Archives available at journals.mriindia.com

International Journal of Recent Advances in Engineering and Technology

ISSN: 2347-2812
Volume 14 Issue 1s, 2025

NEXUS-A Secure Voice Assistant Virtual Robot Using ZTA And Reinforcement Learning

Kalyani Joshi[1], Vaibhav Lonkar[2], Sakshi Jadhav[3], Prof. Mayuri Auti[4]

[1,2,3,4]*department of AI & DS engineering, Jaihind College of Engineering,* Pune, India
kalyanijoshi139@gmail.com[1],vaibhav.d.lonkar.86@gmail.com[2],jadhavsakshi109@gmail.com[3], maauti.jcoe@gmail.com[4]

Peer Review Information

Submission: 20 Jan 2025
Revision: 24 Feb 2025
Acceptance: 27 March 2025

Keywords

Voice Assistant
AI
Biometric Authentication
Zero Trust Architecture
Reinforcement Learning

Abstract

With the rapid advancement of voice assistant technology, ensuring security and privacy remains a critical challenge. This research introduces a Secure AI Voice Assistant Robot that incorporates Zero Trust Architecture (ZTA) and Multi-Factor Authentication (MFA) to establish a highly secure framework. By integrating Voice Biometric Authentication (VBA) and fingerprint recognition, unauthorized access is effectively mitigated. Additionally, Support Vector Machine (SVM) and Reinforcement Learning techniques enhance authentication accuracy and adaptive threat detection.

The proposed security model was rigorously tested under various threat scenarios, demonstrating its effectiveness in protecting sensitive user data. The integration of ZTA, MFA, and AI-driven security strategies provides a comprehensive defence against cyber threats and unauthorized intrusions. Moving forward, future improvements will focus on refining AI-driven anomaly detection, enhancing real-time security adaptability, and expanding encryption techniques to further secure sensitive interactions. These enhancements aim to bolster security while maintaining seamless user interaction.

INTRODUCTION

Voice assistants have transformed human-computer interaction, enabling hands-free operations in smart environments. However, security vulnerabilities, including unauthorized access, privacy breaches, and AI-based attacks, necessitate a more robust security framework.

To address these concerns, this paper introduces a Secure AI Voice Assistant Robot that integrates advanced security measures, including Zero Trust Architecture (ZTA), Voice Biometric Authentication (VBA), Multi-Factor Authentication (MFA), Support Vector Machine (SVM), and Reinforcement Learning. ZTA is a security model that assumes no entity inside or outside the network is trustworthy by default; thus, verification is required at every access point. VBA is a biometric authentication method that identifies users based on their unique voice patterns, ensuring an additional layer of security.

MFA further strengthens authentication by requiring multiple forms of identity verification, such as voice and fingerprint recognition. SVM is a machine learning algorithm used in the system to improve the accuracy of voice authentication by distinguishing between legitimate and unauthorized users. Reinforcement Learning, a type of machine learning that learns through continuous feedback, helps enhance security by dynamically adapting to potential threats.

By leveraging these technologies, this Secure AI Voice Assistant Robot ensures a high level of security while maintaining user-friendly interactions. The research aims to improve authentication precision, prevent unauthorized access, and offer a scalable security solution for AI-driven voice assistants.

LITERATURE SURVEY

[1] Dr. S. Brindha (2024) discuss the development of an intelligent AI-based voice assistant, emphasizing security and efficiency. Their study explores various authentication mechanisms and highlights the limitations of traditional password-based security. Our research extends this work by implementing ZTA, VBA, MFA, and AI-driven security enhancements.

[2] Shubham Singh (2024) investigate AI-based voice assistants and their role in home automation. They analyze vulnerabilities associated with smart home integrations and suggest security improvements. Our work builds upon their findings by integrating biometric authentication and reinforcement learning for enhanced security.

[3] Chu (2023) provide a systematic review of AI-based robots in education. Their research highlights the growing adoption of AI in various domains, emphasizing the importance of secure communication. Our study applies these insights to develop a security-focused voice assistant framework.

[4] Cheng and Roedig (2023) review security and privacy challenges in personal voice assistants. They identify risks such as data breaches, voice spoofing, and unauthorized access. Our research addresses these concerns by implementing SVM for authentication accuracy and reinforcement learning for adaptive security measures.

[5] Soori. (2023) explore AI, machine learning, and deep learning applications in robotics. Their work highlights the potential of AI-driven security mechanisms. Our study aligns with their findings by incorporating machine learning techniques such as SVM and reinforcement learning for authentication and threat detection.

[6] Sikarwar (2022) examines the implementation of AI-based voice assistants and their security challenges. Our research builds upon their work by proposing a more advanced security framework incorporating ZTA and biometric authentication.

[7] Vighnesh (2022) discuss voice-controlled home automation and security systems. Their study emphasizes the need for secure voice authentication in smart environments. Our work extends this by integrating MFA and AI-driven security enhancements.

[8] Jha (2022) presents a Python-based voice assistant. While their work focuses on implementation, our research enhances security aspects through advanced authentication mechanisms.

[9] Sharif (2020) analyze security vulnerabilities in smart home voice assistants. Their study underscores the risks associated with data privacy and unauthorized access. Our research mitigates these risks by integrating ZTA and AI-based security enhancements.

METHODOLOGY

The AI Voice Assistant Robot is developed with a multi-layered security architecture that integrates biometric authentication, AI-driven security enhancements, and Zero Trust principles.

System Architecture

The architecture of Secure AI Voice Assistant Robot follows a structured workflow ensuring secure authentication and interaction. As depicted in the architecture diagram:

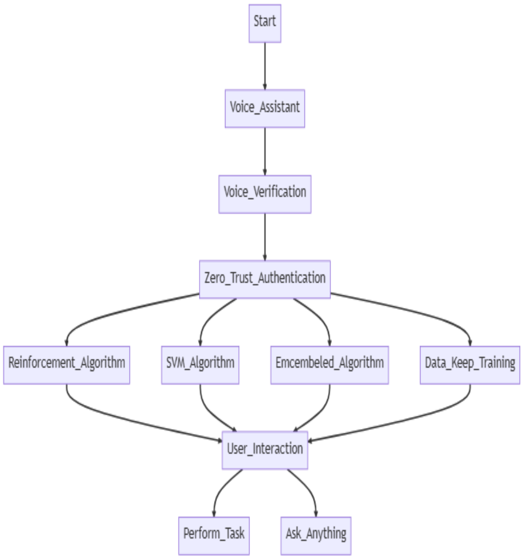

Fig 1. System Architecture

- Voice Assistant Activation: The system begins by enabling the voice assistant, awaiting user input.
- Voice Verification: The user's voice is analyzed for biometric authentication.
- Zero Trust Authentication: Every access request undergoes continuous verification. This includes:
- Reinforcement Learning Algorithm: Continuously learns and adapts based on security threats.
- SVM Algorithm: Classifies legitimate and unauthorized users for authentication accuracy.

- Ensemble Learning Algorithm: Enhances authentication robustness by combining multiple AI models.
- Data-Keeping & Training: Improves security performance through continuous model updates.
- User Interaction Module: Upon successful authentication, users can interact with the system to perform tasks or request information.
- Task Execution: The system securely processes commands while monitoring for potential security threats.

This architecture ensures high security and adaptability, minimizing risks of unauthorized access.

Technologies and Software Used

- Python: Used for AI model development and system logic implementation.
- TensorFlow/Keras: Frameworks for training deep learning models.
- OpenCV: Used for fingerprint and biometric verification.
- Support Vector Machine (SVM): Implements voice authentication and classification.
- Reinforcement Learning: Enhances adaptive security against evolving threats.
- Flask: Backend framework for system integration.
- SQL/NoSQL Database: Securely stores user authentication data.

Development Process

The development of the Secure AI Voice Assistant Robot involved multiple stages:

1. *Data Collection and Preprocessing*
   - Voice Data Acquisition: Users provided voice samples for biometric authentication.
   - Feature Extraction: Extracted key voice features such as MFCC (Mel-Frequency Cepstral Coefficients), pitch, and tone.
   - Fingerprint Data Collection: Stored digital fingerprint scans for multi-factor authentication.

2. *Model Training and Implementation*
   - Support Vector Machine (SVM) for Voice Authentication:
   - Trained on labeled voice datasets.
   - Classified user voice samples as "Authorized" or "Unauthorized."
   - Reinforcement Learning for Adaptive Security:
   - Implemented using Q-learning to adapt security measures dynamically.
   - Adjusts authentication sensitivity based on suspicious activity patterns.

3. *Integration with Zero Trust Architecture (ZTA)*
   - Continuous Verification: Each command undergoes security validation.
   - Role-Based Access Control (RBAC): Limits permissions based on authentication level.
   - Real-Time Threat Detection: Identifies unusual access attempts and blocks unauthorized requests.

4. System Testing and Optimization
   - Simulated Unauthorized Access: Tested against voice spoofing and biometric forgery.
   - Authentication Speed Optimization: Reduced processing delays in voice and fingerprint verification.
   - Security Stress Testing: Evaluated resilience against AI-based cyberattacks.

This development cycle ensures that our Secure AI Voice Assistant Robot achieves high authentication accuracy and strong security.

Training Dataset

The dataset includes voice biometric parameters, fingerprint verification status, and authentication results.

Columns:

- User_ID – Unique identifier for each user.

Pitch (Hz) – Fundamental frequency of the user's voice.

- MFCC Features – Extracted Mel-Frequency Cepstral Coefficients (MFCC) from voice samples.
- Energy Level (dB) – Measures voice amplitude.
- Fingerprint Match – Boolean value (1 = Match, 0 = No Match).
- Previous_Access_Attempts – Number of failed authentication attempts.
- Threat Score (0-1) – Dynamic security score calculated by Reinforcement Learning.
- Access Granted – Final authentication result (1 = Granted, 0 = Denied).

User_ID	Pitch (Hz)	MFCC_Feature_1	MFCC_Feature_2	Energy Level (dB)	Fingerprint Match	Previous_Access_Attempts	Threat Score	Access Granted

U001	120	0.25	-0.17	65	1	0	0.05	1
U002	200	0.38	-0.24	72	1	1	0.1	1
U003	135	0.2	-0.12	68	0	3	0.45	0
U004	180	0.29	-0.19	70	1	0	0.07	1
U005	150	0.21	-0.14	60	0	2	0.3	0
U006	210	0.4	-0.28	75	1	0	0.03	1
U007	165	0.27	-0.18	67	1	1	0.12	1
U008	140	0.22	-0.15	63	0	4	0.5	0
U009	190	0.35	-0.22	69	1	0	0.06	1
U010	175	0.3	-0.2	71	1	2	0.15	1
U011	160	0.26	-0.16	66	1	1	0.09	1
U012	145	0.23	-0.13	62	0	3	0.4	0
U013	155	0.28	-0.21	64	1	0	0.04	1
U014	205	0.39	-0.27	74	1	0	0.02	1
U015	185	0.32	-0.23	70	1	1	0.11	1
U016	130	0.18	-0.1	61	0	5	0.55	0
U017	195	0.36	-0.25	73	1	0	0.08	1
U018	170	0.31	-0.19	69	1	1	0.14	1
U019	125	0.19	-0.11	59	0	4	0.48	0
U020	220	0.42	-0.3	76	1	0	0.01	1

Explanation of Training Features:

Pitch (Hz): Higher frequencies indicate a sharper voice signature.

MFCC Features: Key extracted features from voice samples, analysed by SVM.

Energy Level (dB): Measures the intensity of the speaker's voice.

Fingerprint Match: A binary feature determining whether the fingerprint scan is valid.

Previous Access Attempts: Higher values may indicate potential security threats.

Threat Score: Determined by Reinforcement Learning, adjusting security dynamically.

Access Granted: Final classification label (1 for authenticated users, 0 for rejected users).

Usage in Machine Learning Models:

- SVM: Uses Pitch, MFCC Features, and Energy Level to classify authorized and unauthorized users.
- Reinforcement Learning: Adjusts authentication thresholds based on Threat Score.
- Multi-Factor Authentication (MFA): Ensures a combination of voice and fingerprint for security.

RESULT

The system was tested across multiple security scenarios, including unauthorized voice attempts, fingerprint spoofing, and AI-based attacks. Results show that VBA and fingerprint verification significantly reduce unauthorized access. The integration of SVM improves authentication precision, while Reinforcement Learning dynamically adapts security measures based on real-time threats. ZTA implementation enhances communication security and minimizes security breaches. The system successfully executes voice commands only when authentication criteria are met, ensuring a secure user experience. Compared to traditional voice assistants, this framework improves authentication accuracy and security resilience.

The testing data evaluates the performance of the Secure AI Voice Assistant Robot across multiple security scenarios. Key performance metrics include Authentication Accuracy (%), Threat Detection Rate (%), and False Acceptance Rate (FAR).

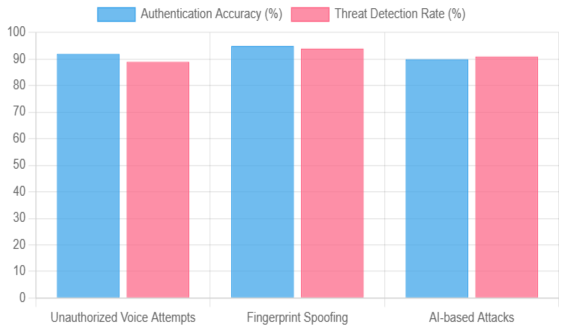

Fig 2. Testing in Real time

The system was tested in real-world conditions with various attack scenarios, such as voice spoofing, fingerprint duplication, and AI-driven adversarial attacks. The results demonstrated that the integration of SVM for voice classification and

Reinforcement Learning for adaptive security measures significantly improved authentication precision. The Zero Trust Architecture (ZTA) framework further ensured that every access request was continuously verified, enhancing overall security.

Conclusion

The Secure AI Voice Assistant Robot successfully integrates multi-factor authentication (MFA), Zero Trust Architecture (ZTA), and AI-driven security mechanisms to provide robust authentication and access control. The Support Vector Machine (SVM) model enhances voice authentication accuracy, while Reinforcement Learning dynamically adapts to emerging security threats. The biometric-based authentication prevents unauthorized access, and real-time monitoring ensures continuous security verification. The system has demonstrated high reliability in various attack scenarios, including voice spoofing, fingerprint duplication, and AI-based threats. By incorporating encrypted communication and access control mechanisms, the assistant maintains a secure environment for command execution and data protection.

Future research will focus on enhancing the assistant's security framework by integrating AI-driven anomaly detection and behavioral biometrics for improved identity verification. The system could also benefit from blockchain technology, ensuring tamper-proof authentication records. Additionally, improving natural language understanding (NLU) and user experience while maintaining security standards is crucial. Further, expanding the assistant's adaptability to IoT devices and smart home environments could make it a comprehensive security solution for next-generation AI voice assistants.

References

Dr. S. Brindha et al. (2024).“Intelligent AI Based Voice Assistant.” PSG Polytechnic College, Coimbatore, India.

Shubham Singh, Shubham Singh Panwar, Harsh Dahiya, and Khushboo (2024). “Artificial Intelligence Voice Assistant and Home Automation.” International Journal of Science and Research Archive, 12(01), 2006–2017. Accepted on 30 May 2024.

Chu, S.-T., Hwang, G.-J. and Tu, Y.-F. (2023). “Artificial Intelligence-Based Robots in Education: A Systematic Review of Selected SSCI Publications.”, National Taiwan University of Science and Technology .

Cheng, P., and Roedig, U. (2023). ““Personal Voice Assistant Security and Privacy— Survey.”

Soori M., Arezoo B., Dastres R. (2023). “Artificial Intelligence, Machine Learning and Deep Learning in Advanced Robotics: A Review.”, Department of Aeronautical Engineering, University of Kyrenia , Kyrenia, North Cyprus, Via Mersin 10, Turkey; CAD/CAPP/CAM

Sikarwar S. (2022).”AI-Based Voice Assistant. Department of Electronics and Communication, MITS Gwalior.

Vighnesh M, Andrew John, Merin Shibu and M Jagannath (2022). “Voice-controlled home automation, security system and virtual joystick-controlled robot for patients in home quarantines.” J. Phys.: Conf.Ser. 2318 012021.

Pratyush Jha (2022).” Voice Assistant using Python”

Sharif, K.et al. (2020).” Smart Home Voice Assistants: A Literature Survey of User Privacy and Security Vulnerabilities.” 10.1109/ACCESS.2020.2968526.

Tushar Gharge, Chintan Chitroda, Nishit Bhagat, Katha Priya Giri, “AI Smart Assistant,” International Research Journal of Engineering and Technology (IRJET),vol: 06 Issue: 01,PP-3862-3863,January 2019

Dr. Kshama, V. Kulhalli, Dr. Kotrappa Sirbi, Mr. Abhijit J. Patankar, “Personal Assistant with Voice Recognition Intelligence,” International Journal of Engineering Research and Technology. vol 10, no.1, pp. 416-418, (2017).

Kukade, Ruchita G. Fengse, Kiran D. Rodge, Siddhi P. Ransing, Vina M. Lomte "Virtual Personal Assistant for the Blind,” International Journal of Computer Science and Technology (JCST), vol 9, Issue 4, PP.2251-2253,October - December 2018.

M. A. Jawale, A. B. Pawar, D. N. Kyatanavar, “Smart Python Coding through Voice Recognition,” International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol: 8 Issue-10, PP-3283-3284, August 2019.

Isha S. Dubey, Jyotsna S. Verma, Ms. Arundhati Mehendale, "An Assistive System for Visually Impaired using Raspberry Pi," International Journal of Engineering Research & Technology (IJERT), vol 8 Issue 05, PP-608-609, May 2019.

VetonKëpuska, "Next-Generation of Virtual Personal Assistants (Microsoft Cortana, Apple Siri, Amazon Alexa, and Google Home)," International Journal for Research in Applied Science & Engineering Technology (IJRASET), vol 10 Issue 04, PP-2251-2253 Apr 2022