IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Secure Mobile Two-Factor Authentication Leveraging Active Sound Sensing

[1]Sherin Mariya James, [2]Sumi S
[1]Student, [2]Professor
[1] Computer Science and Engineering (Cyber Security),
[1] St. Joseph's college of Engineering & Technology, Palai, India

Abstract: Two-factor authentication (2FA) has emerged as a cornerstone of digital security in an age where mobile devices and Internet-of-Things (IoT) ecosystems dominate everyday interactions, effectively mitigating risks associated with password vulnerabilities such as phishing and credential compromise. This review paper offers a thorough examination of the evolutionary trajectory of acoustic-based authentication mechanisms, with a special emphasis on active sound sensing techniques that enable secure, zero-interaction 2FA. Commencing with pioneering ambient audio methods for shared key generation, the analysis progresses through sensor fusion strategies, prox imity detection in voice-enabled IoT environments, and culminates in sophisticated echo-based frameworks like Proximity-Echo. We elucidate the rationale behind each developmental phase, conduct comparative assessments of technical trade-offs—particularly in terms of usability, at tack resilience, and computational efficiency—and highlight implications for embedded mobile systems. The paper concludes with a practical workflow integrating active beep emission and echo signature analysis, alongside forward-looking research avenues encompassing multi-modal sensor integration, post-quantum adaptations, and energy-efficient implementations.

Index Terms - Two-Factor Authentication (2FA), Active Sound Sensing, Proximity Detection, Acoustic Fingerprinting, Zero-Interaction Authentication, Relay Attacks, Man-in-the-Middle Attacks, IoT Security

I. INTRODUCTION

Mobile security landscapes are evolving at a breakneck pace, driven by the ubiquity of smart phones, wearables, and voice-powered assistants that seamlessly integrate into users' daily routines. Beyond mere convenience, these devices handle sensitive operations ranging from financial transactions to health monitoring, making robust authentication imperative. Traditional single factor methods, predominantly password-based, fall short against modern threats like brute-force attacks and social engineering. Enter two-factor authentication (2FA), which mandates an additional verification layer—often device possession or biometric traits—to fortify access controls. Yet, mainstream 2FA implementations, such as SMS codes or push notifications, impose user interactions that can frustrate adoption, particularly among vulnerable demographics like the elderly or those with impairments. This usability gap has catalyzed innovations in zero interaction authentication (ZIA), where devices leverage contextual cues for seamless verification. Acoustic sensing stands out in this domain, harnessing ubiquitous microphones and speakers to infer proximity or device identity without explicit user input. Early explorations relied on passive ambient audio to derive shared secrets, capitalizing on environmental sound similarities for secure key exchange. Subsequent refinements introduced active signals—emitted beeps or chirps—to enable precise measurements like time-of-flight or echo reflections, bolstering defenses against relay and man-in-the-middle (MiM) attacks. This progression addresses core challenges: ensuring security in noisy, dynamic environments while minimizing computational overhead on resource-constrained devices. This review synthesizes these advancements, spotlighting "Proximity-Echo: Secure Two Factor Authentication Using Active Sound Sensing" as a pivotal milestone. We chronicle the f ield's chronology, dissect methodologies, and evaluate trade-offs through comparative

lenses. Emphasis is placed on practical deployments in mobile and IoT contexts, where audio hardware is readily available. To fully appreciate the design imperatives, it is essential to consider the multifaceted requirements of acoustic-based systems. These include not only technical efficacy but also alignment with real-world constraints such as battery life and regulatory compliance. The evolution reflects a deliberate response to emerging threats, where initial passive techniques gave way to active paradigms capable of withstanding sophisticated adversarial tactics. Furthermore, the integration of acoustic methods into broader security ecosystems under scores their versatility. For instance, in mobile banking or healthcare apps, where rapid yet secure access is paramount, these techniques offer a balance between protection and user experience. As we delve deeper, the interplay between innovation and practicality becomes evident, guiding future enhancements in this domain

II. LITERATURE REVIEW

A.2013: Secure Communication Based on Ambient Audio

Context-In the nascent stages of context-aware security, ambient audio emerged as a viable modality for establishing secure channels among proximate devices, leveraging shared environ mental sounds to infer co-presence without explicit data exchange. This period marked a shift from traditional key distribution methods toward unobtrusive, environmentally derived secrets, addressing the growing need for ad-hoc secure communications in pervasive computing environ ments.

Method-Schürmann et al. employ audio fingerprinting techniques, extracting features like spectrograms from ambient recordings, and apply fuzzy cryptography—such as error-correcting codes—to reconcile minor discrepancies in fingerprints, generating identical cryptographic keys on participating devices. The process involves synchronized sampling, feature vector computa tion, and noise-tolerant key derivation, ensuring that even slight variations in audio capture do not hinder key agreement.

Application to mobile 2FA- This approach suits scenarios where devices in close prox imity, like smartphones in a room, need to authenticate without user intervention, forming the bedrock for later ZIA systems in mobile environments. It enables seamless possession-based 2FA by verifying shared audio contexts, particularly useful in settings like office collaborations or public WiFi hotspots.

Strengths and limits- The method's unobtrusiveness and high entropy in fingerprints enhance security against eavesdropping, validated through experiments in diverse settings like offices and roads. Statistical tests confirm the randomness and uniqueness of derived keys. However, vulnerability in silent or replicable environments limits its standalone reliability, prompting shifts toward active sensing to introduce controlled variability and improve robustness

B.2014: Comparing and Fusing Different Sensor Modalities for Relay At tack Resistance in Zero-Interaction Authentication

Context- Relay attacks pose a significant threat to ZIA by falsifying proximity; this work addresses it by exploring multi-sensor contexts beyond single modalities, recognizing that in dividual sensors may falter in specific adversarial conditions, thus necessitating a diversified approach to co-presence detection.

Method-Truong et al. evaluate WiFi, Bluetooth, GPS, and audio for co-presence, using feature similarity metrics such as correlation coefficients, and fuse them via machine learning classifiers (e.g., decision trees) to improve detection accuracy under adversarial models like Dolev-Yao. The fusion process aggregates probabilities from each modality, enhancing overall resilience.

Application to mobile 2FA- Audio's room-level precision complements other sensors, enabling resilient 2FA in mobile logins where devices must confirm physical nearness. This is particularly relevant for scenarios involving laptops and smartphones, where fused contexts prevent unauthorized access in public spaces.

Strengths and limits. Fusion boosts resilience and usability, with empirical data from realistic settings showing reduced false positives and maintained low overhead. It also handles partial sensor compromise effectively if not all modalities are affected. Yet, computational overhead in processing multiple streams and potential sensor compromise necessitate careful integration, influencing subsequent hybrid designs that prioritize selective fusion.

C. 2017: PIANO: Proximity-Based User Authentication on Voice-Powered Internet-of-Things Devices

Context- Voice-IoT devices introduce unique challenges like forgery in speaker recognition; PIANO counters this with proximity as an authentication proxy, emerging amid the rise of smart assistants where traditional biometrics prove insufficient against replay attacks.

Method- Gong et al. utilize active acoustic signals over Bluetooth for distance estimation via the ACTION protocol, which involves signal emission, detection, and threshold-based access granting. Distance is computed using acoustic properties like time-of-flight, ensuring precise proximity verification.
Strengths and limits. Security, reliability, and personalization are strong, with theoretical proofs against forgery and empirical validation in IoT setups showing low error rates. However, multipath interference in cluttered environments and dependency on Bluetooth highlight needs for echo-based refinements to mitigate signal distortions.

D. 2018: Secure Context-Based Pairing for Unprecedented Devices
Context-Ad-hoc pairing in smart environments requires contextual keys; this extends ambient audio with voice commands, responding to the demand for spontaneous secure connections in increasingly dense device networks.
Method- Nguyen et al. combine speech recognition for device identification with audio fingerprints for key generation using fuzzy cryptography schemes. The process extracts class identifiers from spoken intents and derives keys from the same audio, ensuring dual uniqueness.
Application to mobile 2FA. Facilitates spontaneous secure connections, applicable to mobile 2FA in dynamic settings like public meetings or shared workspaces, where unknown devices must pair securely.
Strengths and limits- Natural interaction boosts usability, with Android implementations demonstrating high success rates and resistance to unauthorized pairing. However, reliance on audible commands restricts applicability in silent or noisy scenarios, limiting its versatility.
E. 2021: Proximity-Echo: Secure Two-Factor Authentication Using Active Sound Sensing
Context-Building on priors, this introduces active echoes for robust proximity proofs in 2FA, addressing limitations in passive methods susceptible to environmental replication.
Method- Ren et al. emit beeps alternately, segment chirps from echoes using period selection, compensate for microphone energy losses, and compare signatures via similarity metrics to detect proximity.
Application to mobile 2FA. Core for interaction-free verification, resisting MiM across devices and scenarios, ideal for online banking or email access on mobiles.
Strengths and limits-High accuracy of over (95%) and resistance to attacks, with testing done across different devices. Environmental changes may need some tuning, but compensation methods help reduce issues.

F. 2025: Two-Factor Authentication Based on Acoustic Fingerprinting in Modulation Domain
Context-Tackles persistent noise and distance issues via modulation, representing the latest in resilient fingerprinting amid advancing adversarial capabilities.
Method- Uses PSK-modulated signals, channel delay estimation via phase changes, noise removal from demodulated data, and transfer learning to capture subtle device differences for authentication.
Application to mobile 2FA-Future-proof for noisy, variable-distance environments like urban commutes, providing enduring security in evolving mobile landscapes.
Strengths and limits-Excellent noise tolerance and accuracy, with user experiments confirming efficacy; implementation complexity and training requirements pose deployment challenges.

III. ComparativeAnalysis andIntegrated Workflow for Secure Acoustic Based 2FA

Comparative Analysis Across Techniques, Domains, Security Focus, and Limitations, Highlight ing Evolutionary Improvements in Resilience and Efficiency, with a Proposed Acoustic 2FA Workflow Integrating Active Sensing, Proximity Verification via Robust Signatures, and Seam less Yet Traceable Authentication

Table 2.1: Comparative analysis of significant research works in acoustic-based authentication (2013–2025).

Paper	Year	Technique	Application Domain	Security Focus	Limitations
Schurmann et al.	2013	Ambient audio fingerprinting with fuzzy cryptography	Proximate device key generation in mobile settings	Eavesdropping and partial context reproduction resistance	Vulnerability in silent or easily replicable environments; lacks active contro
Truong et al.	2014	Multi-sensor fusion (audio, Wi-Fi, etc.) for co-presence detection	Zero-interaction relay-attack mitigation in authentication systems	Relay and partial Sensor compromise under Dolev–Yao model	increased computational overhead from fusion processing; dependency on multiple sensors
Gong et al	2017	Active acoustic signals for distance estimation (AC-TION protocol)	Proximity authentication in voice-powered IoT devices	Forgery attacks in IoT device pairs; distance-based access control	Susceptibility to multipath interference; reliance on Bluetooth connectivity
Nguyen et al.	2018	Voice-command integrated audio fingerprinting for pairing	Ad-hoc secure pairing in smart environments	Spontaneous unauthorized access and pairing attempts	Dependency on Audible commands; limited in silent or high-noise scenarios
Ren et al.	2021	Active beep emission with echo-location signatures	Mobile 2FA via proximity detection without interactions	Man-in-the-middle and co-located attacks across device models	Need environmental tuning; potential variations in echo path
Ren et al.	2023	Magnitude/phase distortion fingerprinting with distance conditions	Robust device authentication in varying acoustic conditions	Impersonation and MiM attacks with Signal normalization	Higher computational demands on resource-constrained devices
Ren et al.	2025	Modulation-domain (PSK)	Noise- and	Channel distortions	

		fingerprinting with ML-based classification	distortion-tolerant 2FA authentication in dynamic environments	and subtle frequency variations used for device-level verification	Complexity in ML model tuning; requires extensive labeled training

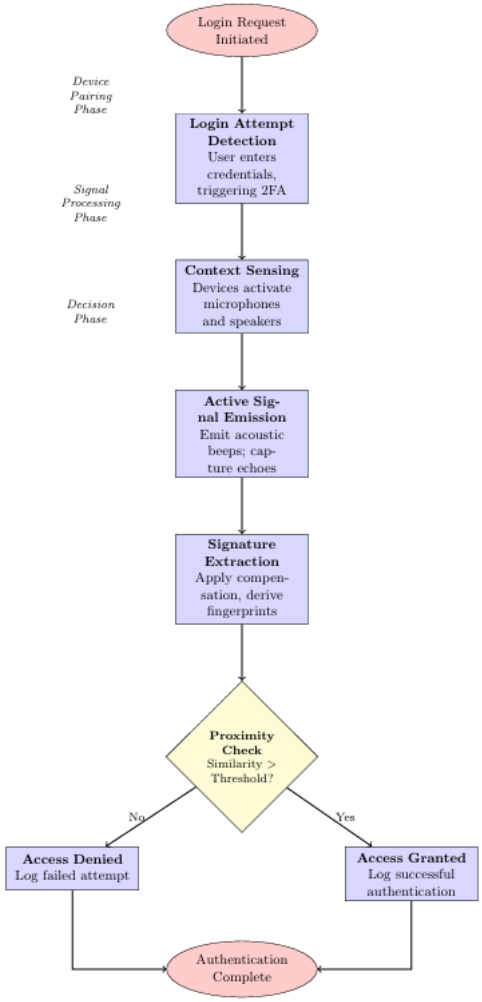

Figure 1: Proposed workflow for acoustic 2FA: sense actively with controlled signals, verify proximity through robust signatures,and authenticate seamlessly while ensuring traceability

IV. Discussion and Practical Note

When to employ active sensing. It excels in proximity-critical 2FA where passive methods falter due to replicable ambients or low entropy; reserve for high-security mobile logins like banking apps . For low-risk scenarios or indoor static settings, ambient fusion suffices to maintain efficiency without unnecessary signal emissions. The choice hinges on threat levels and environmental predictability

Optimizing efficiency. Minimize emissions to conserve battery life on wearables; implement adaptive batching for non-urgent verifications and leverage low-power audio modes. Sensor fusion can enhance accuracy without excessive cost, but selective activation based on context (e.g., motion detection) prevents drain Practical deployments should profile energy usage across device models to ensure longevity.

Operational considerations. Ensure cross-device compatibility through standardized signal parameters; implement privacy safeguards like on-device processing to avoid raw audio transmission. Regulations demand auditable logs without data leakage, so anonymize entries and integrate with compliance frameworks . Training users on system behaviors, though minimal due to zero-interaction, aids trust-building. Additional

notes include scalability: in multi-user environments, differentiate signals to avoid interference. Future-proofing involves monitoring hardware evolutions, as microphone sensitivities vary, potentially requiring recalibration protocols

V. Conclusion

Acoustic-based 2FA has transitioned from ambient-derived keys to advanced active sensing paradigms, delivering secure and intuitive alternatives to interactive verification. The domain acknowledges that (i) contextual audio must adapt to noise and attacks through controlled emis sions, (ii) active techniques provide precise proximity proofs while blending seamlessly into device capabilities, and (iii) efficiency is paramount for widespread adoption, achieved via optimizations like energy compensation and minimal interactions. The outlined workflow embodies these principles: initiate sensing on demand, extract ro bust signatures with adaptive processing, verify proximity efficiently using similarity metrics, and maintain audit trails for regulatory adherence. Moving forward, explorations into hybrid multi-modals for enhanced resilience, quantum-resistant cryptographic integrations to future proof against emerging computations, and AI-driven anomaly detection—tailored for mobile constraints—will further solidify acoustic 2FA's role in secure digital ecosystems, ensuring both protection and accessibility in an increasingly connected world

References

[1] D. Schürmann and S. Sigg, "Secure Communication Based on Ambient Audio," IEEE Trans actions on Mobile Computing, vol. 12, no. 2, pp. 358-370, Feb. 2013.
[2] H. T. T. Truong et al., "Comparing and Fusing Different Sensor Modalities for Relay At tack Resistance in Zero-Interaction Authentication," 2014 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), pp. 163-171, 2014.
[3] N. Z. Gong et al., "PIANO: Proximity-Based User Authentication on Voice-Powered Internet of-Things Devices," 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), pp. 2212-2222, 2017.
[4] N. Nguyen and S. Sigg, "Secure Context-Based Pairing for Unprecedented Devices," 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 119-124, 2018.
[5] Y. Ren et al., "Proximity-Echo: Secure Two-Factor Authentication Using Active Sound Sens ing," IEEE INFOCOM 2021- IEEE Conference on Computer Communications, pp. 1-10, 2021.
[6] Y. Ren et al., "Secure and Robust Two-Factor Authentication via Acoustic Fingerprinting," IEEE INFOCOM 2023- IEEE Conference on Computer Communications, pp. 1-10, 2023.
[7] Y. Ren et al., "Two-Factor Authentication Based on Acoustic Fingerprinting in Modulation Domain," IEEE Transactions on Mobile Computing, vol. 24, no. 5, pp. 4235-4247, May 2025.