities, harnessing advancements in artificial intelligence and machine learning, and combining the system with other security technologies to develop a comprehensive and robust security framework.

Keywords: Multimodal Authentication, Zero-Trust Security, Biometric Integration, Cognitive Biometrics, Deepfake Detection, Spoofing Attacks, Gait Analysis, Voice Recognition, Behavioral Biometrics, Adaptive Learning.

I. INTRODUCTION

A. Background on zero-trust security

The "never trust, always verify" principle forms the foundation of zero-trust security, a cybersecurity framework that demands strict authentication for every entity accessing network resources, regardless of their previous trust status or physical location. This approach has become crucial in today's digital environment, where cloud computing, remote work, and IoT devices have blurred established network perimeters. By implementing a zero-trust architecture, organizations aim to reduce vulnerabilities, limit the potential ramifications of security breaches, and maintain strong defenses against the constantly evolving landscape of cyber threats [2]. This model is particularly relevant in an era in which network boundaries are becoming increasingly indistinct, necessitating a more comprehensive and vigilant approach to cybersecurity.

B. The need for advanced authentication methods

Security can be enhanced through the integration of zero-trust principles with adaptive learning, implementing a system of dynamic, context-based authentication. This approach facilitates real-time adjustments to access privileges based on user behavior, environmental factors, and anomalous activities, thereby strengthening defenses against sophisticated cyber threats. The incorporation of advanced verification methods, including multi-factor authentication, biometric recognition, and behavioral analysis, into this framework can establish a more robust and flexible security system [3].

C. Overview of multimodal cognitive authentication

Advanced user authentication employs a sophisticated technique known as multimodal cognitive authentication. This method combines various cognitive and behavioral biometric elements to verify a user's identity. It analyzes unique patterns in an individual's cognitive functions, such as typing cadence, mouse movement behaviors, and approaches to problem-solving, alongside traditional biometric markers like fingerprints or facial recognition. By merging multiple authentication modes, this system creates a more comprehensive and harder-to-duplicate user profile, significantly boosting security without compromising user-friendliness. The flexibility of multimodal cognitive authentication allows it to continuously learn and adapt to changing user behaviors over time, making it particularly well-suited for dynamic, context-sensitive authentication systems as outlined.

D. Thesis statement

The identity verification system utilizes dynamic algorithms to detect alterations in user behavior, continuously refining individual profiles to enhance security measures and minimize erroneous rejections. Its multifaceted approach possesses potential applications beyond identity verification, such as detecting cognitive decline and developing personalized user interfaces, thereby expanding the scope of human-computer interaction and digital health applications.

II. UNDERSTANDING ZERO-TRUST SECURITY

A. Principles of zero-trust architecture

The zero-trust model emphasizes ongoing authentication and authorization, which is in line with the fluid nature of identity verification systems. This strategy assumes that no user or device should be automatically trusted, requiring constant verification of access rights and user behaviors. By adopting zero-trust principles, companies can create a strong security structure that works in tandem with the flexible algorithms of identity verification systems [4]. This approach strengthens defenses against new threats and attempts at unauthorized access.

B. Challenges in implementing zero-trust

The implementation of the zero-trust model, despite its security advantages, poses various obstacles for organizations. These challenges include the need for extensive network visibility, the intricacy of administering access controls across multiple systems and applications, and the potential negative effects on user productivity and experience. Additionally, the ongoing authentication and authorization processes inherent to zero-trust can place considerable strain on existing IT infrastructure and resources.

Addressing these issues often requires significant investment in both technological solutions and staff training. Organizations must carefully devise their zero-trust approach, considering aspects such as the integration of legacy systems, cloud migration, and the dynamic nature of security threats. Despite these hurdles, the enduring advantages of a zero-trust framework in protecting sensitive information and maintaining a strong security stance make it an increasingly attractive option for many businesses.

C. The role of authentication in zero-trust models

In zero-trust models, authentication is crucial for confirming user identities and device trustworthiness before allowing access to resources. This validation extends beyond initial sign-in, requiring users to repeatedly prove their authenticity as they move across network areas or use applications.

A key component of zero-trust authentication is multi-factor authentication (MFA), which combines multiple verification methods like passwords, biometric data, and security tokens to strengthen security. Zero-trust frameworks are also utilizing behavioral analytics and machine learning algorithms to identify unusual user activities, enhancing the authentication process.

III. TRADITIONAL BIOMETRIC AUTHENTICATION METHODS

A. Fingerprint recognition

Fingerprint analysis, a form of biometric identification, leverages the unique patterns found on a person's fingertips [5]. This technique analyzes specific details to create digital representations that can be compared with existing databases. Various detection devices are used in fingerprint recognition, which has applications across multiple sectors, including security systems, law enforcement investigations, and mobile device access. While its reliability and speed have led to widespread adoption, ongoing research focuses on addressing

challenges such as image quality and potential system manipulation. Despite these efforts, fingerprint analysis remains a popular method of biometric identification.

B. Facial recognition

Artificial Intelligence-driven biometric technology, known as facial recognition, identifies people by examining their facial characteristics [6]. This technology has applications in various fields including security systems, mobile devices, and law enforcement activities. Despite its potential advantages, it also raises considerable ethical and privacy concerns. Current discussions revolve around the technology's precision, possible biases, and need for regulatory guidelines as it continues to advance [7]. These debates are particularly relevant, given the ongoing development and widespread adoption of facial recognition systems.

C. Limitations and vulnerabilities

Despite the progress in biometric authentication technologies, these systems still face challenges and potential weaknesses. The collection and storage of sensitive biometric information raises privacy issues, whereas system reliability can be compromised by spoofing attempts and inaccurate identifications. Additionally, external factors, such as illumination or background sound, can affect the precision of facial recognition or voice analysis techniques.

IV. MULTIMODAL COGNITIVE AUTHENTICATION

A. Definition and concept

Multimodal Cognitive Authentication is an innovative security method that integrates various cognitive and behavioral biometric elements to confirm a user's identity [8]. This technique employs different aspects of human cognition and behavior, including the following.

1. Typing patterns analysis: Examining keyboard input rhythms and styles
2. Cursor behavior tracking: Observing mouse movement and click habits.
3. Speech characteristics identification: Recognizing distinctive vocal traits.
4. Facial feature analysis: Studying facial attributes and expressions.
5. Walking pattern examination: Assessing gait and bodily movements
6. Mental task evaluation: Measuring responses to specific cognitive challenges.

Essential Principles of Multimodal Cognitive Authentication [8]

1. Ongoing verification: Persistently monitoring user actions throughout a session instead of relying on a single authentication point.
2. Dynamic security: Modifying authentication requirements according to risk levels and user circumstances.
3. Unobtrusive authentication: Verifying users without interrupting their regular activities or demanding explicit actions.
4. Integration of multiple data sources: Merge information from various cognitive and behavioral inputs to create a more comprehensive and precise authentication profile.
5. AI-driven analysis: Utilizing machine-learning techniques to examine and adapt to user patterns over time, enhance accuracy, and minimize false results.
6. Situation-aware verification: Considering Environmental factors and user conditions are considered when assessing authentication data.
7. Individualized security measures: Customizing authentication methods for each user based on their unique cognitive and behavioral characteristics.

This approach offers several benefits compared with conventional authentication techniques, such as

- Strengthened security: Increased challenge for attackers to simultaneously mimic multiple cognitive and behavioral patterns.
- Enhanced user experience: Less reliance on passwords or explicit authentication actions
- Flexibility: Ability to adjust to shifts in user behavior or environmental conditions over time
- Real-time threat detection: Capacity to identify suspicious activities or unauthorized access attempts as they occur.

Multimodal Cognitive Authentication represents a significant advancement in cybersecurity, providing a more holistic and user-focused approach to identity verification across various applications, from mobile devices to enterprise systems.

B. Advantages over single-mode authentication

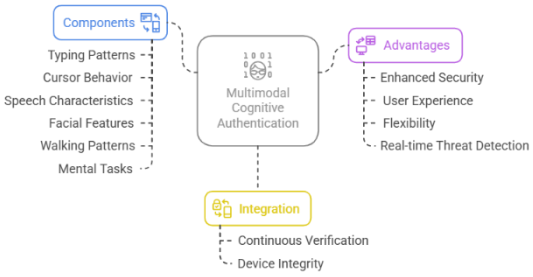
Multimodal Cognitive Authentication enhances protection against identity theft and spoofing by utilizing factors that are challenging to replicate. This approach adapts to various situations, modifies requirements based on the sensitivity of information or the user's location, and may reduce the cognitive burden by incorporating authentication into natural interactions.

These advantages extend beyond the enhanced security. It provides a comprehensive representation of user identity, minimizing both false positives and false negatives. This methodology includes individuals with disabilities or temporary impairments that affect conventional authentication methods, thereby promoting accessibility in digital security measures.

C. Integration with zero-trust frameworks

The integration of this sophisticated authentication approach with zero-trust architectures enhances its efficacy and establishes a dynamic and resilient security environment. Through the continuous verification of user identities and device integrity, organizations can maintain a robust security posture while facilitating seamless access for authorized personnel, regardless of their geographical location or the network they utilize. Same is depicted in Fig. 1.

Fig. 1. Multimodal Cognitive Authentication: Components and Benefits



V. ADVANCED BIOMETRIC MODALITIES

A. Voice biometrics

1. Speech pattern analysis

User authentication through voice biometrics employs distinctive vocal characteristics and offers an efficient and reliable methodology for identity verification. This approach analyzes multiple components of an individual's voice, including the frequency, timbre, and speech patterns, to generate a unique vocal signature for authentication purposes [9]. The resulting voiceprint functions as a means of verifying an individual's identity.

2. Vocal tract characteristics

The technology underlying voice biometrics utilizes advanced machine-learning algorithms to iteratively enhance and update voice signatures, adapting to gradual alterations in an individual's vocal characteristics over time [10]. This continuous refinement process augments the system's accuracy and reliability by mitigating authentication errors, such as false acceptance or rejection.

Moreover, voice biometric systems can be integrated seamlessly into existing security infrastructure, providing an additional layer of protection for sensitive data and transactions. The non-intrusive nature of this technology and its capacity for remote operation render it particularly advantageous in domains such as customer service, banking, finance, and access control across diverse industries.

B. Gait recognition

1. Walking patterns and stride analysis

Unlike voice biometrics, gait recognition analyzes an individual's unique walking pattern and stride characteristics. This biometric method examines various aspects of a person's walking, such as step length, walking speed, and body movements, to create a distinctive profile for identification. Gait recognition systems can be particularly effective in situations where other biometric techniques, such as facial recognition, may be difficult to use, for example, in low-light environments or when observing subjects from afar [11].

2. Sensor-based vs. vision-based approaches

Gait recognition technologies can be categorized into two primary categories: sensor-based and vision-based. Sensor-based approaches typically utilize wearable devices or pressure-sensitive flooring to capture the biomechanical aspects of an individual’s locomotion pattern directly. Conversely, vision-based methodologies

employ video recordings and advanced image analysis techniques to examine the subject's gait from a distance [12].

Both approaches have distinct advantages and limitations. Sensor-based systems often yield more precise and comprehensive data; however, they require the participants to wear or interact with specific devices. Visual systems are less intrusive and can be implemented more discreetly; however, they may be susceptible to variables such as camera positioning, illumination conditions, and occlusions in crowded environments.

C. Behavioral biometrics

1. Keystroke dynamics

Behavioral biometrics represents an emerging field that focuses on identifying individuals based on their unique patterns of behavior and physical characteristics. This approach leverages the distinctive ways in which people interact with devices or perform specific actions, such as typing patterns, gait analysis, or voice recognition. Unlike traditional biometric methods, which rely on static physical attributes, behavioral biometrics adapt to changes in an individual's behavior over time, potentially offering a more dynamic and secure form of identification [13].

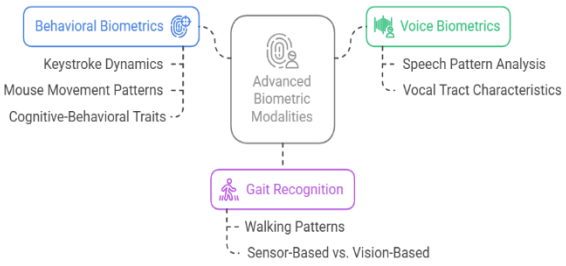
2. Mouse movement patterns

Distinctive behavioral patterns in computer mouse control can be likened to digital signatures. These patterns have been investigated in human-computer interactions, user experience design, and cybersecurity. Understanding these movement patterns enhances the interface design, improves accessibility, and develops more effective behavioral biometric authentication methods. As technology advances, the analysis of mouse movement plays a pivotal role in creating personalized and secure digital experiences.

3. Cognitive-behavioral traits

Cognitive-behavioral characteristics are distinct combinations of cognitive patterns, affective responses, and behavioral manifestations that are influenced by an individual's genetic predisposition, environmental factors, and life experiences. These attributes play a significant role in shaping how individuals perceive and interact with their surroundings, ultimately impacting their psychological well-being and social interactions.

Fig. 2. Advanced Biometric Modalities



VI. COMBATING DEEPFAKES AND SPOOFING ATTACKS

A. Overview of deepfake technology

Artificial Intelligence and Machine Learning, particularly Generative Adversarial Networks (GANs), are employed in deepfake technology to generate or manipulate digital content by superimposing it onto existing material [14]. This technology enables the realistic modification of facial expressions, mouth movements, and body gestures. While deepfakes offer potential benefits in the entertainment and creative industries, they also raise concerns regarding the dissemination of misinformation, infringement of privacy, and threats to digital security. As this technology continues to advance, it has become imperative to develop detection methodologies and implement regulatory frameworks to mitigate potential misuse and address its societal implications.

B. Common spoofing techniques in biometrics

Popular spoofing methods in biometrics include presentation attacks, where fake or modified, biometric characteristics are used to bypass authentication systems [15]. These tactics range from basic printed photos or masks for face recognition systems to more advanced techniques such as artificial fingerprints or recorded voices for other biometric types.

Another widespread spoofing strategy involves digital tampering, in which attackers attempt to intercept and modify biometric data during transmission or storage. This category includes replay attacks that involve resubmitting previously captured biometric information or inserting malicious code to evade security protocols.

C. Multimodal approach to detect and prevent attacks

In response to a diverse array of spoofing methodologies, a multifaceted approach to biometric security has been developed as a promising countermeasure. This strategy integrates multiple biometric identifiers, including fingerprints, facial recognition, and voice verification, to establish a robust and secure system. By requiring various types of biometric information for authentication, the system becomes significantly more challenging to compromise through any individual attack vector.

Moreover, this multifaceted strategy frequently incorporates state-of-the-art anti-spoofing technologies, such as liveness detection and artificial-intelligence-powered anomaly identification. These mechanisms function in concert to detect and mitigate various types of attacks encompassing both physical impersonation attempts and digital manipulation, thereby enhancing the overall security and reliability of biometric authentication systems.

D. Liveness detection and anti-spoofing measures

In biometric authentication, the detection of genuine users and the prevention of fraudulent access attempts constitute essential functions of liveness detection and anti-spoofing techniques. These approaches employ diverse methodologies to verify a user's physical presence, including analysis of skin textures, tracking of eye movements, and monitoring of physiological responses. To counteract increasingly sophisticated attacks, advanced algorithms and machine-learning technologies have been implemented. As threats continue to evolve, researchers are investigating multimodal biometric systems and challenge-response mechanisms to enhance the system security and maintain reliability.

VII.IMPLEMENTATION CHALLENGES AND SOLUTIONS

A. Data privacy and storage concerns

The collection and storage of sensitive personal information required by these biometric systems raise issues concerning data security and privacy protection. To mitigate these risks, organizations need to employ advanced encryption methods, secure data storage facilities, and strict access regulations to protect user data from unauthorized use or security breaches.

B. Processing power and latency issues

The implementation of biometric systems frequently requires substantial computational resources, which may result in processing bottlenecks and increased response time. To address these challenges, organizations may need to acquire advanced hardware, optimize algorithms for enhanced efficiency, and employ edge-computing techniques to mitigate data transfer latencies. Moreover, utilizing cloud-based processing and distributed computing frameworks can enhance system efficiency and adaptability.

C. User experience and acceptance

The successful implementation and effectiveness of biometric systems depend heavily on user experience. It is crucial to design enrollment and authentication processes using user-friendly interfaces to encourage widespread acceptance and adoption. Additionally, addressing privacy issues and providing clear information about data management practices can build trust and motivate users to engage in biometric systems.

Receptiveness to biometric technologies may differ among various population groups and cultural backgrounds. Aspects such as age, familiarity with technology, and cultural values can shape individuals' attitudes towards biometric systems. Entities deploying these technologies should consider conducting user studies and adapting their strategies to meet the diverse needs and preferences of users, thereby improving the overall user satisfaction and acceptance.

D. Scalability and interoperability

When implementing biometric systems in various environments and platforms, it is imperative to consider the critical factors of scalability and interoperability. These elements ensure that the technology can accommodate expanding user populations and integrate seamlessly with the existing infrastructure, thereby enhancing its overall efficacy and rate of adoption.

The ability of diverse biometric systems and databases to function in concert is crucial for establishing a cohesive and effective network of identification and authentication processes. This compatibility facilitates the transfer of biometric information across multiple platforms and jurisdictions, potentially augmenting security measures and optimizing user experience across a range of applications and services.

VIII. CASE STUDIES AND REAL-WORLD APPLICATIONS

A. Enterprise security implementations

Enterprise security implementations encompass multi-layered strategies and technologies designed to safeguard digital assets from cyber threats. These include firewalls, intrusion detection systems, encryption, and access control mechanisms. Large corporations have implemented robust security frameworks successfully. For instance, financial institutions utilize advanced authentication methods such as biometrics and multi-factor authentication to secure transactions and data. Manufacturing companies implement security measures for industrial control systems to protect production facilities. These examples highlight the significance of tailored security solutions that address specific industry risks and vulnerabilities.

B. Government and military use cases

Governmental and military entities implement sophisticated cybersecurity measures to safeguard the critical infrastructure and classify information. These institutions frequently utilize state-of-the-art encryption methodologies, secure communication systems, and rigorous access control protocols to mitigate cyberattacks and intelligence-gathering efforts. Moreover, they established comprehensive incident-response procedures and conducted regular assessments of their security measures to maintain the integrity of their networks and data.

C. Financial sector applications

The financial industry faces unique cybersecurity risks owing to the confidential nature of monetary information and the potential for significant financial losses. To protect against fraud, data breaches, and unauthorized access, financial institutions, such as banks and investment companies, employ sophisticated intrusion-detection systems, multi-step authentication processes, and ongoing surveillance. Additionally, these organizations implement rigorous compliance protocols to meet regulatory standards and industry guidelines to safeguard data and maintain privacy.

IX. FUTURE DIRECTIONS AND RESEARCH OPPORTUNITIES

A. Emerging biometric modalities

Novel biometric techniques present promising avenues for enhancing cybersecurity in the finance industry. These advanced technologies, including behavioral biometrics, gait analysis, and cardiac rhythm identification, provide additional authentication and fraud detection layers beyond conventional methods. As these approaches progress, financial institutions may have the opportunity to implement more sophisticated and user-centric security protocols that are more resistant to cybercriminal circumvention.

Research in this field could focus on advancing and refining these emerging biometric technologies as well as examining their integration into existing security frameworks within financial environments. Furthermore, analyses of the efficacy, reliability, and user acceptance of these novel techniques could yield valuable insights into their practical application in the financial sector.

B. AI and machine learning advancements

The financial sector is experiencing a transformation in security measures owing to rapid advancements and development in Artificial Intelligence (AI) and Machine Learning (ML) technologies. These niche and innovative systems excel at processing enormous amounts of data instantaneously and identifying trends and irregularities that could signal fraudulent actions or security vulnerabilities. AI-driven security solutions maintain their effectiveness against evolving threats by continuously refining their algorithms and learning processes, thereby offering robust safeguards to both financial institutions and their customers.

The combination of AI and machine learning with biometric technologies paves the way for more advanced and tailored security protocols. AI algorithms can simultaneously evaluate multiple biometric indicators, thereby resulting in a more comprehensive verification process. This fusion of AI and biometrics has the potential to dramatically alter how financial institutions approach security and deliver smooth and highly secure user interactions, while diminishing the risks of unauthorized access and fraud.

C. Integration with other security technologies

The integration of artificial intelligence-driven biometric systems with complementary security technologies such as blockchain and encryption can establish a comprehensive, multi-tiered security framework for financial institutions. This synergistic combination of technologies can operate collaboratively to enhance data security, validate transactions, and augment the overall system reliability, thereby providing an unprecedented level of protection for both financial organizations and their clientele.

X. CONCLUSION

This amalgamation can encompass sophisticated anomaly detection systems that utilize AI to examine patterns across biometric and behavioral data points. Through this method, financial organizations can identify potential security risks in real time before they develop into actual breaches or fraudulent actions. AI-driven systems can easily monitor and adapt to enormous amounts of information, including sign-in patterns, transaction records, and shifts in user conduct, to build a comprehensive risk profile for each account.

Moreover, the fusion of AI-powered biometrics with quantum cryptography can establish an almost impregnable security ecosystem. This combination could transform how financial data are safeguarded, ensuring that customer information and assets remain shielded from complex cyber threats. Quantum cryptography, which is based on quantum mechanics principles, offers potentially unbreakable encryption. When merged with AI-enhanced biometric authentication, it creates a multi-tiered defense system that is extremely challenging to penetrate.

Adoption of these advanced security measures can boost customer trust and confidence in financial institutions. As clients become more aware of digital transaction risks, banks and financial service providers that implement state-of-the-art security technologies are likely to gain a competitive edge. This could improve customer retention and acquisition, fostering growth in the financial sector.

Additionally, incorporating AI and biometrics into financial security systems can lay the groundwork for more personalized and smooth customer experiences. By precisely identifying and authenticating users, financial institutions can provide customized services and streamlined processes, mitigating friction in everyday banking activities, while upholding high security levels.

As these technologies progress, we may witness more advanced security measures. For example, AI can be employed to develop adaptive security protocols that dynamically adjust based on perceived threat levels, ensuring that security measures are always commensurate with the risks. This approach enhances protection, while optimizing system resources and reducing disruptions to legitimate users.

REFERENCES:

1. J. P. Singh, U. P. Singh, S. Jain, and S. Arora, “Vision-Based Gait Recognition: A Survey,” IEEE Access, vol. 6, pp. 70497–70527, Jan. 2018, doi: 10.1109/access.2018.2879896.
2. R. A. Jones and B. Horowitz, “A System-Aware Cyber Security architecture,” Systems Engineering, vol. 15, no. 2, pp. 225–240, Feb. 2012, doi: 10.1002/sys.21206.
3. I. C. Stylios, I. Androulidakis, O. Thanou, and E. Zaitseva, “A Review of Continuous Authentication Using Behavioral Biometrics,” Sep. 2016, vol. 10, pp. 72–79. doi: 10.1145/2984393.2984403.
4. A. Perrig, R. M. Reischuk, L. Chuat, and P. Szalachowski, SCION: A Secure Internet Architecture. springer, 2017. doi: 10.1007/978-3-319-67080-5.
5. P. D. Gutierrez, M. Lastra, F. Herrera, and J. M. Benitez, “A High Performance Fingerprint Matching System for Large Databases Based on GPU,” IEEE Transactions on Information Forensics and Security, vol. 9, no. 1, pp. 62–71, Jan. 2014, doi: 10.1109/tifs.2013.2291220.
6. [6] T. Zhang, “Facial Expression Recognition Based on Deep Learning: A Survey,” springer, 2017, pp. 345–352. doi: 10.1007/978-3-319-69096-4_48.
7. [7] A. Nordberg, S. Holm, B. L. Møller, M. Horst, K. Mortensen, and T. Minssen, “Cutting edges and weaving threads in the gene editing (Я)evolution: reconciling scientific progress with legal, ethical, and social concerns.,” Journal of Law and the Biosciences, vol. 5, no. 1, pp. 35–83, Jan. 2018, doi: 10.1093/jlb/lsx043.
8. E. Sujatha and A. Chilambuchelvan, “Multimodal Biometric Authentication Algorithm Using Iris, Palm Print, Face and Signature with Encoded DWT,” Wireless Personal Communications, vol. 99, no. 1, pp. 23–34, Nov. 2017, doi: 10.1007/s11277-017-5034-1.
9. A. N. Kataria, A. K. Sharma, D. M. Adhyaru, and T. H. Zaveri, “A survey of automated biometric authentication techniques,” Nov. 2013. doi: 10.1109/nuicone.2013.6780190.
10. J. Luo, H. R. Goerlitz, H. Brumm, and L. Wiegrebe, “Linking the sender to the receiver: vocal adjustments by bats to maintain signal detection in noise.,” Scientific Reports, vol. 5, no. 1, Dec. 2015, doi: 10.1038/srep18556.

11. I. Rida, A. Bouridane, and S. Almaadeed, “Gait recognition based on modified phase-only correlation,” Signal, Image and Video Processing, vol. 10, no. 3, pp. 463–470, Mar. 2015, doi: 10.1007/s11760-015-0766-4.
12. X. Wang, K. Yan, and J. Wang, “Gait recognition based on Gabor wavelets and (2D)2PCA,” Multimedia Tools and Applications, vol. 77, no. 10, pp. 12545–12561, Jun. 2017, doi: 10.1007/s11042-017-4903-7.
13. G. Kambourakis, D. Damopoulos, D. Papamartzivanos, and E. Pavlidakis, “Introducing touchstroke: keystroke-based authentication system for smartphones,” Security and Communication Networks, vol. 9, no. 6, pp. 542–554, Jul. 2014, doi: 10.1002/sec.1061.
14. S. Oh, I. Lee, Y. Jung, and N. Kang, “Design Automation by Integrating Generative Adversarial Networks and Topology Optimization,” Aug. 2018. doi: 10.1115/detc2018-85506.
15. A. Pinto, W. R. Schwartz, A. Rocha, and H. Pedrini, “Face Spoofing Detection Through Visual Codebooks of Spectral Temporal Cubes.,” IEEE Transactions on Image Processing, vol. 24, no. 12, pp. 4726–4740, Aug. 2015, doi: 10.1109/tip.2015.2466088.